4(13)/2023

SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy

Czy branża security lubi dzielić się wiedzą?

Jak przekonać CEO, że cyberbezpieczeństwo jest ważne?

Czy szkolenia dotyczące cybersecurity stały się sposobem na biznes?

Automatyzacja procesów bezpieczeństwa

Jak dobrać skuteczne zabezpieczenie?

SPIS TREŚCI

SZANOWNI PAŃSTWO,

rozwijając się dla Was i mając na uwadze Wasze oczekiwania, staramy się tworzyć nowoczesne wydawnictwo, które spełnia wszelkie kryteria pisma dostarczającego unikalną, rzetelną i potwierdzoną doświadczeniem wiedzę.

W "Security Magazine" pojawił się dział newsowy, w którym zachęcamy firmy z branży do współtworzenia i przekazywania nam najnowszych informacji dotyczących osiągnięć, innowacji i sukcesów na skalę ogólnopolską czy światową. Prosimy o przesyłanie krótkich wiadomości nie starszych niż dwa tygodnie do dnia redakcyjnego deadlinu (20. dnia miesiąca poprzedzającego wydanie) na naszą skrzynkę e-mail.

Z okazji naszej wydawniczej rocznicy zorganizowaliśmy konkurs, w którym wspólnie wyłoniliśmy "Artykuł Roku Security Magazine". Serdecznie gratuluję zwycięzcom, a Wam, Czytelnicy, dziękuję za zaangażowanie w głosowanie na najlepszy tekst.

Widać, że rosnące tempo naszego rozwoju sprawia, że stajemy się coraz ważniejszym partnerem dla firm z branży security i cybersecurity. Coraz częściej otrzymujemy prośby o patronat medialny nad najważniejszymi branżowymi wydarzeniami w Polsce. Firmy obdarzają nas zaufaniem, publikując na łamach naszego e-pisma swoje wizytówki, a indywidualni eksperci chętnie nawiązują z nami współpracę redakcyjną. W wywiadach udzielanych naszemu magazynowi znani branżowi fachowcy dzielą się swoimi przemyśleniami. Treści naszych autorów docierają średnio do 30 tys. osób (liczba pobrań) miesięcznie.

Serdecznie polecam lekturę tego wydania i zachęcam do współpracy!

Rafał Stępniewski

ARTYKUŁ ROKU SECURITY MAGAZINE

Mamy zaszczyt ogłosić wyniki konkursu “Artykuł Roku Security Magazine”! Przez ostatni miesiąc głosowaliście na najlepszy artykuł opublikowany w ciągu ostatniego roku na łamach naszego e-pisma. Dziękujemy za liczne głosy i aktywny udział w konkursie, a zwycięzcom serdecznie gratulujemy!

Na łamach wydań 1-11 “Security Magazine” ukazało się ponad 100 artykułów, spośród których jury redakcyjne, organizując konkurs "Artykuł Roku Security Magazine" z okazji pierwszej rocznicy naszego wydawnictwa wyłoniło finalistów.

W pierwszym etapie 23 lutego wybraliśmy osiem spośród 100 artykułów eksperckich.

Kryteria wyboru:
a) **Wartość merytoryczna:** Artykuł zawiera merytorycznie bogatą i aktualną treść.
b) **Jakość informacji:** Artykuł jest oparty na wiarygodnych źródłach i zawiera rzetelne informacje.
c) **Jasność i przejrzystość prezentowanych idei:** Artykuł jest łatwy do zrozumienia i czytania. Napisany w jasny sposób, a prezentowane w nim idee oraz pomysły są przejrzyste i logiczne.
d) Poprawność językowa: Artykuł napisany w poprawnej formie językowej i zgodnie z wytycznymi redakcyjnymi.
e) **Oryginalność.**

Drugi etap to wyłonienie 24 lutego przez jury czterech spośród ośmiu artykułów.

Kryteria wyboru oprócz powyższych to dodatkowo:
a) **Wpływ:** Artykuł ma realny wpływ na czytelników i ich postawy wobec bezpieczeństwa w firmie.
b) **Praktyczność**: Artykuł zawiera praktyczne wskazówki i narzędzia, które można zastosować w praktyce w celu poprawy bezpieczeństwa w różnych kontekstach.

Czwórka finalistów wzięła udział w głosowaniu Czytelników na LinkedIn i Facebooku. Ostateczne o wynikach konkursu zdecydowały głosy Czytelników.

Gratulujemy zwycięzcom i finalistom!

Na zwycięzców czekają nagrody, które w realny sposób przyczynią się do budowania przez nich marki ekspertów, a po szczegóły odsyłamy do REGULAMINU KONKURSU.

Chcemy podziękować wszystkim Czytelnikom, którzy wzięli udział w konkursie i oddali swoje głosy. Bez Waszego zaangażowania nie byłoby możliwe wyłonienie zwycięzcy. **Dziękujemy, że jesteście z nami!**

Zapraszamy do lektury kolejnych wydań “Security Magazine” i artykułów grona eksperckiego. Razem tworzmy społeczność entuzjastów bezpieczeństwa, wymieniających się wiedzą i doświadczeniami oraz tych, którzy tej wiedzy potrzebują.

ZWYCIĘZCY KONKURSU ARTYKUŁ ROKU SECURITY MAGAZINE

1 intellias

"INFORMACYJNE BEZPIECZEŃSTWO PRZEDSIĘBIORSTWA PRZY OGRANICZONYM BUDŻECIE"

173 GŁOSY

2 GRANDMETRIC

"KORZYŚCI KONTROLOWANYCH ATAKÓW HAKERSKICH"

98 GŁOSÓW

---

48 GŁOSÓW tpay

"E-HANDEL NA MUSZCE CYBERPRZESTĘPCÓW. JAK POWINIEN BRONIĆ SIĘ RYNEK?"

3 GŁOSY seris konsalner

"TECHNOLOGIZACJA BRANŻY SECURITY. OSZCZĘDNOŚCI A ROSNĄCA PRESJA PŁACOWA"

SECFENCE POD SKRZYDŁAMI GOOGLE

Polski startup Secfense znalazł się wśród 15 firm z 8 europejskich krajów, wybranych do uczestnictwa w Google for Startups Growth Academy: Cybersecurity. Wśród 120 zgłoszeń, krakowska firma zyskała szansę na rozwój dzięki wsparciu Google. Startupy uczestniczące w programie mają istotny wkład w zabezpieczenie aplikacji zdrowotnych, obronę edukatorów i ochronę łańcucha dostaw czystej wody. Google udostępni im najlepsze narzędzia, praktyki i kontakty, pomagając w dalszym rozwoju.

STRATY LICZONE W SETKACH TYSIĘCY

7% firm w Polsce może pochwalić się pełną dojrzałością swoich systemów cyberbezpieczeństwa - wynika z 1. edycji raportu Cisco Cybersecurity Readiness Index: Resilience in a Hybrid World. W skali globalnej jest to 15% firm. Koszt bycia nieprzygotowanym może być wysoki - 59% pytanych z Polski stwierdziło, że w ciągu ostatniego roku doświadczyło incydentu związanego z cyberbezpieczeństwem.
W 51% przypadków straty przekroczyły 100 tys. USD, a w 18% - aż 500 tys. USD.

CYBERBEZPIECZEŃSTWO W SZKOŁACH

"Zdolność zarządzania technologią jest ważna, by pomóc uczniom w znalezieniu dobrej pracy. Pracodawcy szukają osób, które mają umiejętności związane z podejmowaniem wyzwań technicznych i cyberataków" - powiedział gubernator Dakoty Północnej. Tam do szkół publicznych wchodzi przedmiot: cyberbezpieczeństwo. Jest to pierwszy stan w USA, który zdecydował się na taki krok.

Zapraszamy do dzielenia się z nami newsami (do 500 zzs) z Twojej firmy, organizacji, które mają znaczenie ogólnopolskie i globalne.

Zachęcamy do przesyłania newsów na adres redakcja@securitymagazine.pl do 20. dnia każdego miesiąca.

Redakcja "Security Magazine"


ZAPISZ SIĘ NA
NEWSLETTER
BY NIE PRZEOCZYĆ
KOLEJNEGO WYDANIA
SECURITY MAGAZINE
Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy
SECURITY MAGAZINE
ZAPISZ SIĘ
NEWSLETTER
YOUR EMAIL HERE
SUBSCRIBE

CZY BRANŻA SECURITY LUBI DZIELIĆ SIĘ WIEDZĄ?

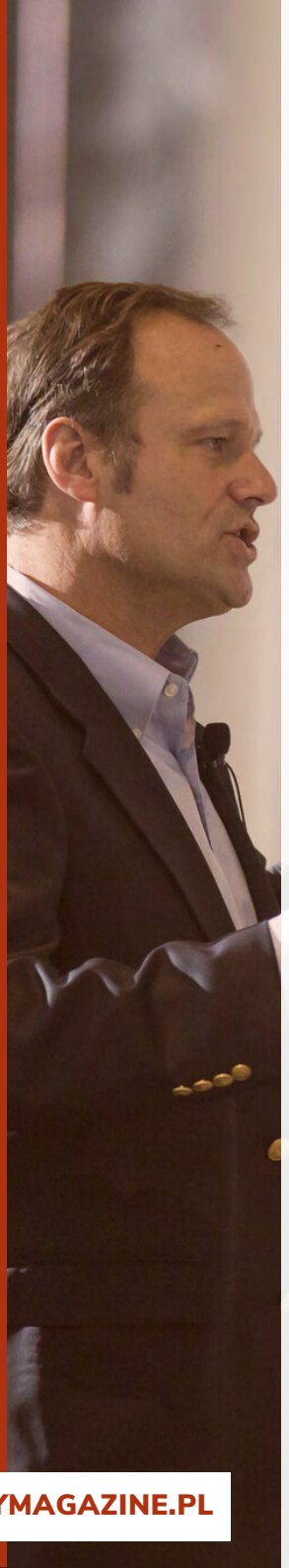
Daniel Kamiński
AlertControl

W rozmowie z ekspertem, Danielem Kamińskim, prezesem AlertControl, zastanawiamy się, czy mówienie na szerokim forum o wiedzy i doświadczeniu ekspertów związanych z bezpieczeństwem nadal jest tematem tabu? Dlaczego? Jakie branża ma obawy z tym związane? Czy firma przez dzielenie się wiedzą może utracić przewagę konkurencyjną? A może zbuduje reputację, zaufanie i lojalność klientów, co w dalszej perspektywie przyspieszy rozwój branży bezpieczeństwa?

Czy i co zmieniło się w branży security na przestrzeni ostatnich lat, że stała się ona bardziej otwarta na dialog, na dzielenie się wiedzą, mówienie szerokiemu odbiorcy o rozwiązaniach, doświadczeniu?

Daniel Kamiński: Nie jestem pewien, czy branża security stała się bardziej otwarta na dzielenie się wiedzą. Moim zdaniem, tylko mała jej część, która chce się przygotować na przyszłościowe wyzwania, stała się bardziej odważna, innowacyjna. Oczywiście, firmy o międzynarodowych korzeniach mają szybszy dostęp do najlepszych praktyk. Mogą korzystać z 150-letniej historii doświadczeń i zwykle promują otwarte podejście. W takich firmach jest więcej uznanych autorytetów i wizjonerów. Mniejsze firmy regionalne opierają się najczęściej na doświadczeniu oraz przedsiębiorczości swoich właścicieli. Tam więcej jest naśladowców, którzy starają się ograniczyć ryzyka, wdrażając sprawdzone rozwiązania.

Transformacja, której jesteśmy świadkami, pozwoliła zaistnieć firmom, które zaczęły rozwijać się szybciej niż rynek. Właściciele tych firm i ich kadra zarządzająca uczestniczą w konferencjach, testują nowe rozwiązania, tworzą innowacyjne usługi. Nie boją się dzielić informacjami. Wiedzą, że od pomysłu do wdrożenia mija minimum dwa lata, więc gdy konkurencja uruchomi podobne rozwiązanie, pomysłodawcy będą dominującym graczem.



Jakie korzyści niesie ze sobą dzielenie się wiedzą w branży ochrony i security?

D.K.: Jedną z głównych korzyści jest budowanie świadomości klientów oraz przedstawicieli branży. Nasz rynek ma dopiero 35 lat, wiele rzeczy odkrywamy na bazie własnych doświadczeń. Ze względu na niskie koszty pracy nasz rynek przypominał model ochrony znany z krajów azjatyckich (np. Malezja, Filipiny) czy afrykańskich (np. RPA). Mało techniki, za to pracownik ochrony fizycznej na każdym "rogu". Dziś szybki wzrost płacy minimalnej powoduje, że liczba pracowników ochrony maleje i wzrasta ilość zabezpieczeń elektronicznych. Brakuje kadry technicznej, bo inne branże lepiej płacą.

Dociekliwe osoby obserwujące inne rynki mogą zauważyć, że w krajach Europy Zachodniej podobne zjawiska miały miejsce kilkanaście lat temu. Tamte rynki musiały się przeorganizować. Dziś mają mało ochrony fizycznej, bo tańszy jest leasingowany robot patrolujący (15 euro na godzinę) niż człowiek w ochronie (18 euro na godzinę). U nas nie ma jeszcze takich stawek, ale szybko idziemy w tym kierunku i myślę, że, za kilka lat się spotkamy. Powinniśmy więc podpatrywać, jaką drogę przeszły firmy na innych rynkach oraz dostosowywać ją do obecnych możliwości technologicznych. Dzielenie się wiedzą wpłynie na poprawę jakości usług, wzrost zaufania do przedstawicieli branży oraz na większe zainteresowanie wśród talentów. Rolą stowarzyszeń branżowych i osób rozpoznawalnych w branży jest dzielenie się wiedzą i wpływanie na postrzeganie naszej branży.

W jaki sposób publikowanie artykułów w branżowych czasopismach i uczestnictwo w konferencjach wpływają na rozwój osobisty i zawodowy?

D.K.: Pisanie artykułów to odpowiedzialność. Treści są oceniane przez czytelników, więc trzeba się przygotować. Zebrać informacje, przestudiować dostępne publikacje, omówić zagadnienie z innymi specjalistami. To powoduje, że pisząc artykuł uczymy się

i porządkujemy swoją wiedzę. Z kolei udział w konferencjach, to szansa na wymianę opinii. Konfrontację wiedzy i doświadczeń z innymi specjalistami. To miejsce, gdzie uważny słuchacz pozna potrzeby klientów i będzie mógł poszerzyć doświadczenia. W trakcie kolejnej konferencji będzie mógł mówić językiem korzyści, który dociera do słuchaczy. Tego nie da się uzyskać w zaciszu biura.

Czy istnieją jakieś ryzyka związane z dzieleniem się wiedzą w branży ochrony i security? Jakie są najczęstsze obawy?

D.K.: Dzieląc się wiedzą, musimy być ostrożni. Niechcący możemy pomóc przestępcom pokonać zabezpieczenia. Dlatego w miejscach publicznych nie wyjaśniamy wrażliwych kwestii oraz nie dzielimy się szczegółami na temat tego, jak przestępcy dokonali włamania.

Omawiamy ogólne kwestie, wpływamy na wyobraźnię i stymulujemy proces myślowy. Oczywiście, w kuluarach, wśród znanych nam osób dzielimy się zaawansowaną wiedzą. Część osób z mniejszym doświadczeniem irytuje się, gdy nie chcemy rozmawiać o szczegółach. To szczelne środowisko, ale wraz z ilością wdrożeń, stają się jego częścią.

Wśród pracowników istnieje przesąd, że nie warto się dzielić wiedzą, bo inna osoba zabierze nam pracę. Mam inne zdanie, moja ścieżka kariery opiera się na tym, że awansowałem, gdy miałem wyszkolony zespół na tyle, że mogli pracować beze mnie. Miałem sporo szczęścia, że trafiałem na ludzi, którzy cenili rozwój współpracowników. Wielu z nich do dziś to moi mentorzy.

Jakie metody dzielenia się wiedzą są, Pana zdaniem, najskuteczniejsze? Czy preferuje Pan jakieś konkretne kanały komunikacji?

D.K.: Wszystko zależy od tego, do jak dużej grupy chcemy dotrzeć. W przypadku kilku osób najlepsze jest osobiste spotkanie. Bardzo dobre są konferencje, tam można mówić do dużej grupy, nawet kilkuset osób. Niestety, efekt jest mniejszy, tylko część osób odbierze przekaz.

Artykuły mają dużą siłę. Docierają do wielu osób. Działają wolno, tak jak kropla drąży skałę, ale zostawią wyraźny ślad. Obecnie jeszcze skuteczniejsze w masowym przekazie są krótkie filmy 1-2 minutowe na YouTube czy 15-20 sekundowe na TikToku. Szybkie, krótkie, celowane przekazy zmieniają świat. Nie mam w tym jeszcze doświadczenia, ale

mocno obserwuję ten trend. Aby dotrzeć do szerokiego grona, trzeba m.in. dostosować swój język do poziomu zrozumienia zwykłych ludzi, a nie tylko specjalistów i ekspertów.

Jakie podjąć kroki, by móc zrealizować ten cel?

D.K.: To trudne pytanie, bo dotyczy własnych ograniczeń. Nie widzimy swoich słabości, muszą nam o nich powiedzieć najbliższe życzliwe osoby. My musimy być gotowi usłyszeć ten przekaz. Ja przez długi ok-res koncentrowałem się na współpracy ze specjalistami. Mówiłem żargonem, zakładałem, że rozmówca ma podstawy, więc mogę mówić skrótami. Im większą miałem wiedzę, tym częściej widziałem, że inne osoby nie mogą mnie zrozumieć. Nawet korektorzy artykułów mieli wiele pytań o wyjaśnienie znaczenia zdania czy akapitu.

Wtedy zrozumiałem, że co mi po wiedzy, jeśli nie jestem w stanie wy-tłumaczyć zwykłemu człowiekowi, na czym polega różnica między profesjonalnym rozwiązaniem oraz marketowym. Zacząłem zmieniać słownictwo, aby brzmieć mniej 'profesorsko". Postanowiłem wplatać historie z życia, aby słuchacze oczyma wyobraźni mogli się z nimi utożsamiać. Testowałem i nadal testuję swoje umiejętności na sąsiadach, we wpisach na portalach społecznościowych, itp. Pracuję nad tym i wiem, że jeszcze trochę czasu będę potrzebował, aby mówić zwykłym językiem o technicznych aspektach.

Jakie korzyści niesie ze sobą używanie prostszego języka dotyczącego branży security, ale skierowanego do osób, które chciałyby skorzystać ze wsparcia tejże branży? Czy uważa Pan, że to pozytywnie wpłynęło na Pana biznes i budowanie marki?

D.K.: Prostszy język dociera do większej grupy ludzi. Buduje zaufanie wśród klientów. To przekłada się na zamówienia. Wzrost zaproszeń do projektów oraz wzrost wartości

projektów potwierdzają, że to skuteczny sposób zarówno na samorozwój, ale również na lepsze osiągnięcia dla firmy. Porównując to do piłki nożnej, inne sukcesy ma się, grając w lidze okręgowej, a inne w ekstraklasie. Większe i ciekawsze projekty powodują wzrost doświadczenia, pozwalają zająć się jeszcze ciekawszymi projektami. Dzięki takiemu podejściu miałem okazję uczestniczyć w międzynarodowych projektach. Zapewne nie jest to ścieżka dla każdego, ponieważ przy każdym nowym lub większym projekcie, trzeba się wiele nauczyć w krótkim czasie. Ale mnie to pasjonuje.

Jakie są Pana przemyślenia na temat przyszłości branży ochrony i security? Czy widzi Pan wyzwania, które stoją przed ekspertami w tych dziedzinach w najbliższym czasie?

D.K.: Branża się zmieni i to bardzo. Obecna konsolidacja rynku przyśpieszy - zostaną firmy gotowe na rozwój technologiczny. Wiele usług zniknie z rynku, część zostanie zastąpiona techniką, część przejdzie do IT/ICT. Wzrosną koszty pracy, jeszcze trudniej będzie znaleźć osoby na techniczne stanowiska. Firmy wyspecjalizują się w instalacjach teletechnicznych, zarządzaniu załogami interwencyjnymi, itp. Dziś możemy zaobserwować to w Wielkiej Brytanii, Francji, Holandii. Duża część klientów indywidualnych zrezygnuje z ochrony, bo pracując zdalnie, będą cały czas w domach. Rozwinie się self-monitoring, który na świecie ma cztery razy więcej użytkowników niż profesjonalne usługi, z kolei w Polsce jest mało popularny. Zwiększy się podział na duże i małe instalacje, bo są tam potrzebne inne kompetencje. Centrum monitorowania coraz częściej będzie migrowało w kierunku SOC (security operation center w cyberbezpieczeństwie). Zmieni się dużo i utrzymają się tylko firmy i osoby gotowe do samorozwoju otwarte na przyszłościowe wyzwania.

W jaki sposób dba Pan o rozwój swoich kompetencji zawodowych w branży ochrony i security? Jakie źródła wiedzy Pan preferuje?

D.K.: Dużo czytam publikacji międzynarodowych. Jeżdżę na targi security do innych krajów (od Tajwanu po USA). Spotykam się z dostawcami rozwiązań i rozmawiam z nimi o tym, co przyniesie przyszłość. Umawiam się z dużymi krajowymi firmami i międzynarodowymi przedstawicielami firm w Polsce, aby poznać ich plany inwestycyjne, wiedzieć, czego szukają. Rozmawiam z wiodącymi autorytetami na konferencjach, aby się inspirować innym spojrzeniem na świat. Sam chodzę na szkolenia, ale również szkolę innych. Dopytuję się moich partnerów biznesowych o to, jak osiągnęli sukces. Co ciekawe, każda osoba, która osiągnęła sukces, chętnie dzieli się tym, gdy zapytamy.

Jakimi radami chciałby Pan podzielić się z osobami, które dopiero zaczynają swoją karierę w branży ochrony lub security i chcą osiągnąć sukces w swojej dziedzinie?

D.K.: Po prostu rozwijajcie się. Dajcie sobie czas i zgłaszajcie się do wielu ciekawych projektów, które dadzą Wam doświadczenie. Przy odrobinie szczęścia znajdziecie życzliwego mentora, który pomoże Wam rozwinąć skrzydła.

Dziękujemy za rozmowę.

Rozmawiała:
Monika Świetlińska

PATRONAT
SECURITY MAGAZINE

POLSECURE 2023

MIĘDZYNARODOWE TARGI 25-27 KWIETNIA

Zaplanowane w terminie od 25 do 27 kwietnia Międzynarodowe Targi POLSECURE będą okazją do zapoznania się z ofertą firm specjalizujących się w produkcji wyposażenia specjalnego, środków ochrony osobistej, sprzętu ratowniczego, oprogramowania łączności, dowodzeniu czy kontroli oraz do wymiany doświadczeń i rozmów o rzeczywistych potrzebach służb mundurowych.

Wydarzenie odbędzie się po raz drugi pod Honorowym Patronatem Ministra Spraw Wewnętrznych i Administracji i po raz kolejny organizowane jest przy wsparciu Komendy Głównej Policji. Partnerem strategicznym jest Grupa WB. Wśród wystawców, którzy do tej pory potwierdzili swój udział w wydarzeniu są m.in. Enigma Systemy Ochrony Informacji Sp. z o.o., GLOMEX-MS POLSKA Sp.z o.o., Griffin Group S.A. Defence Sp. k., Grupa WB, HOLSTERS HPE Polska Grzegorz Szymański, KLIMAWENT S.A., , LUBAWA, MEGMAR LOGISTICS & CONSULTING Sp. z o.o., MODULAR SYSTEM, Spółki Polskiej Grupy Zbrojeniowej, TRANSCOM INTERNATIONAL, TVPRZEMYSLOWA NOWAK SPÓŁKA KOMANDYTOWA, WORKS 11 Sp.z o.o., ZDUNEK PREMIUM Sp. z o.o. i inne.

Targi dedykowane są służbom odpowiedzialnym za bezpieczeństwo publiczne, w tym Policji, Straży Granicznej, Straży Pożarnej, a także Służbie Ochrony Państwa i Służbie Więziennej. Ofertą mogą też być zainteresowane służby specjalne, Krajowa Administracja Skarbowa oraz organizacje ratownicze GOPR, TOPR, WOPR. POLSECURE 2023 będzie miało też ofertę skierowaną do ratowników medycznych. Merytorycznym uzupełnieniem wystawy będzie międzynarodowa konferencja organizowana przez KG Policji.

POLSECURE dołączyło w 2022 roku do portfolio Targów Kielce obok wystaw skierowanych do służb mundurowych.

Targi Kielce
exhibition & congress centre
30 LAT YEARS

polsecure

II Międzynarodowe Targi POLSECURE

25-27.04.2023

WYDARZENIA TOWARZYSZĄCE

- **Międzynarodowa Konferencja Policyjna**
  Zakres tematyczny: cyberbezpieczeństwo, laboratorium kryminalistyczne, logistyka
- **Pokazy dynamiczne**
- **Prezentacje sprzętu**

Więcej informacji na **polsecure.targikielce.pl**

Patronat Honorowy

Minister Spraw Wewnętrznych i Administracji

POLICJA

SŁUŻBA WIĘZIENNA

RCB

LOTNICZE POGOTOWIE RATUNKOWE

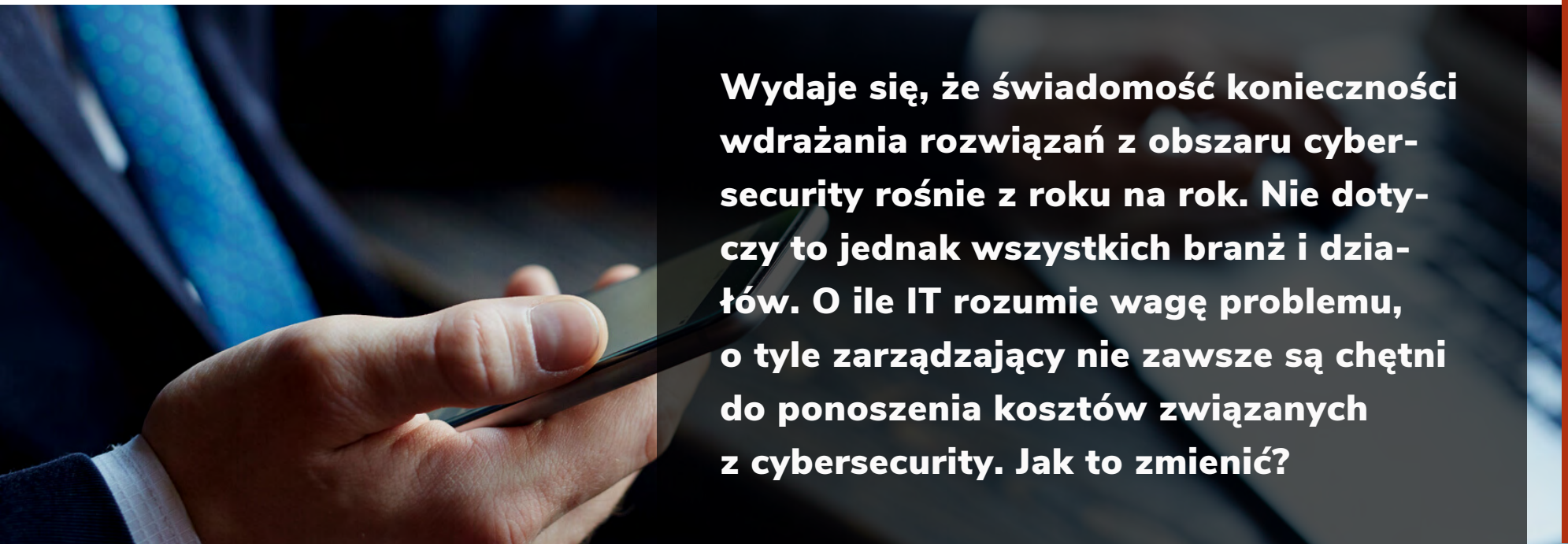
NCBR
Narodowe Centrum Badań i Rozwoju

INSPEKCJA TRANSPORTU DROGOWEGO

ABW

JAK PRZEKONAĆ CEO, ŻE CYBERBEZPIECZEŃSTWO JEST WAŻNE?

Krzysztof Andrian
Concept Data



Wydaje się, że świadomość konieczności wdrażania rozwiązań z obszaru cybersecurity rośnie z roku na rok. Nie dotyczy to jednak wszystkich branż i działów. O ile IT rozumie wagę problemu, o tyle zarządzający nie zawsze są chętni do ponoszenia kosztów związanych z cybersecurity. Jak to zmienić?

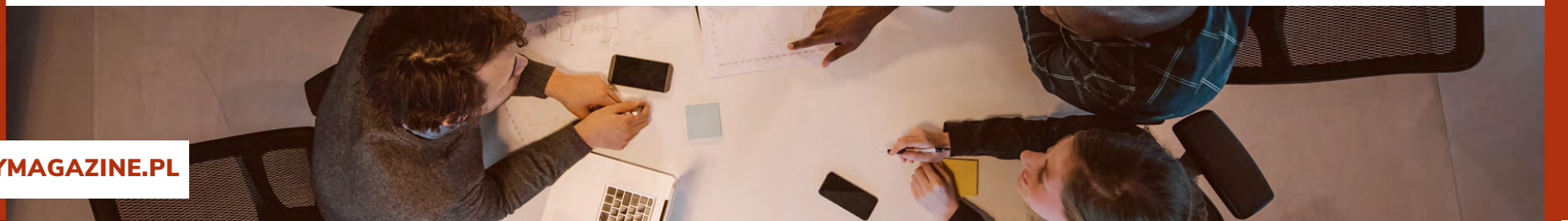
Przekonanie nieprzekonanych nie jest łatwe, ale jednak możliwe. Kluczowe staje się w tym procesie budowanie świadomości tego, czym jest cyberatak, w kogo mogą uderzyć cyberprzestępcy i – co najważniejsze – jak taki atak może wpłynąć na działalność całej firmy. A wraz ze zmieniającym się sposobem prowadzenia biznesu, z rozrastającą się infrastrukturą IT i liczbą aplikacji biznesowych wykorzystywanych na co dzień oraz wraz z rosnącymi możliwościami cyberprzestępców ten wpływ staje się coraz bardziej dotkliwy.

WYCIEK DANYCH TO NIE TYLKO PROBLEM IT

Najważniejsze jest to, by przekonać zarządzających, że cyberatak nie jest sprawą IT. A wiele osób tak myśli. „Nawet jeśli coś się stanie, dział IT albo zewnętrzna firma rozwiążą nasz problem, usuną wirusy, doprowadzą systemy do porządku i po kilku godzinach wszystko będzie działać jak przed incydentem. Ostatecznie wydamy jakieś pieniądze na odzyskanie danych, gdyby nasze zasoby zostały zaszyfrowane przez ransomware."

To jest bardzo krótkowzroczne myślenie. Po pierwsze – koszty, które niesie ze sobą cyberatak, są ogromne. Jak wynika z raportu FBI, tylko w Stanach Zjednoczonych szkody finansowe wynikające z cyberataków osiągnęły w 2022 roku 10,2 mld dolarów. Warto zwrócić uwagę, że same koszty okupu, odzyskania danych, uruchomienia infrastruktury IT czy opłacenia kar (np. wynikających z RODO) są tylko czubkiem góry lodowej.

Firma po cyberataku cierpi na wiele różnych sposobów. Mało która firma działa dziś w oderwaniu od innych, od kanałów cyfrowych. Prawie każda kontaktuje się z podwykonawcami czy kontrahentami przez pocztę e-mail, często udostępnia im swoje systemy. W przypadku zainfekowania tych systemów złośliwym oprogramowaniem cierpi reputacja firmy i jej kontakty z partnerami i współpracownikami, którzy zaczynają się zastanawiać, czy oni sami są teraz bezpieczni. Dodatkowo – jeśli z firmy wycieką dane klientów, zaufanie do niej maleje. Badania pokazują też, że spadają wyceny skutecznie zaatakowanych spółek.



Dodatkowo – przywracanie systemów po cyberataku i tym samym – płynności pracy może trwać naprawdę długo. A każdy dzień przestoju to dodatkowy koszt, to niewywiązanie się z umów, to nieporozumienia z kontrahentami, usługobiorcami i klientami. Problem jest zatem znacznie szerszy i stanowczo dotyczy nie tylko działów IT, ale i zarządów przedsiębiorstw.

KTO POWINIEN MYŚLEĆ O CYBERBEZPIECZEŃSTWIE?

Pytanie brzmi – czy dotyczy wszystkich firm w takim samym stopniu. Oczywiście nie. Jest część firm, których świadomość zagrożenia jest bardzo wysoka, bo albo doświadczyły już cyberataku lub działają w regulowanych branżach (bankowość i ubezpieczenia, medycyna, farmacja). Wiele pozostałych traktuje cyberbezpieczeństwo jako zło konieczne. Dopóki nic złego się nie stanie, nie chcą inwestować w narzędzia i standardy, które mogą zapobiec incydentom.

To nie jest jednak rozsądne działanie. Jeśli zarządzający chce wiedzieć, czy powinien traktować cyberbezpieczeństwo poważnie, musi odpowiedzieć sobie na podstawowe pytanie: które dane w organizacji stanowią o jej przewadze konkurencyjnej? Następnie powinien przeanalizować, gdzie te dane są przechowywane i jak dobrze chronione. Prawdą jest, że każda firma, które przewaga konkurencyjna opiera się na własności intelektualnej, powinna szczególnie chronić swoje zasoby. Wyniki badań R&D, prototypy, patenty – to są dane wrażliwe, które również mogą zainteresować cyberprzestępców. A ich upublicznienie wiąże się z utratą konkurencyjności i roli na rynku.

BIZNES CORAZ PODATNIEJSZY

Zagadnienie cyberbezpieczeństwa jest coraz ważniejsze – i to w coraz większej liczbie przedsiębiorstw – bowiem wyraźnie zmieniają się wykorzystywane w biznesie modele pracy. Rozproszenie zespołów, praca zdalna, praca na urządzeniach mobilnych, coraz więcej aplikacji biznesowych w chmurze, coraz więcej zewnętrznych partnerów, kontrahentów, współpracowników łączących się w taki czy inny sposób z systemami wewnętrznymi firmy – w takich warunkach coraz ciężej jest dbać o bezpieczeństwo danych. I coraz łatwiej wpuścić do sieci firmy osobę niepowołaną.

To sprawia, że każda firma pracująca w takim modelu (a tak naprawdę wystarczy, żeby zarząd firmy pracował na laptopach poza firmową siecią, by mieć do czynienia z modelem rozproszonym) musi zwrócić szczególną uwagę na ochronę zasobów informacyj-nych. Absolutną podstawą jest w tym przypadku dbanie o bezpie-czny dostęp do systemów, zarządzanie cyfrową tożsamością, wdra-żanie wieloskładnikowego uwierzytelniania, narzędzi SSO, Adaptive MFA.

Innym słowem dbanie o to, aby do firmowej sieci nie dostały się niepożądane osoby, które wykradną dane czy zainfekują systemy złośliwym oprogramowaniem. Jedynym sensownym podejściem, które powinny stosować firmy pracujące w zespołach rozproszonych, jest podejście Zero Trust – czyli traktowanie każdej osoby próbującej dostać się do systemów firmy z podejrzliwością i sprawdzanie jej.

PODEJŚCIE HOLISTYCZNE I PARTNERSTWO Z DOSTAWCĄ

Rozumiem jednak, że to, co dla ludzi IT jest oczywiste, dla zarządów czy dyrektorów finansowych może być zupełnie nieznanym obszarem. A w takich warunkach pojawia się nieufność i wątpliwości. Jakie rozwiązania wybrać? Czy zainwestować w to, co jest dziś „modne", czy raczej w niszowe rozwiązania? Co zrobić, żeby nie przepłacić? Skoro w IT wszystko się tak szybko zmienia, jaką mam gwarancję, że to, co wybiorę dziś, sprawdzi się także jutro? I w końcu – a co, jeśli to wcale nie zadziała?

I na takie wątpliwości można znaleźć odpowiedź. Rośnie dziś rola partnerstwa biznesowego, także z dostawcą rozwiązań z zakresu cyberbezpieczeństwa. I z własnego doświadczenia mogę powiedzieć, że tylko taka współpraca ma sens. Nie da się skutecznie zabezpieczyć przedsiębiorstwa, wdrażając rozwiązanie, które co prawda sprawdza się globalnie, ale niekoniecznie pasuje do strategii i procesów działających w konkretnej firmie.

Podstawą wyboru rozwiązań security jest ścisła kooperacja z dostawcą. Z dostawcą, który z jednej strony ma w portfolio różne narzędzia IT, a z drugiej dogłębnie pozna całą firmę, jej procesy, plany rozwoju i strategię (przynajmniej średnioterminową, jeśli nie długoterminową), technologie, z jakich korzysta – i dopiero na podstawie tej wiedzy zaproponuje roz-

wiązania, które będą dopasowane do potrzeb przedsiębiorstwa.

Dlaczego to takie ważne? Bo cyberbezpieczeństwa nie da się potraktować w kategoriach zadania na miesiąc czy dwa. Żeby strategia zabezpieczeń była skuteczna, musi być całym programem rozpisanym na lata. Musi obejmować nie tylko narzędzia, ale też procesy i ludzi. Bo to ludzie są najsłabszymi ogniwami bezpieczeństwa, to oni z braku czasu chcą chodzić na skróty. Same narzędzia zatem nic nie dadzą, jeśli nie powiąże się ich ze sposobem pracy oraz z edukacją i szkoleniami pracowników.

Co ważne, to nie jest marzenie, do którego warto dążyć, ale bardzo realny i funkcjonujący na rynku model współpracy. W Concept Data od lat właśnie w taki sposób pracujemy z naszymi klientami, dla których jesteśmy przede wszystkim doradcami. Nie tylko proponujemy rozwiązania, które będą w konkretnym przypadku najskuteczniejsze, ale też tworzymy strategie transferu wiedzy oraz analizujemy to, co już w ramach cyberbezpieczeństwa zostało w firmach wdrożone. Bo technologie zmieniają się bardzo szybko – i podejście, które zostało zastosowane w firmie kilka lat temu, może wymagać dziś mniejszego lub większego odświeżenia.

CO PRZEKONA ZARZĄD?

Podsumowując. Gdybym miał stworzyć listę argumentów, które warto przedstawić zarządowi niechętnemu do wdrażania rozwiązań z obszaru security, umieściłbym na niej następujące punkty:

- Cyberatak jest bardzo kosztowny.
- Cyberatak zakłóca działanie firmy, powoduje przestoje, często uniemożliwia pracę, realizację zadań, kontraktów, wywiązywanie się z umów i zobowiązań.
- Wyciek czy naruszenie danych wpływa negatywnie na reputację firmy.
- Brak zabezpieczeń lub odpowiedniej reakcji na cyberatak obniża zaufanie kontrahentów, klientów i inwestorów do firmy.
- Utrata danych lub brak przygotowania na taki incydent mogą nieść ze sobą poważne konsekwencje prawne.
- Cyberprzestępcy mogą wykraść także informacje o patentach, opracowywanych przełomowych technologiach, własność intelektualną, która stanowi przewagę konkurencyjną przedsiębiorstwa.

Jak przekonać CEO, że cyberbezpieczeństwo jest ważne?

- Nowe modele pracy, w tym praca w zespołach rozproszonych, praca zdalna i hybrydowa będą zwiększać podatność firmy na cyberataki.
- Wdrożenie jakichkolwiek rozwiązań to za mało – najsłabszym ogniwem bezpieczeństwa jest człowiek, dlatego cyberbezpieczeństwo musi stać się programem, strategią, łączącą w sobie także uświadamianie i szkolenie pracowników.
- Wydatki na rozwiązania z zakresu cybersecurity można kontrolować, racjonalizować, a także rozkładać w czasie, dobierając narzędzia dopasowane do rzeczywistych potrzeb firmy – pod warunkiem, że współpracuje się z dostawcą, który chce te potrzeby zrozumieć.

Od cyberbezpieczeństwa nie da się dziś uciec. Każda firma, która pracuje w rozproszeniu i tworzy własność intelektualną, musi poświęcić temu zagadnieniu dużo uwagi. Dzięki współpracy z doświadczonymi doradcami można stworzyć długofalowe strategie, które uchronią firmy przed cyberatakami i ich – nie tylko finansowymi – skutkami.

PATRONAT
SECURITY MAGAZINE

KONFERENCJA
FORUM BEZPIECZEŃSTWA ORGANIZACJI W RZESZOWIE!

21 kwietnia odbędzie się pierwsza edycja konferencji Forum Bezpieczeństwa Organizacji organizowana przez e-nform we współpracy z renomowaną uczelnią wyższą WSPiA Rzeszowska Szkoła Wyższa oraz kancelarią Kozioł i Hady-Głowiak Radcowie Prawni.

Forum ma na celu przedstawienie różnych aspektów bezpieczeństwa organizacji oraz zaprezentowanie praktycznych aspektów, strategii i rozwiązań, które pomogą podmiotom osiągnąć swoje cele biznesowe w warunkach ciągłych zmian i wyzwań. W trakcie konferencji omówione zostaną kluczowe zagadnienia takie jak:

- ✔ bezpieczeństwo psychologiczne w firmie,
- ✔ różne oblicza bezpieczeństwa organizacji,
- ✔ biznesowy wywiad strategiczny,
- ✔ bezpieczeństwo informacji, w tym danych osobowych,
- ✔ cyberbezpieczeństwo,
- ✔ nowe wymagania KSH w zakresie oceny sytuacji spółki,
- ✔ zgłaszanie naruszeń i ochrona sygnalistów,
- ✔ zarządzanie kryzysowe.

Konferencja Forum Bezpieczeństwa Organizacji to świetna okazja, aby wysłuchać inspirujących prelekcji, zadać pytania ekspertom w panelach dyskusyjnych oraz wymienić się doświadczeniami i uwagami. Dodatkowo dla chętnych organizatorzy zaplanowali kolację z muzyką klasyczną na żywo.

W trakcie Forum będzie m.in. odbywała się degustacja aromatycznej włoskiej kawy przy ciekawostkach dotyczących tego napoju opowiadane przez Zbigniewa Chlebowskiego.

Dzięki zaangażowaniu firmy Celius będzie można zapoznać się z praktycznym działaniem aplikacji do zarządzania kryzysowego z użyciem profesjonalnych urządzeń końcowych.

ZAPISZ SIĘ!

FORUM BEZPIECZEŃSTWA ORGANIZACJI

KONFERENCJA DLA BIZNESU

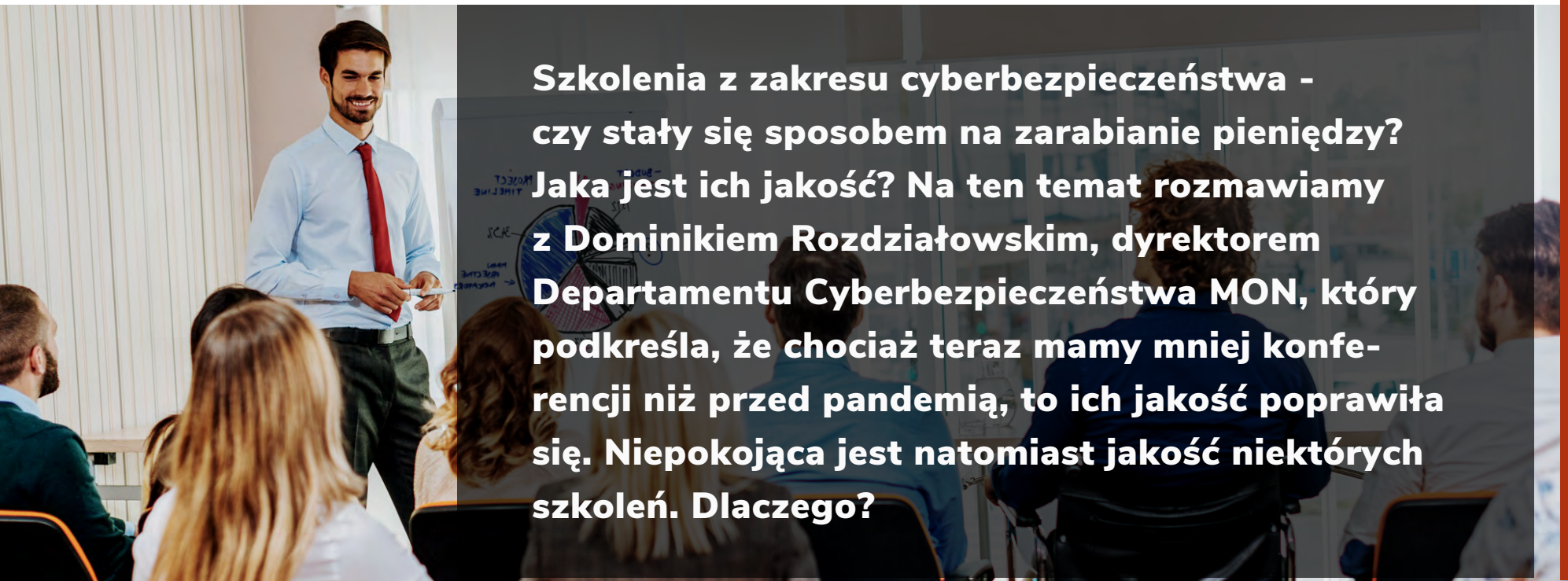
21 kwietnia **2023 r.**

Spotkajmy się w **Rzeszowie!**

WSPiA Rzeszowska Szkoła Wyższa

CZY SZKOLENIA DOTYCZĄCE CYBERSECURITY STAŁY SIĘ SPOSOBEM NA BIZNES?

Dominik Rozdziałowski
Departament Cyberbezpieczeństwa MON



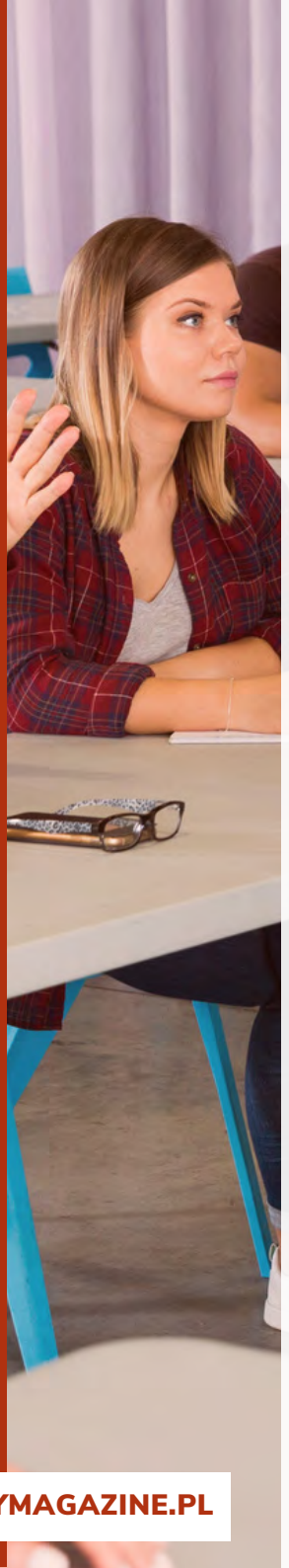
Szkolenia z zakresu cyberbezpieczeństwa - czy stały się sposobem na zarabianie pieniędzy? Jaka jest ich jakość? Na ten temat rozmawiamy z Dominikiem Rozdziałowskim, dyrektorem Departamentu Cyberbezpieczeństwa MON, który podkreśla, że chociaż teraz mamy mniej konferencji niż przed pandemią, to ich jakość poprawiła się. Niepokojąca jest natomiast jakość niektórych szkoleń. Dlaczego?

Czy zauważa Pan wzrost liczby firm oferujących szkolenia i konferencje dotyczące cyberbezpieczeństwa?

Dominik Rozdziałowski: Porównując obecny czas z okresem przed pandemią, konferencji jest wręcz mniej. Natomiast zostało bardzo dużo tych dobrych, w których chcieliśmy znowu uczestniczyć. Słabsze wypadły.

Jeśli chodzi o jakość szkoleń, to jestem przerażony. Od lat wykładam na uczelniach, uczestniczę w konferencjach, więc znam ten świat. A wystarczy, że otworzy się YouTube czy Tik Toka i dowiemy się, jak łatwo zostać programistą. Ostatnio widziałem reklamę: „nie znasz angielskiego, nie umiesz matematyki, nie masz ukończonych studiów, zostań specjalistą cyberbezpieczeństwa! To banalnie proste". My robimy to kilkanaście lat i nikt z nas specjalistą się nie czuje. Ciągle się dokształcamy. Praca w reklamach przedstawiana jest jako miła, przyjemna. Ostatnio przeczytałem informację, że programiści to jeden z najspokojniejszych zawodów świata. Są chyba na drugim miejscu. Nie jestem przekonany, że tak jest, bo, przykładowo, nasi pracownicy mają pracy bardzo dużo.

Jeśli ktoś uważa, że jest specjalistą po pięciu tygodniach, czy miesiącach szkolenia, to tak to nie działa. Jest to zwyczajne wyciąganie pieniędzy. Moim zdaniem, lepiej znaleźć profesjonalne szkolenie, wartościowe studia podyplomowe, żeby zobaczyć, czy to jest dla nas. Można w czasie takich studiów zdobyć podstawy, a dopiero później nadal się szkolić i praktykować.



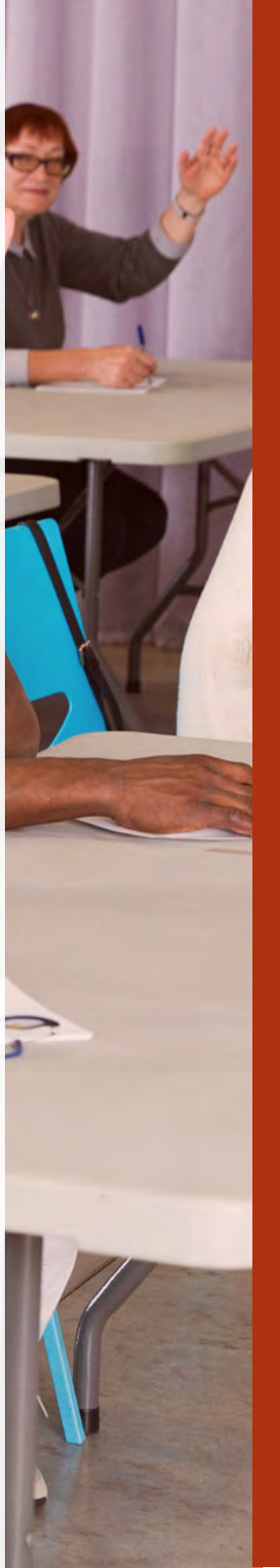
Ministerstwo Obrony Narodowej nadzoruje uczelnie, które doskonale przygotowują do zawodu i służby. To przykładowo, Wojskowa Akademia Techniczna. Jej absolwenci mają dużą wiedzę na temat cyberbezpieczeństwa i programowania, ale trzeba jeszcze lat służby i nauki w praktyce, by zostać specjalistami.

Przychodząc do pracy w Ministerstwie Obrony Narodowej, pierwsze trzy miesiące spędziłem na intensywnym nadrabianiu zaległości, bym mógł, oprócz zarządzania, porozmawiać z pracownikami na tematy technicznie. Pracuję z ludźmi, którzy naprawdę służą, zajmują się tą tematyką cyber w armii od wielu lat i są ekspertami, specjalistami.

Jakie, według Pana, są najważniejsze czynniki, na które warto w ogóle zwrócić uwagę podczas wyboru szkolenia, czy konferencji z dziedziny cyberbezpieczeństwa?

D. R.: Zróbmy samodzielnie rozpoznanie, czyli poczytajmy o miejscu czy kursie. Nie decydujmy się na nie tylko dlatego, że jest reklama na YouTube czy TikToku. Widziałem świetną reklamę jednej z największych w Polsce, renomowanych uczelni. Uważam, że długa, profesjonalna reklama kursu odbywającego się na dużej uczelni, która konkretnie mówi, jakie umiejętności czysto techniczne zdobędziemy, do czego się przyda ta wiedza, w jakim kierunku nas rozwinie - to jest fajny pomysł. Idziemy na taki kurs i on na pokazuje, czy w ogóle jest to dla nas.

Przejrzyjmy informacje o tym, kto oferuje szkolenie, czy to jest renomowana firma, czy jest znana na rynku - takich firm czy uczelni jest mnóstwo. Unikajmy ofert czy reklam firm, zapewniających, że w pięć tygodni zostaniemy informatykiem, programistą, specjalistą w cyberbezpieczeństwa, w dodatku nagrywanych kamerą telefonu, z przekazem, że są to lekkie i przyjemne zawody.



Napiszmy pytanie na forum, przykładowo może być to prowadzone przez Polskie Towarzystwo Informatyczne. Zapytajmy, jaką wybrać uczelnię na początek. Można też zadzwonić do Ministerstwa Obrony Narodowej.

W jaki sposób, według Pana, oceniać wartość w kontekście kosztów takich szkoleń, konferencji?

D. R.: Jeżeli chodzi o szkolenia, to warto brać pod uwagę firmę lub osobę, która będzie trenerem. Sprawdźmy, czy to jest znana firma, renomowana uczelnia. Pamiętajmy, że inaczej będzie wyglądać cena szkolenia lub konferencji w Warszawie, Krakowie, czy Katowicach na największych uczelniach, a inaczej w mniejszych ośrodkach, jak Kielce czy Rzeszów. W mniejszych ośrodkach na pewno jest taniej, ale poziom jest równie wysoki.

Wybierając prywatne szkolenia, kierowałbym się zdaniem innych specjalistów. Dobre rozeznanie jest potrzebne, ponieważ czasami fajne szkolenia są niedrogie i organizowane przez naprawdę duże firmy. Pamiętajmy o tym, że te firmy też szukają specjalistów, osób, które mogą finalnie trafić do nich do pracy. Z tego powodu wcale nie muszą zarobić wielkich pieniędzy na tym szkoleniu.

Natomiast, jeśli chodzi o uczestnictwo w konferencjach, uważam, że te największe w Polsce konferencje są w naprawdę świetnych cenach. Sprawdzajmy ich opinie. Wystarczy po prostu sprawdzić w Google. Opinie innych osób na LinkedIn, Facebooku i innych portalach także są cennym źródłem wiedzy.

A jakie kroki podejmuje Ministerstwo Obrony Narodowej, by zapewnić wysoką jakość szkoleń i konferencji właśnie dla swoich pracowników w dziedzinie cyberbezpieczeństwa?

D. R.: Jako Ministerstwo Obrony Narodowej nadzorujemy merytorycznie kilka uczelni, między innymi Wojskową Akademię Techniczną, Akademię Marynarki Wojennej, Akademię Wojsk Lądowych. Na każdej z tych uczelni mamy kierunki związane cyberbezpieczeństwem. Jest to zarówno typowe cyberbezpieczeństwo, ale i informatyka.
Specjaliści związani z uczelniami często organizują konferencje. Zapraszają na nie wybitnych gości całego świata. Najbliższa będzie w kwietniu w Akademii Sztuki Wojennej. Dlatego mamy bardzo łatwy dostęp do szkoleń. Ponadto nasze kierownictwo już dawno zdecydowało, że wojsko musi się rozwijać, szkolić. Oprócz tych organizowanych przez nas szkoleń, mamy szereg programów, które realizuje-

my. Bierzemy udział w konferencjach zewnętrznych. Jesteśmy gośćmi w naprawdę największych konferencji, pracownicy mojego departamentu sami decydują, w której konferencji chcą uczestniczyć.

Warto pamiętać, że umiejętności cyber są jednymi z kilku potrzebnych w pracy w Ministerstwie Obrony Narodowej. Trwa konflikt wojenny Rosji z Ukrainą i stale pracujemy nad rozwijaniem współpracy z zagranicą, korzystanie z najlepszych wzorców i uczymy się od najlepszych. Chętnie korzystamy z umiejętności oraz wiedzy kolegów z innych krajów oraz ze świata biznesu.

Pozostając przy temacie świata biznesu, ale także organizacji pozarządowych, instytucji niekoniecznie związanych z obroną narodową. Czy firmy powinny inwestować w wydarzenia z dziedziny cyberbezpieczeństwa? Jakie mogą mieć z tego korzyści?

D. R.: Jeśli któraś firma jeszcze nie inwestuje w szkolenia swoich pracowników z cyberbezpieczeństwa, to byłoby to dla mnie zaskoczenie. Bardzo mocno namawiam właścicieli firm i kierownictwo do tego, by to zmieniło. Pamiętajmy, że bezpieczeństwo organizacji zaczyna się tam, gdzie są nasi pracownicy. W każdym miejscu, do którego jeżdżą, nasza firma musi być bezpieczna. Praca na odległość jest wygodą, ale niesie także niebezpieczeństwa. Dlatego często nie dostrzegamy wielu korzyści oraz strat, które zostałyby wygenerowane, gdyby nie zabezpieczenia.

Wystarczy przez miesiąc, rok nie aktualizować oprogramowania Windows, programu antywirusowego. Momentalnie zauważymy problemy,

które pojawią się niemalże od razu. Dlatego ważne jest korzystanie ze szkoleń, ale nie tylko szkoleń pracowników zajmujących się obsługą strony www, czy sieci.

Pamiętajmy, że wszyscy korzystamy z elektroniki w firmie: z internatu, z różnych sprzętów, między innymi smartfonów. Ostatnio jest mnóstwo dyskusji, czy na urządzeniach prywatnych pracownicy powinni sprawdzać służbową pocztę, logować się do firmowych aplikacji.

Pracodawcy muszą inwestować w nas, pracowników i naszą wiedzę, umiejętności. To jest bardzo ważne, zarówno w kontekście bezpieczeństwa dużej organizacji, jak i małej jednoosobowej firmy.

Ponadto należy sobie ustalić zasady, spisać politykę bezpieczeństwa i tych ustalonych zasad bezwzględnie się trzymać. Trzeba pamiętać, aby cyklicznie zrobić jej przegląd. Czasami należy ją udoskonalić, zmienić. Być może będzie ją trzeba trochę złagodzić, bo często na początku trochę przesadzamy z restrykcjami.

Na koniec wrócę do edukacji. Czy istnieją alternatywne metody podnoszenia wiedzy o cyberbezpieczeństwie, które są równie skuteczne jak tradycyjne szkolenia czy konferencje? Jeśli tak, to jakie to są sposoby? Gdzie można taki informacji szukać?

D. R.: Polecam w szczególności samokształcenie. Wystarczy skorzystać z wybranej wyszukiwarki, bardzo merytoryczną wiedzę można znaleźć bardzo łatwo. Na YouTube są filmiki znanych osób. Można korzystać z materiałów ogólnie dostępnych, można wziąć udział w konkursach wiedzy o cyberbezpieczeń-

stwie o różnych poziomach. Organizuje je m.in. Ministerstwo Obrony Narodowej i inne ministerstwa.

Konkursy są naprawdę o różnych poziomach trudności, w finałach możemy spotkać osoby, z którymi porozmawiamy, które pokażą nam, w jaki sposób coś wykonać, zaprezentują błędy.

Zachęcam także do korzystania ze stron internetowych dużych firm. Tam też jest mnóstwo informacji o cyberbezpieczeństwie i jego zasadach. Warto śledzić największe portale internetowe związane z tym tematem.

Polecamy więc śledzić popularne i sprawdzone serwisy poświęcone cyberbezpieczeństwu, ale także lekturę "Security Magazine". Dziękujemy Panu za rozmowę i porady dotyczące weryfikacji szkoleń i konferencji.

Rozmawiała:
Anna Petynia-Kawa

PATRONAT
SECURITY MAGAZINE

DRUGA EDYCJA
CYBERTEK TECH FESTIVAL

DOŁĄCZ DO NAS
I ENJOY THE CYBER!

CyberTek Tech Festival to II edycja profesjonalnego, międzynarodowego, wyjątkowego wydarzenia budującego społeczność specjalistów w zakresie cyberbezpieczeństwa sieci przemysłowych. Tegoroczna konferencja odbędzie się pod hasłem: ENJOY THE CYBER.

Wymieniaj doświadczenia, dyskutuj o dobrych praktykach w doborowym towarzystwie i atmosferze sprzyjającej kreatywności oraz nawiązywaniu znajomości, które zaprocentują.

CyberTek Tech Festival jest w całości poświęcony cyberbezpieczeństwu systemów przemysłowych, natomiast jego nadrzędnym celem jest upowszechnianie wiedzy i budowanie partnerstwa wokół idei „Ekosystemu cyberbezpieczeństwa", która propaguje pryncypia współpracy na rzecz cyberbezpiecznego przemysłu, w tym kontekście wdrażania w życie Ustawy o KSC.

Wydarzenie kierowane jest przede wszystkim do osób, na których spoczywa odpowiedzialność za stworzenie, skuteczne wdrożenie lub realizację programów bezpieczeństwa obejmujących sieci i systemy przemysłowe.

To konferencja tworzona dla ekspertów przez ekspertów w dziedzinie cyberbezpieczeństwa.

Tematyka poruszana podczas konferencji:

- Red Team, Pentesty, Offensive Security w OT
- Blue Team (GRA, branżowe scenariusze)
- Incident Response, Security Operations Center (SOC), Security, Orchestration and Automation (SOAR) dla OT
- Specyfika Digital Forensics/Incident Response dla elementów systemów automatyki (PLC, HMI)
- Śledzenie zagrożeń w OT, szacowanie ryzyka i ciągłość działania
- Zapewnienie zgodności, Audyt Cyber w OT, KSC, NIS2, IEC62443
- Nadzór i zarządzanie bezpieczeństwem OT/IT; Cyberprogram w firmie
- Architektura i narzędzia (cyber)bezpieczeństwa w OT
- Monitorowanie OT; #SBOM
- Dostęp zdalny
- Historie i wpadki z obszaru bezpieczeństwa IT/OT, doświadczenia z wdrożeń
- Trendy i technologie, zmieniające sieci przemysłowe, czyli jak na paradygmaty cyber w OT wpływają: chmura, 5G, IoT
- Zero Trust vs. IoT
- Software Defined Network (SDN) w ICS
- Migracja z SDH – MPLS-TP
- i wiele innych.

CyberTek Tech Festival

Muzeum Śląskie, Katowice

24-26.05.2023

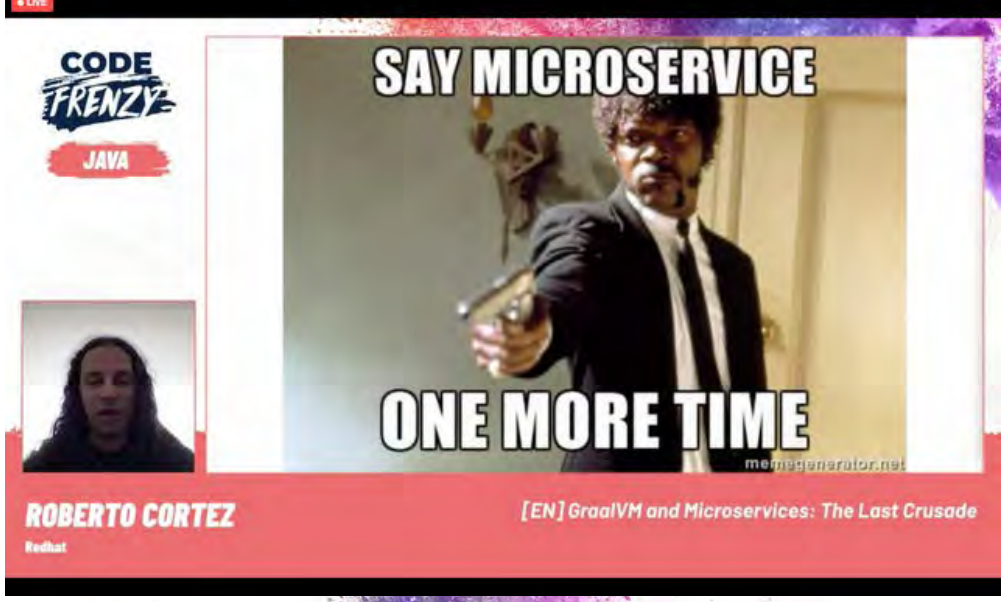
10% ZNIŻKI DLA NASZYCH CZYTELNIKÓW

Skontaktuj się z organizatorem mailowo, aby otrzymać rabat: konferencja@cybertek.com.pl

Szczegóły s. 16

900 UCZESTNIKÓW. 4 PANELE DYSKUSYJNE, 35 WYKŁADÓW. CODEFRENZY ZA NAMI

PATRONAT
SECURITY MAGAZINE



Pierwsza edycja wirtualnej konferencji CodeFrenzy przeszła już do historii. To interdyscyplinarne wydarzenie, poświęcone najciekawszym tematom ze świata IT, zgromadziło niemal 900 osób.

W trakcie 5 intensywnych dni streamingu odbyły się 4 panele dyskusyjne oraz 35 wykładów z wiodącymi specjalistami między innymi z zakresu ICT, cyberbezpieczeństwa, DevOps czy Javy. Największą oglądalnością cieszyła się ścieżka Security, choć w innych dniach uczestnicy aktywnie uczestniczyli w prezentacjach.

Nadszedł jednak moment, by wyjść ze sfery online i rozpocząć sezon spotkań na żywo. Wszystkie osoby, które są zainteresowane zagadnieniami prezentowanymi podczas CodeFrenzy, mogą teraz pogłębić swoją wiedzę oraz wziąć udział w stacjonarnych wydarzeniach.

PRZED NAMI

4Developers - interdyscyplinarny Festiwal IT (18 kwietnia 2023),

PLNOG 31 - konferencja branży ICT i telkom (15-16 maja 2023),

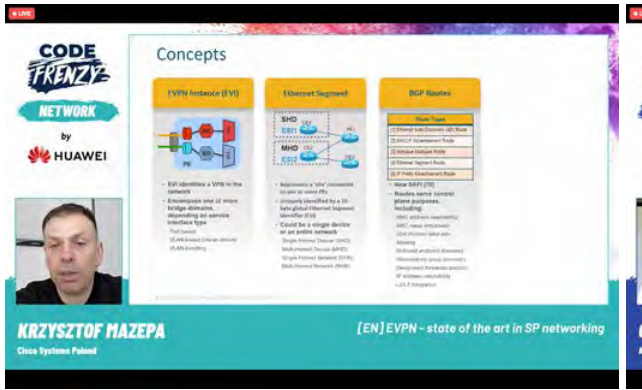
CONFidence - międzynarodowa konferencja cybersecurity (5-6 czerwca 2023),

HackYeah - największy hackathon w Europie (30 września - 1 października 2023),

JDD - konferencja dla miłośników języka Java (24-25 października 2023).

Dlaczego warto wziąć udział w konferencji offline? Oprócz dużej dawki aktualnej wiedzy w wybranym przez siebie zakresie, jest to również okazja na bardziej bezpośrednią wymianę doświadczeń i nawiązanie wartościowych kontaktów w branży.

Warto się zarejestrować i przekonać na własnej skórze, dlaczego mimo przemian w branży IT konferencje stacjonarne wciąż są niezwykle popularne.



PRACOWNIK OCHRONY - KONIECZNOŚĆ CZY RELIKT PRZESZŁOŚCI?

Tomasz Grzelak
Stay Safe Poland

Pracownicy ochrony obecni są w wielu miejscach - od instytucji publicznych po prywatne przedsiębiorstwa. Często pojawiają się na pierwszej linii w przypadku zagrożenia. Czy ich praca jest potrzebna w dzisiejszych czasach? Czy jest to zawód, który wymiera, czy może ma przed sobą jeszcze przyszłość?

Podczas gdy na całym świecie branża ochrony ma nawet 100-letnią tradycję, w Polsce do 1989 roku ochrona komercyjna praktycznie nie istniała. Zmiany ustrojowe odwróciły sytuację. Właśnie wtedy pojawiły się firmy świadczące usługi ochrony, lecz dopiero Ustawa o ochronie osób i mienia (Dz.U. nr 114, poz. 740 z późn. zm.) uchwalona 22 sierpnia 1997 roku była pierwszym aktem prawnym rzetelnie regulującym funkcjonowanie podmiotów zajmujących się bezpieczeństwem. Niestety, rynek w Polsce jest dość mocno rozdrobniony, z tysiącami wydanych licencji przez co agencje ochrony często walczą o przetrwanie. To z pewnością nie wpływa pozytywnie na jakość świadczonych usług. Ale czy wina leży tylko po stronie usługodawcy? Czy usługobiorcy, dla których często głównym kryterium wyboru jest stawka za roboczogodzinę, nie są również winni obecnej sytuacji w Polsce?

PRACOWNIK OCHRONY, CZYLI KTO?

Praca w branży ochrony od lat budzi skrajne emocje. Z jednej strony są to ludzie, którzy mają za zadanie zapewnić bezpieczeństwo i ochronę innych, z drugiej zaś bywają traktowani z góry, jako osoby o niskich kwalifikacjach. Czy słusznie?

Pracownik ochrony to nie tylko osoby w mundurach, którzy pilnują wejścia do budynków. To

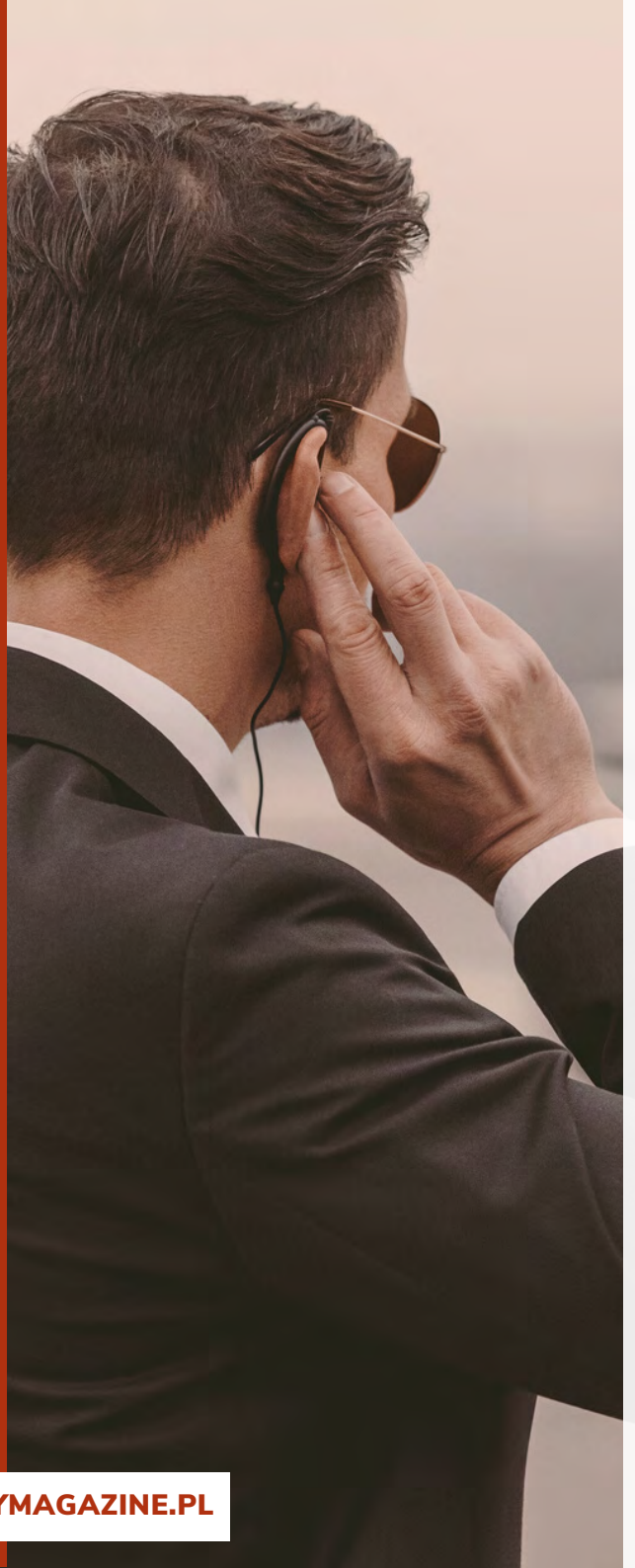
także ludzie, którzy pracują w sklepach, marketach, bankach, magazynach, firmach, hotelach czy na imprezach masowych. Wszędzie tam, gdzie istnieje ryzyko zagrożenia dla życia, zdrowia lub mienia. Ich zadaniem jest nie tylko zapewnienie bezpieczeństwa, ale i reagowanie na niebezpieczeństwo, udzielanie pierwszej pomocy czy prowadzenie ewakuacji. Praca pracownika ochrony wymaga nie tylko odpowiednich predyspozycji, ale i wiedzy oraz umiejętności.

Przede wszystkim powinien być to człowiek, który cieszy się zaufaniem innych, jest wytrwały, skoncentrowany, spostrzegawczy, cierpliwy i zdecydowany. Ważne są także umiejętności interpersonalne, komunikacyjne oraz negocjacyjne. Powinien posiadać nie tylko odpowiednie uprawnienia, ale i doświadczenie oraz odpowiednie szkolenia. Znajomość przepisów prawa dotyczących ochrony osób i mienia, znajomość zasad udzielania pierwszej pomocy, radzenia sobie w sytuacjach kryzysowych oraz korzystania z różnych środków technicznych, takich jak monitoring czy systemy alarmowe to również przydatne umiejętności w tej branży. Czy mamy takich pracowników? Nie zawsze...

SYTUACJA W POLSCE

Niskie płace, niejasne formy zatrudnienia, przypadkowo zatrudniane osoby tylko po to, by wywiązywać się z podpisanych umów. Ponadto praca w ciasnych, dusznych pomieszczeniach, 24 godziny na dobę 7 dni w tygodniu wraz z częstymi czynnościami pobocznymi, takimi jak odśnieżanie, zamiatanie chodników i koszenie trawników. Między innymi te rzeczy spowodowały, iż wizerunek branży ochrony w Polsce nie jest zbyt korzystny. Czy można się dziwić, iż ludzie, mogący wnieść jakieś umiejętności lub wartość do firmy, nie byli specjalnie zainteresowani taką posadą?

Swoje zrobiły również braki kadrowe. Ze względu na spadające bezrobocie i migracje zarobkowe, agencje ochrony borykają się z poważnymi problemami kadrowymi z wykwalifikowanymi, jak i niewykwalifikowanymi pracownikami. Niedobory kadrowe są szczególnie widoczne w okresie wakacyjnym, kiedy wzrasta zapotrzebowanie na osoby pracujące w kurortach turystycznych lub do ochrony dużych imprez masowych. Co możemy zatem z tym zrobić?



POTRZEBNE ZMIANY

Obecnie w branży bezpieczeństwa zatrudnionych jest około 250 000 pracowników. Na szczęście, rozwój gospodarczy kraju, zmiany legislacyjne oraz wprowadzenie nowych standardów pracy doprowadziły do widocznych i pozytywnych zmian również w branży ochrony.

Aby przyciągnąć nowych pracowników, firmy tworzą atrakcyjne oferty pracy, proponując kandydatom nie tylko wynagrodzenie, ale również np. pakiety ubezpieczeń, opiekę medyczną czy zajęcia sportowe. Pracownicy wreszcie nie są zatrudniani na „śmieciowych" umowach, a standardowych o pracę z przysługującym urlopem i zwolnieniem lekarskim. Płace rosną również z powodu zwiększonej konkurencji oraz „kradzieży" pracowników przez inne sektory, takie jak budownictwo i transport.

Część agencji skierowała się w stronę specjalizacji, tworząc nowe stanowiska pracy, takie jak agenci ochrony z większym zakresem zadań czy operatorzy monitoringu wizyjnego mający odpowiednie predyspozycje do takiej pracy.

Klienci również się zmienili. Przedsiębiorstwa mające własne standardy pracy dla swoich pracowników, niejako wymuszają na agencjach ochrony podobnego podejścia do swoich. Oczywiście, nadal dużym problemem jest cena usług powodująca, iż negocjacje między obiema stronami są coraz trudniejsze i po części przyczyniają się do ograniczania korzystania z ochrony fizycznej na rzecz usług zdalnych opartych na rozwiązaniach technicznych. To ciekawy kierunek, któremu warto przyjrzeć się bliżej.

ZABEZPIECZENIA TECHNICZNE

Bezpieczeństwo techniczne pojawiło się dość szybko wraz z rozwojem usług ochrony. Początkowo ze względu na wysoką cenę były to bardzo ograniczone systemy antywłamaniowe i napadowe, a analogowe systemy monitoringu wizyjnego oraz kontroli dostępu były rzadkością. Mimo to, gdy były używane prawidłowo, dodawały wartości systemom bezpieczeństwa.

Ostatnimi laty nastąpiła wyraźna zmiana. Branża systemów zabezpieczeń technicznych rozwija się szybko i dynamicznie. Systemy alarmowe, kontroli dostępu czy CCTV są już praktycznie standardem w większości przedsiębiorstw. Okres pandemii dodatkowo przyśpieszył ten proces, powodując wprowadzenie na rynek nowych rozwiązań i stopniowe zastępowanie pracowników ochrony w pewnych obszarach. Dzięki wykorzystaniu zaawansowanych systemów monitoringu, analizy obrazu czy sztucznej inteligencji, procesy ochronne mogą być znacznie bardziej efektywne i dokładne. Na przykład, systemy monitoringu z wykorzystaniem sztucznej inteligencji są w stanie automatycznie analizować obrazy i wykrywać niebezpieczne sytuacje, takie jak włamania czy nielegalne przekroczenie granicy. Systemy te wykorzystują zaawansowane algorytmy które pozwalają na rozpoznanie obiektów oraz sytuacji, a następnie podejmowanie odpowiednich działań takich jak alarmowanie pracowników ochrony czy wysłanie powiadomienia do służb odpowiedzialnych za bezpieczeństwo.

Biorąc pod uwagę spadające ceny nowych technologii, ich szerokie zastosowanie oraz rosnące koszty pracy spodziewam się kontynuacji tendencji szerokiego wdrażania usług zdalnych. Ale bez dobrze wyszkolonej i zrekrutowanej kadry nowa technologia jest bezużyteczna. W końcu to człowiek w sytuacji kryzysowej musi ocenić sytuację, przeanalizować wszystkie informacje i często podjąć decyzje które

mogą decydować o czyimś zdrowiu lub życiu. Wymaga to zatrudniania operatorów monitoringu wizyjnego potrafiących obsługiwać wiele obiektów jednocześnie, mających dobry wzrok, koncentrację, potrafiących łączyć fakty.

Nowoczesna technologia to także szansa na przyciągnięcie młodych ludzi, chcących realizować swoje ambicje zawodowe w dziedzinach związanych z inteligentnymi urządzeniami.

ZWIĘKSZENIE KOMPETENCJI PRACOWNIKÓW OCHRONY

Jednym z kluczowych aspektów zwiększenia kompetencji pracowników ochrony jest odpowiednie szkolenie. Szkolenia powinny obejmować różne zagadnienia z zakresu ochrony osób i mienia, takie jak techniki interwencyjne, obsługa sprzętu ochronnego, zasady działań w sytuacjach kryzysowych, prawo ochrony osób i mienia oraz psychologia. Ważne jest również, aby szkolenia były regularnie odnawiane i uaktualniane, aby pracownicy ochrony byli na bieżąco z najnowszymi trendami i technologiami w branży ochrony.

Kolejnym ważnym aspektem zwiększenia kompetencji pracowników ochrony jest selekcja odpowiednich kandydatów.

Pracownicy ochrony powinni mieć odpowiednie cechy osobowościowe, takie jak spokój, umiejętność radzenia sobie w sytuacjach stresowych, skrupulatność oraz uczciwość. Ważne jest również, aby mieli oni odpowiednie kwalifikacje oraz doświadczenie w dziedzinie ochrony osób i mienia.

Podsumowując, pracownik ochrony był, jest i nadal będzie potrzebny. Bezpieczeństwo jest bowiem priorytetem dla każdej osoby, firmy czy kraju. Niemniej jednak, praca pracownika ochrony musi się zmieniać i dostosowywać do zmieniających się warunków. Pracownicy muszą być lepiej wykwalifikowani, a ich praca powinna być bardziej ukierunkowana.

Branża ochrony powinna też inwestować w rozwój pracowników, zapewniając dedykowane szkolenia oraz kursy. Odpowiednio przeszkolony pracownik w połączeniu z narzędziami, jakie dają nowe technologie w obiektach to obecnie najlepsze połączenie. I takie hybrydowe modele w najbliższym czasie powinny być rozwijane w branży.

PATRONAT
SECURITY MAGAZINE

Bilety PRESALE 40% taniej od ceny ostatecznej!

CYBERSEC FORUM/EXPO 2023 to kluczowe i jedyne w swoim rodzaju wydarzenie dotyczące cyberbezpieczeństwa w Europie. Od 2015 roku CYBERSEC zapewnia przestrzeń do wymiany poglądów, dyskusji i prezentacji dotyczących największych wyzwań stojących nie tylko przed społeczeństwem, ale i światem wirtualnym.
CYBERSEC to nie tylko FORUM – to również jedna z największych przestrzeni EXPO, która stwarza możliwość do rozwijania kontaktów biznesowych kluczowym przedsiębiorcom z Polski i całego świata, a także jest szansą na zaprezentowanie swoich innowacyjnych produktów i usług.

17. edycja CYBERSEC FORUM/EXPO odbędzie się pod hasłem przewodnim PARTNERSHIPS FOR CYBER RESILIENCE. To kontynuacja zeszłorocznych rozważań na temat działania w jedności w celu zachowania cyberbezpieczeństwa oraz skupienia się na budowaniu cyberodporności - niezwykle kluczowej w czasach niepokoju i niepewności, w jakich przyszło nam funkcjonować.

Cyberbezpieczeństwo to temat złożony i powinien być analizowany z różnych perspektyw. Dlatego dyskusje będą odbywały się ramach 5 unikalnych ścieżek tematycznych:

- STATE,
- DEFENCE,
- BUSINESS,
- STREAM
- EU POLICY FORESIGHT.

Sprawdź agendę wydarzenia!

Bezpłatne bilety

Organizator przewidział ograniczoną pulę darmowych biletów STANDARD dla: studentów, sektora naukowego, administracji publicznej, jednostek samorządu terytorialnego, organizacji pozarządowych oraz administracji wojskowej!

JAK DOBRAĆ SKUTECZNE ZABEZPIECZENIE?

Katarzyna Bieńkowska
Silny&Salamon

Sprawna logistyka oznacza pewny łańcuch dostaw i elastyczne procesy, w których łączone są technologicznie zaawansowane rozwiązania z klasycznymi. Właściwe zabezpieczenia podnoszą bezpieczeństwo i optymalizują operacje w firmach, co ma bezpośredni wpływ na obsługę klientów. Pomocnym narzędziem dla branży jest pierwszy na rynku bezpłatny "Poradnik 2023 - Jak dobrać skuteczne zabezpieczenie" przygotowany przez ekspertów z Silny&Salamon, który pozwoli świadomie przeanalizować potrzeby i dobrać właściwe rozwiązanie dla firmy.

Specjaliści zajmujący się bezpieczeństwem i logistyką biorą pod uwagę wiele aspektów m.in: procesy zachodzące w firmach, ergonomię, czy troskę o zrównoważony rozwój. Dlatego dostępność szerokiego wachlarza zabezpieczeń plombowych, sprawia, że decyzja o doborze odpowiednich nie jest łatwa. Stąd wiedza na temat charakterystyk i funkcjonalności poszczególnych zabezpieczeń, a także specyficznych potrzeb różnych branż, stanowi solidne wsparcie dla osób zajmujących się bezpieczeństwem.

Dlatego postanowiliśmy zebrać informacje bazujące na naszym ponad 30-letnim doświadczeniu w obszarze zabezpieczania łańcucha dostaw w zwarty i przejrzyście zaprojektowany materiał pt. „Poradnik 2023 – Jak dobrać skuteczne zabezpieczenie". Chcemy w ten sposób ułatwić dobór dopasowanych do potrzeb zabezpieczeń, które odgrywają ważną rolę w łańcuchu dostaw. Dodatkowo, dokonaliśmy segmentacji według branż i rodzajów produktów, przytoczyliśmy też przykłady wdrożeń. Mam nadzieję, że ten materiał ułatwi odnalezienie się w konkretnej sytuacji biznesowej.

ZADAJ SOBIE 5 PYTAŃ

Poznanie odpowiedzi na 5 kluczowych pytań zadanych w poradniku, pozwoli na świadomą analizę potrzeb i dobór optymalnych rozwiązań.

Jak dobrać skuteczne zabezpieczenie?

Podstawowe pytanie odnosi się do funkcji plomby, czy ma spełniać tylko funkcję zabezpieczającą, czy też informacyjną. Ta pierwsza chroni przed kradzieżą, przemytem, nieuprawnionym wejściem, naruszeniem czy zabrudzeniem zawartości. Z kolei druga niesie dodatkowe informacje umieszczone bezpośrednio na niej.

Kluczowe z punktu widzenia doboru rozwiązania, jest to, gdzie i co plomba ma zabezpieczać. Może chronić dostęp do opakowań typu worek, pojemnik, beczka, karton, ale też pomieszczeń, środków transportu, czy liczników, dlatego też od konkretnego zastosowania zależy kształt i długość operacyjna plomby.

Równie ważne jest to, czy plomba ma być jedno czy wielorazowego użytku. W związku z tym, że idea plombowania polega na tym, aby po otwarciu zabezpieczenia ślady manipulacji były widoczne, nie można więc było ponownie użyć plomby, większość z nich jest jednorazowa. Warto jednak wiedzieć, że zaawansowane technologicznie plomby mają więcej funkcji, są też droższe i wykorzystuje się w nich mechanizmy umożliwiające wielokrotne użycie. W tego typu zabezpieczeniach nie tylko fizyczne uszkodzenie jest oznaką naruszenia, ale też wysyłany w czasie rzeczywistym sygnał.

Kolejna kwestia do rozważenia to rodzaj materiału z jakiego wykonana jest plomba. Plomby mogą być zrobione z różnych tworzyw, jednorodnych lub kombinacji kilku, a tym samym posiadać odmienne właściwości, być twardsze lub bardziej elastyczne oraz charakteryzować się określoną wytrzymałością. W zależności od indywidualnych oczekiwań klienta i procesów logistycznych w danej firmie, każdy z tych czynników odgrywa swoją rolę.

Ostatnie pytanie, które warto zadać przed doborem rozwiązania, dotyczy obowiązującego systemu oznaczeń w firmie. W związku z tym, że najważniejszą cechą plomby jest jej unikatowość, kluczowe jest zdefiniowanie sposobu jej nadania. Może być to indywidualny numer w postaci sekwencji liczb lub kodu kreskowego, a dodatkowo kolor czy doda-

tkowy nadruk w postaci logo lub nazwy.

TECHNOLOGIA, OSZCZĘDNOŚCI I ELASTYCZNOŚĆ DZIAŁANIA

Odpowiedzi na pięć pytań, przez które prowadzi poradnik, ułatwią dobranie właściwych zabezpieczeń plombowych, co wraz z wyborem sprawdzonego dostawcy, pozwoli zadbać o oszczędności i elastyczność.

Odpowiednie oznaczanie, pakowanie i przekazanie towarów do środka transportu zabezpieczonego plombą zapewnia, że nienaruszony ładunek dotrze do miejsca docelowego. Pomagają w tym zaawansowane zabezpieczenia, działające w ramach systemów RFID, które usprawniają też procesy zarządzania towarami w magazynie i są wsparciem dla procesu pickingu, ale także klasyczne plomby, jak i etykiety bazowe umieszczane na pojemnikach wielorazowego użytku.

Poza sprawnymi procesami logistycznymi, oszczędności można odnaleźć również w precyzyjnie zamodelowanych powierzchniach magazynowych uwzględniających ekologiczne i energooszczędne rozwiązania, ale też inwestycje w technologie, a więc automatyzację oraz cyfryzację procesów. Oszczędności przynosi też wcześniejsze planowanie zamówień, gdyż dłuższa perspektywa i większe ilości dają pewność dostępności produktów po dotychczasowych cenach oraz pozwalają otrzymać lepsze warunki handlowe.

Bliskie jest nam myślenie, że inwestycje w perspektywie czasowej to

oszczędności. Inwestycje w technologie i zabezpieczenia plombowe pozwalają chronić towary i zawczasu zapobiec stratom i uszkodzeniom. To również współpraca ze sprawdzonym partnerem, który obok atrakcyjnej oferty cenowej, gwarantuje brak dodatkowych kosztów i pewność dostaw na czas. Nasi klienci wiedzą, że mogą polegać na nas w każdych warunkach, a szybkość w działaniu dzięki niezbędnej infrastrukturze i własnej drukarni, jest naszą przewagą.

WIEDZA DOSTĘPNA OD RĘKI

Złożoność procesów logistycznych i mnogość wyzwań, z jakimi mierzą się specjaliści od logistyki, sprawia, że usystematyzowany materiał w formie przejrzystego dokumentu, dostępny bezpłatnie, może być użytecznym narzędziem, które pozwoli dobrać optymalne rozwiązanie i zaoszczędzić czas.

Zachęcam do kontaktu z Dagmarą Puścikowską, by otrzymać nieodpłatnie testowy zestaw plomb oraz sprawdzić ich wytrzymałość w realnych warunkach.

Dodatkowo, by osobiście porozmawiać o doborze zabezpieczeń plombowych z zespołem Silny&Salamon, zapraszam na Międzynarodowe Targi Transportu, Spedycji i Logistyki, które odbędą się 4-6 kwietnia w Ptak Warsaw Expo na stoisko C317a. To także okazja, aby wysłuchać prelekcji naszej ekspertki pt. „Jak dobrać skuteczne zabezpieczenie w łańcuchu dostaw”.


Polityka ®
Bezpieczeństwa
SZKOLENIA
Z OCHRONY DANYCH
OSOBOWYCH
SPRAWDŹ OFERTĘ

AUTOMATYZACJA PROCESÓW BEZPIECZEŃSTWA

Jakub Goral
Energy Logserver

Kiedy mamy do czynienia z rozbudowanym środowiskiem informatycznym, manualna obsługa zdarzeń bezpieczeństwa to trudne zadanie. Może prowadzić do wydłużenia czasu wykrycia incydentu i narażenia krytycznych systemów. Automatyzacja procesów bezpieczeństwa pomaga wymiernie usprawnić codzienną pracę SOC.

INCYDENTY BEZPIECZEŃSTWA W 2022 ROKU

Wiele firm i organizacji obserwuje nasilenie występowania incydentów bezpieczeństwa. Według raportu „ENISA Threat Landscape 2022" główne zagrożenia to:

- Ransomware,
- Malware,
- Ataki socjotechniczne,
- Zagrożenia dotyczące danych (nieautoryzowany dostęp, wyciek),
- Zagrożenia dotyczące dostępności (DDoS, ataki na strony internetowe),
- Dezinformacja,
- Ataki na łańcuchy dostaw.

Mogą one prowadzić do poważnych konsekwencji: ograniczenie przychodów, utrata reputacji czy kradzież wrażliwych danych.

WYZWANIA SOC

Aby zapobiegać atakom, organizacje korzystają z różnych systemów bezpieczeństwa np. EDR, firewall, IDS/IPS, SIEM. Każdy z nich ma osobną konsolę do zarządzania i obsługi. Często w organizacjach funkcjonuje ponad 20 różnych narzędzi bezpieczeństwa. Poza tym ręczne korelowanie informacji jest bardzo nieefektywne.

Kiedy systemy generują zbyt wiele alertów, część może zostać nieobsłużona, zważywszy na to, że obecnie brakuje specjalistów cyberbezpieczeństwa. Regulacje nakładają na organizacje obowiązki dotyczące raportowania naruszeń. W przypadku RODO zgłoszenie do Urzędu Ochrony Danych Osobowych musi nastąpić w terminie 72 godzin.

SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE

Te wyzwania adresuje oprogramowanie SOAR (Security Orchestration, Automation and Response). Umożliwia ono zbieranie informacji o wykrytych incydentach i ich obsługę z poziomu jednej konsoli. Orkiestracja opiera się na integracjach z zewnętrznymi narzędziami.

Możemy wyróżnić dwie grupy integracji. Do pierwszej z nich należą akcje, które pozwalają na analizę danych zawartych w alertach i ich wzbogacanie np.:

- Sprawdź plik lub URL w sandboxie,
- Sprawdź reputację pliku w serwisach Threat Intelligence,
- Poznaj geolokalizację adresu IP,
- Przeanalizuj plik pod kątem reguł YARA.

Druga grupa dotyczy realizacji odpowiedzi na incydent np.:

- Kwarantanna hosta w EDR,
- Zablokuj IP na firewallu lub agencie,
- Zablokuj domenę na proxy,
- Dodaj e-mail do blacklisty na bramce.

W procesie obsługi incydentów skupiamy się na ograniczeniu rozległości ataku i jego wpływu na działanie organizacji. Dążymy do tego, aby zoptymalizować procesy obsługi incydentów i uwolnić analityków od rutynowych, monotonnych zadań. Dzięki temu zmaksymalizujemy zwrot z inwestycji poniesionych na systemy bezpieczeństwa i w pełni wykorzystamy potencjał zespołu. Platforma SOAR umożliwia automatyzację obsługi zdarzeń bazując na integracjach i orkiestracji.

Wybierając system SOAR warto zwrócić uwagę na łatwość integracji z narzędziami, których używamy w organizacji. Ważna jest możliwość pobierania oraz aktuaizowania zdarzeń w użytkowanym systemie ticketowym. Powinniśmy zwrócić uwagę na opcje rozwoju produktu i dodawania nowych integracji.

MIERZENIE EFEKTYWNOŚCI ZESPOŁÓW BEZPIECZEŃSTWA

Do mierzenia efektywności obsługi zdarzeń wykorzystywane są metryki MTTD (Mean Time To etect) oraz MTTR (Mean Time To Respond). Im dłuższy czas wykrycia incydentu i reakcji na niego, tym poważniejszy może mieć wpływ na organizację. Korzystając z SOAR możemy obniżyć zarówno MTTD, jak i MTTR. Orkiestracja pomaga skrócić MTTD poprzez wzbogacanie incydentów o dodatkowe dane kontekstowe. Dzięki temu analitycy bezpieczeństwa spędzą mniej czasu na zbieraniu informacji, a skoncentrują się na bardziej wymagających zadaniach. Z drugiej strony

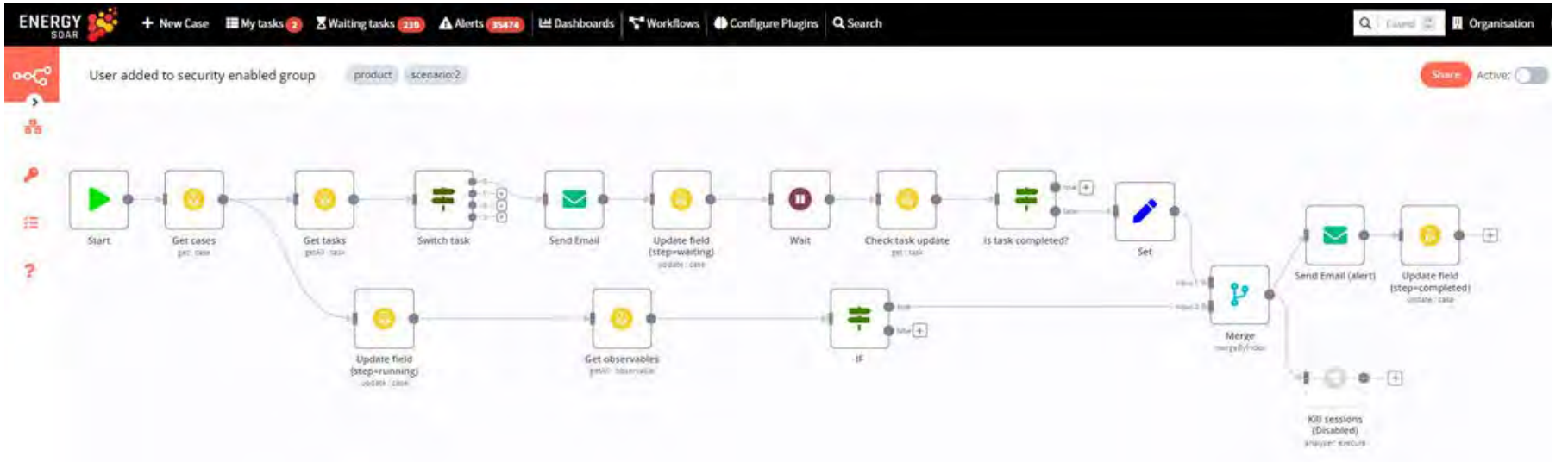
automatyzacja obniża MTTR poprzez wyzwalanie akcji nawet bez konieczności udziału operatora.

BUDOWANIE SCENARIUSZA AUTOMATYZACJI

Playbook to projekt automatyzacji. Składa się z połączonych węzłów, które mają wykonać określone zadania takie jak: przyjmowanie danych, ich procesowanie i wysyłanie dalej. Połączenie między węzłami odpowiada za przekazywanie informacji w ramach zdefiniowanego scenariusza.

Każdy węzeł może mieć jedno lub kilka połączeń. Playbooki mogą być wyzwalane ręcznie, według harmonogramu lub kiedy wystąpi wskazane zdarzenie. Playbook kończy procesowanie, gdy wszystkie połączone węzły przetworzą swoje dane.

Węzły mogą dodawać, usuwać i edytować dane zgromadzone wewnątrz platformy SOAR, jak również integrować się dwukierunkowo z zewnętrznymi aplikacjami czy usługami. Węzły łączą się z systemami zbierania logów, aby pobierać dodatkowe informacje. Wykonują zapytania do baz danych. Integrują się z platformami Threat Intelligence i sandbox. Mogą odbierać i wysyłać maile, czytać i zapisywać pliki. Dodatkowo kluczową rolę pełnią węzły wspomagające takie jak pętle, czy sprawdzenia warunków. Pozwalają one powtarzać zdefiniowane operacje oraz przekierować procesowanie scenariusza na wariantowe ścieżki.



Na koniec możemy również dodać automatyczne akcje blokowania adresów IP, hashy plików, czy wykonania kwarantanny hosta. Definiujemy również powiadomienia przez mail, SMS lub komunikatory internetowe.

W celu uwierzytelnienia do zewnętrznych systemów i usług wprowadzamy loginy, hasła, tokeny lub klucze API oraz adres instancji, z jaką chcemy się połączyć, aby wymieniać informacje. Wprowadzone dane są przechowywane jako gotowe do użycia obiekty, z których korzystamy, gdy dodajemy nowe węzły do playbooka.

Przykłady użycia scenariuszy automatyzacji:

- Analiza reputacji obiektów (np. IP, domena) występujących w alercie w źródłach Threat Intelligence i zablokowanie adresu IP,
- Pobieranie zgłoszeń z systemu ticketowego oraz wzbogacanie ich o dodatkowe informacje i aktualizacja,
- Analiza maili (załącznik, URL), powiadomienie użytkownika i blokowanie,
- Dystrybucja powiadomień o wykrytych podatnościach do właścicieli zasobów na podstawie informacji pobranych z bazy danych,
- Przypomnienia o otwartych zgłoszeniach za pomocą SMS-a, maila, komunikatorów internetowych.

AUTOMATYZACJA - DOBRE PRAKTYKI

Kiedy budujemy playbook, unikajmy bardzo rozbudowanych scenariuszy. W ich przypadku utrzymywanie i rozwiązywanie problemów bywa trudniejsze. Lepiej budować playbooki prostsze, a zarazem modu-

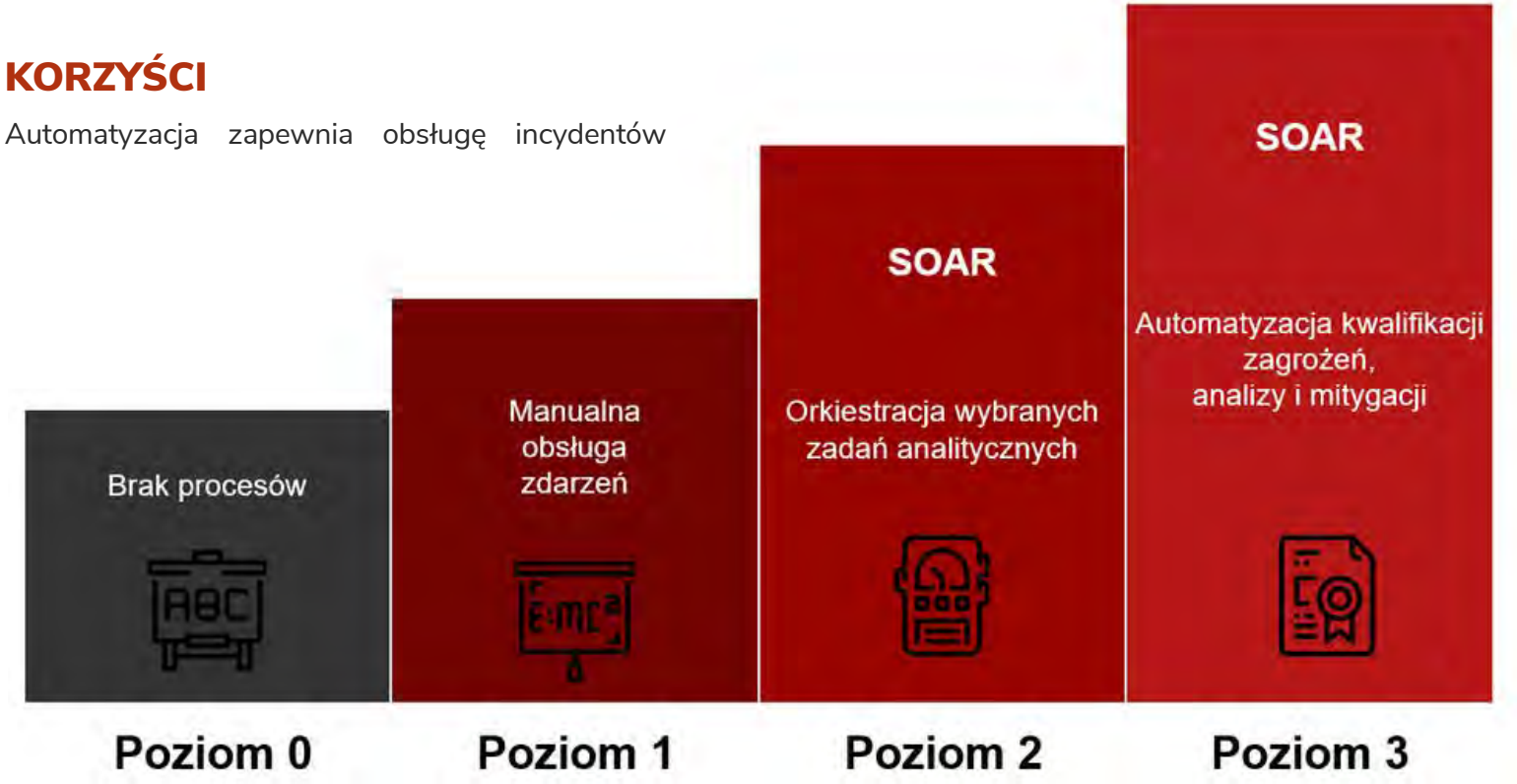
larne , aby mogły być użyte wielokrotnie.

Scenariusze automatyzacji powinny być testowane. Warto pamiętać, aby uwzględniały obsługę błędów. Istotne jest, żeby informacje dotyczące problemów z wykonaniem playbooków były na bieżąco przekazywane do administratorów systemu.

Po zbudowaniu scenariusza warto przeanalizować korzyści płynące z jego implementacji. Każde wykonanie playbooka może być zliczane przez SOAR, aby mierzyć zaoszczędzony czas oraz koszty.

KORZYŚCI

Automatyzacja zapewnia obsługę incydentów w trybie 24x7, nawet jeśli zespół nie pracuje w takim oknie czasowym. Zwiększa produktywność oraz przyspiesza wykrywanie zdarzeń. Pozwala skrócić czas obsługi incydentów, odsiać alarmy false-positive i uwolnić zasoby do bardziej wymagających zadań takich jak pogłębione analizy, czy threat hunting. Wreszcie automatyzacja eliminuje wariantowość, gwarantując obsługę zdarzeń według zdefiniowanego wzorca. Korzystanie z automatyzacji to także wyznacznik dojrzałości procesów bezpieczeństwa w organizacji.



AUTOMATYZACJA. OD CZEGO ZACZĄĆ?

W procesie obsługi incydentów dużo czasu zajmują powtarzalne zadania np. weryfikacja alarmów, zbieranie informacji, sprawdzanie IOC, analiza obiektów w sandbox.

Dochodzą do tego działania dotyczące komunikacji (wysyłanie powiadomień i eskalacji), czy rejestracji postępu prac np. zakładanie zgłoszeń w systemach ticketowych.

Te żmudne czynności wykonywane w sposób manualny często blokują potencjał zespołu SOC.

Kluczem do rozwiązania problemu jest skuteczna automatyzacja procesów z wykorzystaniem platformy SOAR. Automatyczne wzbogacanie incydentów o niezbędne dane pozwala operatorowi skupić się na sednie zagrożenia. Integracja SOAR z systemami bezpieczeństwa pozwala zrobić krok dalej, całkowicie niwelując potrzebę angażowania zespołu SOC w pracę nad powielającymi się incydentami.

ODO

WDROŻENIA | AUDYTY | SZKOLENIA

„ODO SZKOLENIA“

BERKA JOSELEWICZA 15/11
42- 202 CZĘSTOCHOWA

600 299 249

BIURO@ODOSZKOLENIA.PL

SPECJALIZACJE

RODO

SZKOLENIA

AUDYTY

WDROŻENIA

Specjaliści RODO – zarówno w zakresie usług doradczych, jak i wdrożeniowych.

Z naszych dedykowanych usług, jak i szkoleń specjalistycznych korzystają przedstawiciele niemal każdej branży, jak również sektora publicznego. Wspieramy firmy i Instytucje w procesach rozwojowych, dlatego oferta naszych szkoleń jest rozbudowana oraz przystosowywana do wymagań i rozwoju biznesu naszych Klientów. ODO Szkolenia to specjaliści, eksperci, praktycy, świetni szkoleniowcy – oferujemy najwyższej jakości konsultacje, szkolenia, audyty.

Działamy na terenia całej Polski.

Uczestniczymy w grupach roboczych, należymy do branżowych Stowarzyszeń Inspektorów Ochrony Danych (SABI), szkolimy studentów. Nasi eksperci pełnią funkcje IOD.

PRAWNE ASPEKTY OCHRONY DANYCH OSOBOWYCH, NOWYCH TECHNOLOGII A ETYKA

Magdalena Celeban
ODO Szkolenia

Zazwyczaj mówiąc o nowych technologiach i zapewnieniu bezpieczeństwa przetwarzania danych osobowych z ich wykorzystaniem nie zastanawiamy się nad problemem etyki. Być może zapominamy o tym, co najważniejsze, zbyt mocno akcentując przepisy prawa.

Celem artykułu jest zwrócenie uwagi, być może chwilowe zamyślenie się nad problematyką związanej z prawnymi przepisami jak również i etycznymi przepisami prawa dotyczącymi ochrony danych osobowych. Szczególnej analizie zostały poddane dylematy z jakimi spotykamy się podczas stosowania przepisów prawa w szczególności podczas próby odpowiedzi na pytanie: czy prawo może zastąpić etykę? Tematyka związana z ochroną danych osobowych jest wyjątkowo interesującą, ale w połączeniu z etyką nabiera dodatkowej barwy i tajemniczości.

PODSTAWY PRAWNE PRZETWARZANIA DANYCH OSOBOWYCH

Od niemalże 5 lat stosujemy w unii europejskiej Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Większość z nas zapytana o podstawy prawne dotyczące ochrony danych osobowych, wymieni właśnie powyższą podstawę.

Nie możemy jednak zapominać, że oprócz RODO, mamy również Konstytucję Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r, która zawiera dwa bardzo istotne zapisy, jest to Art. 49 o brzmieniu: *Zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastą-*

pić jedynie w przypadkach określonych w ustawie i w sposób w niej określony, jak również Art. 51:

1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.
2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.
3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.
4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.
5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

Powyższy przepis często jest nazywany RODO w pigułce.

W Polsce mamy również od 2018 roku zaktualizowaną ustawę o ochronie danych osobowych, która, zapewnia stosowanie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, zwanego RODO.

PRAWNE ASPEKTY OCHRONY DANYCH

Zazwyczaj powołujemy się w naszej pracy na powyższe zapisy, i w nich też upatrujemy szansę na zgodność przetwarzania danych osobowych naszych pracowników i kontrahentów. Wielokrotnie spotykam się z zapytaniem ze strony klienta: „Czy możemy znaleźć jakąś podstawę prawną, aby móc zbierać i gromadzić dane?”.

Niestety w pracy codziennej, w związku z realizację kolejnego celu, kolejnego deadline zapominamy o tym co najważniejsze, czyli podejściu do tematyki ochrony

danych osobowych, jako wartości człowieka, jego prywatności i poczucia bezpieczeństwa, ale również, i chyba, to co najważniejsze etyki podejmowanych decyzji o przetwarzaniu danych osobowych, a być może nawet ich udostępnianiu.

SZTUCZNA INTELIGENCJA

Sztuczna inteligencja w ostatnim czasie budzi gorące dyskusje, na co dzień spotykamy zarówno zwolenników, którzy nie wyobrażają sobie pracy bez wsparcia AI, jak również coraz częściej do głosu dochodzą przeciwnicy, którzy zastanawiają się nad długofalowymi konsekwencjami wykorzystywania AI zarówno w pracy, jak i naszym codziennym życiu. Od pewnego czasu mamy wrażenie, że nie zastanawiamy się już nad tym „czy" ale „kiedy" będziemy musieli się na stałe wprowadzić w naszą pracę nowe technologie.

Problem pojawia się już na etapie zdefiniowania sztucznej inteligencji, nie ma na dzień dzisiejszy jednej definicji, dziedzina ta jest nadal definiowana od nowa i chyba tak już zostanie, bo wraz z rozwojem nowych technologii będzie ewaluować pojęcie sztucznej inteligencji. Dla wielu z nas sztuczna inteligencja oznacza całkowicie co innego, dla jednych z nas to sztuczne formy życia, które mogą przewyższyć ludzką inteligencję, dla innych to tylko technologia przetwarzania danych.

Zapewne sztuczna inteligencja ma szerokie zastosowanie, często nawet nie zdajemy sobie sprawy, jak często się z nią spotykamy na co dzień, na przykład w zakładach produkcyjnych przy analizie danych z wykorzystywaniem danych do ulepszanie produkcji, przemysł 4.0 a właściwie 5.0 daje nam najlepszy obraz na obecny stan wykorzystania nowych technologii.

ETYKA W OCHRONIE DANYCH

Etyka AI i nowych technologii często koncentruje się na tym jak będzie wpływała na ludzi i decydowała o nich, technologia fundamentalnie zmieni ludzi. Nowe technologie kwestionują obecne normy oraz systemy pojęciowe, co jest szczególnie interesujące dla filozofii. Wreszcie, gdy zrozumiemy technologię w jej kontekście, musimy ukształtować naszą reakcję społeczną, w tym regulacje i prawo.

W kontekście stosowania nowoczesnych technologii do przetwarzania danych bardzo ważnym aspektem jest ich etyczne wykorzystanie. W sytuacjach kiedy ludziom trudno jest podjąć pewne decyzje, czasami na pograniczu życia i śmierci, to co

z decyzją podjętą przez AI, jaką podejmie?

Obawy o etyczne przettwarzanie danych i podejmowanie na ich podstawie decyzji wynikają między innymi z trudności ustalenia działań algorytmu oraz zapewnienia poprawności danych pozyskiwanych z różnych źródeł.

Musimy pamiętać, ze podczas podczas analizy danych i wykroczenia poza zgodność z wymogami prawnymi, najważniejszym aspektem powinna być etyka.

Problem etyki jest dostrzegany i podnoszony już coraz częściej w Unii Europejskiej, niejednokrotnie problem podjął już Europejski Inspektor Ochrony Danych, który podkreśla, że należy rozważać etyczny wymiar przetwarzania danych.

PODSUMOWANIE

Podejście związane z etyką podczas podejmowanych działań z zakresu ochrony danych osobowych zarówno z kontrahentami, współpracownikami, jak również podczas zajęć ze studentami jest obowiązkowe. Jest to temat, który powinien szczególnie zainteresować badaczy związanych z bezpieczeństwem, ochroną danych osobowych, czy AI.

W obecnych czasach kiedy technologie zaczynają zajmować kluczowe miejsca w naszym codziennym funkcjonowaniu, nie możemy zapominać o aspektach i czynnikach ludzkich.

Etyczne zagadnienia powinny być uwzględnione w szczególności w przypadku zastosowania rozwiązań informatycznych z zastosowaniem sztucznej inteligencji. W erze cyfrowej wszelkie działania powinny szczególnie doceniać dorobek człowieka, który liczymy wiekami, a nie tylko latami.

Musimy pamiętać, że „Prawo nie zastąpi etyki", przynajmniej tak powinno być, na co wskazuje również historia prawa, która zawsze była spójna z oczekiwaniami ludzi i kolejnych pokoleń.

Prawo ma wspierać i pomagać ludziom w codziennym funkcjonowaniu, jednak zawsze to „człowiek powinien być najważniejszy". Tematyka związana z ochroną danych osobowych na pewno nie jest dla tych, którzy lubią stabilność, osoby zajmujące się tą tematyka muszą być aktywne i wciąż się dokształcać, poszerzać swoja wiedzę. Metody oraz narzędzia wykorzystywane w ochronie danych osobowych należy na bieżąco dostosowywać do nowych wyzwań, zwłaszcza przemian technologicznych.

W TWOJEJ FIRMIE
ZDARZYŁ SIĘ

WYCIEK DANYCH OSOBOWYCH?

MOŻEMY CI POMÓC

SPRAWDŹ JAK

Polityka® Bezpieczeństwa

SECURITYMAGAZINE.PL

WYKRYWANIE ATAKÓW SIECIOWYCH, OCHRONA I MONITORING AI

Redakcja
SECURITY MAGAZINE

Bezpieczeństwo i cyberbezpieczeństwo powinny być synonimami każdej firmy. Jednak nie każda organizacja jest w stanie poprawić te kwestie na własną rękę. Z pomocą przychodzą startupy, które adresują liczne problemy przedsiębiorstw B2B czy B2C. Dowiedz się, jak mogą Ci pomóc.

WYKRYWANIE ANOMALII I ATAKÓW SIECIOWYCH

Cryptomage to startup, który dostarcza tzw. sondę sieciową Network Detection and Response Cryptomage Cyber Eye™ – czyli narzędzie analityczne do wykrywania i prognozowania anomalii w ruchu sieciowym w czasie rzeczywistym. Startup nie zajmuje się wyłącznie badaniem zachowania użytkownika czy urządzeń, ale oferuje też głęboką analizę ruchu sieciowego, stanów i zachowania protokołów sieciowych czy analizy poszczególnych urządzeń w sieci.

Rzeczone narzędzie powstało w oparciu o uczenie maszynowe i algorytmy sztucznej inteligencji. Startup chwali się, że dzięki temu jest w stanie bardzo łatwo identyfikować, monitorować czy segregować transakcje, połączenia i potencjalne złośliwe zdarzenia. Ma to zapewniać organizacjom większe poczucie ochrony, a co ważne – zautomatyzować procesy. Co za tym idzie, incydenty oraz cyberzagrożenia wykrywane są szybciej, a także łatwiej im zapobiegać.

Startup pomaga wykrywać wycieki danych osobowych, analizuje zdarzenia, monitoruje metadane przepływu, przeprowadza analizę behawioralną protokołów i wykrywa anomalie, a także ocenia ryzyko każdego incydentu. A ze względu na to, że technologia ta powstała dzięki uczeniu maszynowemu – system cały czas uczy się na nieznanych protokołach.

Do klientów startupu zaliczają się już Comarch, Tauron, CD Projekt, Bank Ochrony Środowiska, Prokuratura Krajowa, Politechnika Pomorska, Akademia Górniczo-Hutnicza czy Alior Leasing.

MONITORING, NADZÓR INFRASTRUKTURY I ZABEZPIECZENIA

Cyberbezpieczeństwo jest ważne, ale zagrożenia czyhają na nas także w świecie rzeczywistym. Pracownicy mogą być narażeni na różne niebezpieczeństwa, podobnie jak firmowe dane czy zasoby. Wystarczy, chociażby wziąć pod uwagę pożary czy awarie sieci elektroenergetycznych albo kradzieże.

W takim przypadku pomaga ZAZ Security. To startup wywodzący się z Warszawy, który zajmuje się projektowaniem, wdrażaniem i utrzymywaniem różnorodnych systemów technicznych, wspierających bezpieczeństwo w firmach. Organizacja oferuje m.in. elektroniczne systemy ochrony moni-

toringu infrastruktury krytycznej (np. stacji elektroenergetycznych czy węzłów telekomunikacyjnych) oraz architekturę integracji nadzoru pełnej infrastruktury i automatyki budynków czy układów bezpieczeństwa.

Jednak to nie wszystko. Spółka pomaga również w kwestii nadzoru elektronicznych systemów ewidencjonowania kluczy, czy w ogóle tworzy zabezpieczenia np. sygnalizację włamania i napadu, dostępu SKD, rejestracji czasu pracy RCP lub telewizji przemysłowej CCTV.

Startup zajmuje się nawet opieką nad magazynami i obiektami do wytwarzania czy przechowywania materiałów wybuchowych, broni i amunicji. A także sieciami elektroenergetycznymi i instalacjami sterowania ruchem kolejowym. Wszystko to połączone jest w Systemie Skarbiec, którego zadaniem jest zintegrowanie systemów w celu gromadzenia i zarządzania danymi. Spółka chwali się, że to zdecydowanie poprawia nadzór nad systemami bezpieczeństwa.

Oferta startupu jest też na tyle szeroka, że adresuje kwestie sygnalizacji przeciwpożarowej. ZAZ Security dostarcza też system gaszenia gazem czy

aerozolem. Ponadto przechowuje informacje niejawne przedsiębiorstwa. Wśród klientów ZAZ Security są m.in. PKP Energetyka S.A., Warbud S.A., PKP InterCity S.A., Polskie Linie Kolejowe S.A., LOT Aircraft Maintenance Services sp. z o.o., Kancelaria Prezesa Rady Ministrów, Centrum Szkolenia Sił Połączonych NATO czy Krajowa Administracja Skarbowa.

MONITORING AI

Wspominaliśmy o monitoringu i na polskim rynku działa startup, który dostarcza bardzo ciekawe rozwiązanie w tym aspekcie. Chodzi o spółce z siedzibą w Berlinie i Łodzi – Sternkraft Video Telematics. Startup oferuje technologię wideo pracującą 24/7 na rzecz bezpieczeństwa transportu publicznego – Computer Vision. Jest to system kamer, który identyfikuje, ostrzega i zapobiega niebezpieczeństwom.

Technologia ICCTV działa w oparciu o sztuczną inteligencję i nie wymaga nadzoru. System ten wykrywa przestępstwa, zlicza pasażerów, sprawdza, czy kierowca w trakcie jazdy korzysta ze smartfona albo, czy trzyma ręce na kierownicy. Krótko mówiąc, sprawia, że transport jest bezpieczny. System ten sprawdza się zarówno w prywatnych, jak i publicznych spółkach. Startup chwali się, że dzięki ICTTV przestępczość w transporcie publicznym maleje nawet o 50%.

Według Sternkraft zastosowanie takiej technologii obniża też wydatki na monitoring oraz jego nadzór. W końcu nie potrzeba dedykowanej osoby do analizowania, czy wszystko jest w porządku. System jest bowiem w pełni autonomiczny.

Rzetelny® Regulamin

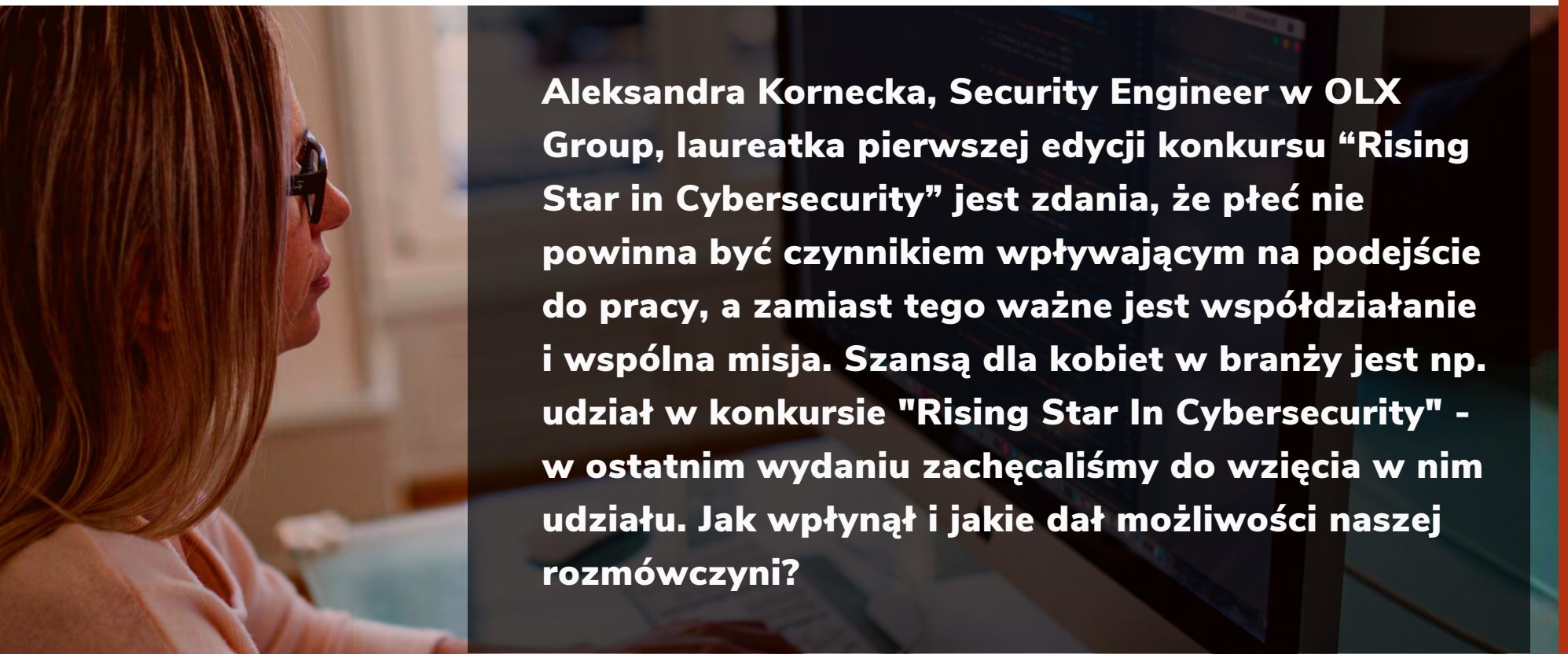
DYREKTYWA OMNIBUS

DOSTOSUJ Z NAMI SWÓJ SKLEP
DO NOWYCH PRZEPISÓW

SPRAWDZAM OFERTĘ

NIE PŁEĆ, A MISJA MA ZNACZENIE W BRANŻY SECURITY

Aleksandra Kornecka



Aleksandra Kornecka, Security Engineer w OLX Group, laureatka pierwszej edycji konkursu “Rising Star in Cybersecurity” jest zdania, że płeć nie powinna być czynnikiem wpływającym na podejście do pracy, a zamiast tego ważne jest współdziałanie i wspólna misja. Szansą dla kobiet w branży jest np. udział w konkursie "Rising Star In Cybersecurity" - w ostatnim wydaniu zachęcaliśmy do wzięcia w nim udziału. Jak wpłynął i jakie dał możliwości naszej rozmówczyni?

Zacznijmy od tego, czy widzi Pani różnice w podejściu mężczyzn i kobiet do pracy w cyberbezpieczeństwie? Jeśli tak, jakie są to różnice?

Aleksandra Kornecka: Prawdę mówiąc, płeć szefów czy współpracowników nigdy nie była dla mnie istotna. Zależy mi na pracy z osobami rozumiejącymi, że cyberbezpieczeństwo to "sport zespołowy".
Znam zarówno kobiety bardzo przejęte misją chronienia zasobów organizacji i pracujące po godzinach, by lepiej wypełnić tą misję, jak i takie, które pracują od 9 do 17 i nie zaprzątają sobie głowy cyberbezpieczeństwem po pracy. Znam mężczyzn, którzy "przeżywają" każdą znalezioną podatność bezpieczeństwa, jak i takich, którzy wykonują obowiązki zawarte w umowie, nie troszcząc się o nic ponad to. Kluczowe jest znalezienie równowagi - tak by dać z siebie zespołowi to co trzeba, ale też nie musieć przesiadywać po godzinach.

Dlaczego w cyberbezpieczeństwie, czy bezpieczeństwie w ogóle, Pani zdaniem, łatwiej pracę znaleźć jednak mężczyznom?

A.K.: Moją pierwszą reakcją na to stwierdzenie był sprzeciw - dlaczego mężczyznom miałoby być łatwiej znaleźć pracę w cyberbezpieczeństwie? Po chwili namysłu stwierdziłam, że coś w tym, niestety, jest - w ostatnich kilkudziesięciu latach mainstream kulturowy wpaja społeczeństwu, że IT, a tym bardziej cyberbezpie-

czeństwo, to jest z jakiegoś powodu branża “typowo dla mężczyzn”. Ja nie widzę takiej zależności. Branża IT jak i cyberbezpieczeństwo naprawdę jest dla wszystkich, którzy są nimi zainteresowani oraz nabywają potrzebne kompetencje.

Być może taka percepcja “że kobietom jest trudniej” bardziej działa z drugiej strony - jako że środowisko tej pracy wygląda na bardziej przystosowane do mężczyzn, bardziej oczywiste dla nich - czy to będą niszowe żarty, czy po prostu przyzwyczajenie do widoku mężczyzn, czy pokłosie stereotypów.

Czasy “chłopców w bluzach z kapturem siedzących w piwnicy” jako tych, którzy głównie zajmują się cyberbezpieczeństwem - ci raczej zajmowali się hackingiem, niż normalna pracą - już minęły. Oczywiście oni nadal funkcjonują, jednak większość ofert pracy na rynku dotyczy “zwykłych stanowisk” w “zwykłych organizacjach”, w których liczy się realna praca i pomoc przy zabezpieczaniu oraz kontrolowanym atakowaniu infrastruktury i aplikacji organizacji w celu zapewnienia jej wystarczającego poziomu bezpieczeństwa przed zagrożeniami z zewnątrz.

Co do kolejnych myśli na temat tendencji płci w pracy - być może paratradycjonalistyczne wychowanie i przestarzałe trendy kulturowe w stylu “kobiety na polonistykę, mężczyźni na matematykę” nadal pokutują i powodują wolniejszy przyrost kobiet w IT.

Może też w jakimś stopniu brakuje tzw. “role models” kobiecych, przez co mniejszej ilości kobiet wydaje się, że to praca też dla nich. Coś w tym jest, bo jeśli widzisz samych mężczyzn w cyberbezpieczeństwie, to trudniej ci uwierzyć, że to branża też dla ciebie. Mam nadzieję, że coraz mniej ludzi będzie myślało w ten sposób, albo chociaż poszukają tych “role models” i odszukają - bo ich nie brakuje, może są czasem po prostu mniej wyeksponowane.

Czy organizacja takich inicjatyw, jak chociażby "Rising Star In Cybersecurity" może zmienić to podejście?

A.K.: Inicjatywy takie jak ten konkurs pomagają pokazać oczywistą oczywistość - że w cybersecurity jest miejsce dla osób identyfikujących się jako kobiety, że one tam są i że trzeba ich więcej. Takie inicjatywy jako kierowane do kobiet mają moc eksponować "role models", które są w branży w mniejszości, pomóc je odkrywać, a tym samym pomagają ośmielać różne osoby do podążania za swoimi zawodowymi zainteresowaniami niezależnie od bagażu doświadczeń rodzinnych i kulturowych.

Co dał Pani udział w konkursie?

A.K.: Korzyści jest wiele. Zarówno pod kątem rozwoju osobistego i kompetencji miękkich, jak i rozwoju w cybersecurity. Konkurs polega na opisaniu, jaki wpływ na firmę miał projekt, który się realizowało samodzielnie lub w zespole. Potem trzeba nauczyć się o nim opowiadać tak, by przekonać jury, że właśnie on był najbardziej zmieniający status quo. W tym celu należy przygotować prezentację oraz przemyśleć zarówno sam opis, jak i wskaźniki biznesowe i/lub techniczne którymi można się pochwalić.
Proces i etapy konkursu przypominają nieco rundy startupowe, kiedy walczy się o pozyskanie inwestorów. Liczą się zarówno twarde fakty, merytoryka, ale też tzw. "buy-in" inwestorów. Tyle że tematem jest cyberbezpieczeństwo, a nagrodą studia.

Jeśli ktoś nie miał dotąd doświadczeń w przemówieniach publicznych, to może być dodatkowo wartościowa przygoda. Ponadto sam konkurs daje dostęp i kontakt do znakomitych specjalistek i specjalistów. Z morza osób na rynku pracy czy kontaktów na LinkedIn stajesz się osobą, którą się pamięta, darzy poważaniem i może w przyszłości, którą chętnie się zatrudni.

Osobiście bardzo doceniłam spotkania z liderkami działów bezpieczeństwa z różnych obszarów, jakie dane mi było poznać w czasie konkursu. To też pole do potencjalnych wspólnych działań w przyszłości, a do tego są to najzwyczajniej w świecie świetne osoby.

Ogromnym zbiorem korzyści są same studia, czyli nagroda w konkursie. Poza oczywistą wartością, jaką jest wiedza i poznanie doświadczeń praktyków wykładających przedmioty w programie tych stu-

diów, studia są genialną okazją do networkingu, nawiązywania kontaktów biznesowych, a nawet przyjaźni.

Są to studia podyplomowe, a zatem mamy tu do czynienia z osobami studiującymi, które już są na rynku pracy i to najczęściej parę lat, które mają też wiele doświadczeń i spostrzeżeń i pole do wymiany wiedzy.

Kto wie, czym mogą zaowocować te kontakty w bliższej lub dalszej przyszłości. Możliwe jest wszystko - od wspólnego prowadzenia podcastu, przez mentoring czy barterowy konsulting aż po założenie razem firmy.

Czy udział w konkursie miał wpływ na Pani karierę zawodową?

Co do wpływu konkursu na moją karierę zawodową, to stanowi on dla mnie świetny wpis do CV, znacząco poszerzył mi też sieć kontaktów, a ponadto trwają obecnie moje studia podyplomowe i już widzę korzyści, o których wspomniałam wcześniej. Część treści z programu studiów przyda mi się niemal od razu w obecnej pracy, także mój przełożony też jest rad, że podeszłam do konkursu i zdobyłam te studia.

Jakie cele chciałaby Pani osiągnąć w przyszłości w dziedzinie cyberbezpieczeństwa? Czy konkurs pomoże w ich realizacji?

Pod względem celów zawodowych konkurs dał mi świetną ”wędkę”, a ode mnie zależy, jakie ryby i ile ich złowię. Zdecydowanie konkurs wspiera realizację celów. Zależy mi bardzo na rozwoju w obszarze cloud security, ale też compliance i tutaj zdecydowanie już znalazłam pomocne treści oraz kontakty. Szczegółowych celów pozwolę sobie nie zdradzać, ale, oczywiście, są wśród

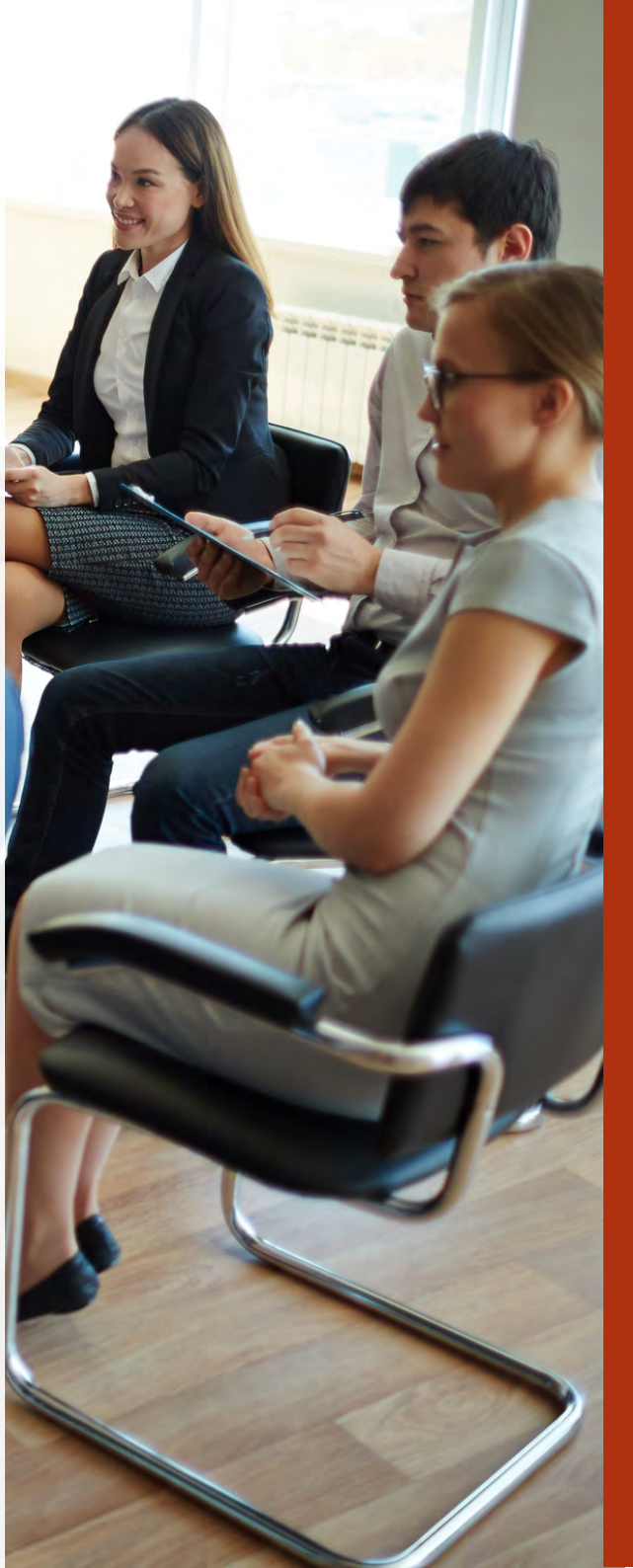
nich certyfikaty branżowe poświadczające kompetencje, jak i różne działania dające zabezpieczenie na przyszłość, by zdobyć jak najlepszą pracę, kiedy przyjdzie czas na taką zmianę.

Im więcej wiemy, tym więcej widzimy, ile jeszcze nie wiemy. Praca w cybersecurity to dla mnie nieustanne poznawanie i przyglądanie się, w którym kierunku chcę iść dalej. Obecnie mam już wystarczające podstawy, by widzieć horyzont możliwości oraz znam obszary potencjalnego rozwoju. Badam cały czas siebie, jak i rynek, by zdecydować, jaki kierunek będzie dla mnie najlepszy.

Jest Pani zaangażowana w działania na rzecz popularyzacji cyberbezpieczeństwa. Jakie działania Pani prowadzi?

A.K.: Od prawie 7 lat jestem zaangażowana w szerzenie wiedzy i wymianę doświadczeń poprzez wystąpienia publiczne na różnych wydarzeniach, np. meetupy, konferencje w Polsce i zagranicą, pisanie artykułów, mentorowanie. Wcześniej jako quality assurance engineer oraz tester, potem jako security engineer.

Jestem też członkinią stowarzyszenia ISSA Polska oraz sympatyczką Cyber Women Community - poznałam tę społeczność dzięki konkursowi. Największym osiągnięciem w mentoringu jest dla mnie moment, kiedy osoba którą uczę/której doradzam dostaje pracę albo, gdy mówi, że widzi postęp w swojej ścieżce. W takich momentach czuję, że to, co robię ma naprawdę sens. Największym osiągnięciem przy wystąpieniach jest dla mnie, kiedy ktoś podzieli się ze mną informację, że to, co przekazałam bardzo mu się przyda albo wyjaśniło mu wiele rzeczy.



Widzę też, że miewam szerokie zasięgi swoich postów na social mediach i od czasu do czasu staram się to wykorzystywać w popularyzacji dobrych praktyk cyberbezpieczeństwa, ostrzeganiu przed cyberoszustwami lub w poszerzeniu zasięgu dla osób poszukujących pracy.

Miłym momentem było, kiedy koleżanka z pracy poprosiła mnie o link do listy "punktów cyberhigieny" napisanej prostym językiem zrozumiałym dla ludzi spoza IT, którą stworzyłam z myślą o bezpieczeństwie znajomych oraz osób z rodziny moich kontaktów. W takich momentach czuję, że to co robię ma naprawdę sens.

Jakie rady miałaby Pani dla kobiet, które chcą rozpocząć karierę w dziedzinie cyberbezpieczeństwa lub zwiększyć swoją wiedzę i umiejętności w tej dziedzinie?

A.K.: Jeśli interesują Cię tematy dotyczące cyberbezpieczeństwa, to nie rezygnuj z ich odkrywania. Poszukuj sprzymierzeńców i życzliwych osób, które Ci pomogą, nie słuchaj osób zniechęcających Cię do tego różnymi słowami. Najgorsze, co można powiedzieć albo usłyszeć: "Nie dasz rady", guzik prawda.

Warto poszukać darmowych wydarzeń na miejscu i online, traktujących o cyberbezpieczeństwie - jak ISSA Polska, Cyber Women Community, konferencje What The Hack, CONFidence, BSides meetup, OWASP meetup, SecOps meetup itd. Warto poszukać lokalnie w swoim mieście.

Co do zwiększania wiedzy i kompetencji, to zależy od kierunku w cyberbezpieczeństwie, jaki nas interesuje. Dobrą wiadomością jest, że w internecie jest ogrom materiałów w różnych formatach, w tym mnóstwo darmowych. Gorsza wiadomość jest taka, że, jeśli nie pracowało się wcześniej w IT, to może być trudno rozeznać się w jakości materiałów, ich przydatności na realnym rynku pracy oraz w zrozumieniu czasami, jak ich bezpiecznie używać.

Ponadto by mieć dobry start w cyberbezpieczeństwie, warto jest przyswoić sobie choć podstawy podstaw IT - np. zrozumieć bardzo ogólnie naturę oprogramowania, hardware'u, budowę aplikacji, podstawy wiedzy o protokołach komunikacji i Internecie. Trzeba rozumieć, z jakich stron mogą nadejść zagrożenia, o których potem przyjdzie nam się uczyć, bądź też, jak zaatako-

wać samodzielnie aplikację w kontrolowanych warunkach - i za zgodą zleceniodawcy.

Dobrze jest też rozeznać, jakie obszary cyberbezpieczeństwa istnieją. Mogę wymienić przykładowo: application security, pentesting, network security, embedded software security, security operations an incident response (oraz Security Operations Center), infrastructure security i cloud security, security awareness and crisis communication, security compliance.
Jako security engineer mam do czynienia po trochu z różnymi z tych obszarów, jednak w zależności od firmy można pracować na specjalizowanym stanowisku. Również nazwy stanowisk potrafią bardzo się różnić w różnych firmach.

Na pewno też warto zadbać o znajomość języka angielskiego pozwalającą na swobodne czytanie dokumentacji i przyswajanie materiałów szkoleniowych. Choć w ostatnich latach pojawiło się wiele materiałów po polsku, to świat cybersecurity, podobnie jak całe IT, porozumiewa się oraz tworzy ważne treści głównie po angielsku. Również informacje o wyciekach, narzędziach, komunikaty są najczęściej po angielsku.

Dla osób szukających wiedzy oraz umiejętności z zakresu bezpieczeństwa aplikacji oraz pentestingu mogę polecić laboratoria na platformach TryHackMe, Hack The Box, OWASP JuiceShop. Ponadto światowy standard bezpieczeństwa a-plikacji OWASP Top Ten (web i mobile), a także OWASP Cheatsheets, a także kolejne projekty OWASP. Polecam też narzędzie Burp Suite Community oraz szkolenia firmy PortSwigger.

Dla pogłębienia wiedzy polecam rozmaite materiały jak np. Rozmowa Kontrolowana podcast, portal Niebezpiecznik, portal Zaufana Trzecia Strona, Hackernews i wiele, wiele innych. Dla osób zapoznających się, czym ogólnie jest cyberbezpieczeństwo po polsku polecam materiały Kacpra Szurka, a także Szkołę Security Macieja Kofela.

Na koniec życzę wszystkim osobom zainteresowanym cyberbezpieczeństwem odważnego dążenia do swoich marzeń oraz bezpiecznego korzystania z technologii wokół nas.

Dziękujemy za rozmowę i życzymy dalszych sukcesów!

Rozmawiała:
Monika Świetlińska


/GDPSYSTEM.EU
ZGODA NA COOKIES
Czy Twoja strona WWW spełnia wymogi prawne i daje możliwość elastycznego zarządzania cookies osobom, które ją odwiedzają?
SPRAWDŹ
SPEŁNIJ WYMOGI PRAWNE

BEZPIECZEŃSTWO DANYCH: DLP I KONTROLA UPRAWNIEŃ

Mateusz Jakubik
iSecure Sp. z o.o.

Ochrona informacji stała się jednym z najważniejszych wyzwań dla firm, instytucji oraz osób prywatnych. Wymiana danych i informacji odbywa się coraz częściej w środowisku cyfrowym, co niesie za sobą zagrożenia związane z kradzieżą, wyciekiem czy utratą poufnych informacji. Aby temu zapobiec, stosuje się różne metody i narzędzia, takie jak Systemy Zapobiegania Wyciekom Danych (DLP - Data Loss Prevention).

Wraz z rosnącym zapotrzebowaniem na ochronę informacji, coraz ważniejszą rolę odgrywają również systemy zarządzania uprawnieniami w systemach IT. Dostęp do danych i aplikacji powinien być nadawany tylko osobom, które faktycznie potrzebują do nich dostępu, co wymaga precyzyjnego określenia uprawnień oraz kontroli nad nimi.

W niniejszym artykule skupimy się na opisie Systemów Zapobiegania Wyciekom Danych oraz roli, jaką odgrywa rozliczalność nadawania uprawnień w systemach IT w kontekście ochrony informacji. Przedstawimy różne aspekty związane z tymi zagadnieniami, w tym m.in. definicję systemów DLP, sposoby ich działania oraz metody kontrolowania i zarządzania uprawnieniami w systemach IT. Omówimy również korzyści, jakie niosą ze sobą stosowanie tych narzędzi oraz wyzwania, jakie mogą pojawić się w procesie ich implementacji i wdrażania.

INFORMACJA – CZYM JEST?

W dzisiejszych czasach mówi się, że informacja to paliwo dzisiejszego świata. Wraz z rozwojem technologii i internetu informacja zaczęła odgrywać jeszcze większą rolę w życiu społecznym, gospodarczym i politycznym.

Wraz z pojawieniem się cyberprzestrzeni, czyli środowiska komunikacji i wymiany danych za pomocą sieci komputerowej, informacja stała się jeszcze bardziej wartościowa, ale i bardziej zagrożona. W cyberprzestrzeni informacje są przechowywane, przetwarzane i przesyłane szybciej i łatwiej niż kiedykolwiek wcześniej. Jednocześnie jednak, wraz z tym, pojawiły się nowe zagrożenia związane z cyberprzestępczością, w tym kradzieżą danych, szpiegostwem przemysłowym i innymi atakami, które mogą zagrażać bezpieczeństwu i prywatności naszych informacji.

W takim kontekście, ochrona informacji w cyberprzestrzeni stała się jednym z kluczowych wyzwań dla biznesu, instytucji i jednostek prywatnych. Wymaga ona odpowiedniej strategii oraz stosowania nowoczesnych narzędzi, takich jak Systemy Zapobiegania Wyciekom Danych (DLP), MDM, szyfrowaniu danych. W cyberprzestrzeni informacja jest narażona na wiele ryzyk, takich jak kradzież, wyciek czy utrata. Atakujący mogą wykorzystać różne me-

tody, takie jak phishing, malware czy social engineering, aby uzyskać dostęp do poufnych danych lub zaszyfrować je, uniemożliwiając ich odczytanie.

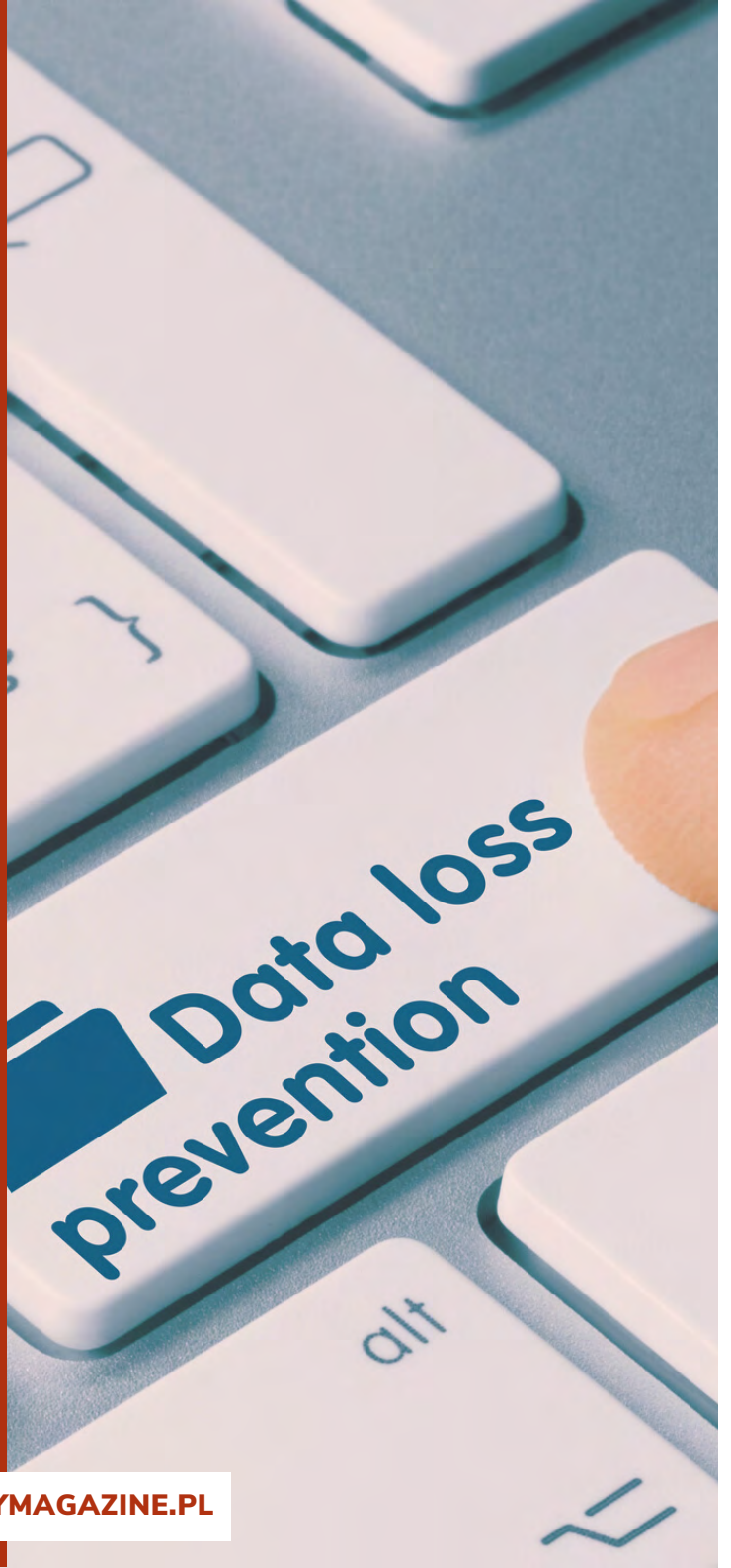
Dodatkowo, w wyniku niewłaściwej ochrony informacji, może dojść do utraty lub uszkodzenia danych, co również może mieć negatywny wpływ na funkcjonowanie firmy czy instytucji.

ZASADA ROZLICZALNOŚCI

Zasada rozliczalności to jedna z podstawowych zasad RODO (Ogólne Rozporządzenie o Ochronie Danych), której celem jest zapewnienie odpowiedzialności za przetwarzanie danych osobowych. Zgodnie z tą zasadą, podmiot przetwarzający (tj. osoba fizyczna lub prawna, organ publiczny lub inna jednostka, która przetwarza dane osobowe) jest odpowiedzialny za przestrzeganie przepisów RODO i musi udowodnić, że przetwarzanie danych osobowych odbywa się zgodnie z przepisami.

Oznacza to, że przedsiębiorstwa, organizacje i inne podmioty, które przetwarzają dane osobowe, muszą podejmować odpowiednie środki bezpieczeństwa oraz zapewnić ochronę danych osobowych przed nieuprawnionym dostępem, utratą lub kradzieżą. Powinni również prowadzić dokumentację dotyczącą przetwarzania danych osobowych oraz prowadzić rejestry i raporty, które umożliwiają identyfikację naruszeń i szybką reakcję w przypadku zdarzeń związanych z ochroną danych.

Zasada rozliczalności wymaga, aby podmiot przetwarzający był w stanie wykazać, że przestrzega przepisów RODO. Oznacza to, że podmioty przetwarzające



muszą prowadzić rejestry działań związanych z przetwarzaniem danych osobowych, a także dokumentować podejmowane przez siebie środki w celu zapewnienia bezpieczeństwa danych osobowych.

W przypadku naruszenia ochrony danych osobowych, podmiot przetwarzający musi być w stanie udokumentować, że podjął wszelkie możliwe środki w celu zapobieżenia naruszeniu i ograniczenia jego skutków.

Wprowadzenie zasady rozliczalności ma na celu zwiększenie odpowiedzialności podmiotów przetwarzających dane osobowe i umożliwienie kontrolowania ich działań przez organy nadzoru. W przypadku naruszenia przepisów RODO, organy nadzoru mogą nałożyć kary finansowe na podmiot przetwarzający dane osobowe, które mogą wynosić nawet do 20 milionów euro lub 4% rocznego światowego obrotu, w zależności od tego, które z tych kwot jest wyższe.

SYSTEMY DLP

Systemy DLP (Data Loss Prevention) to specjalne oprogramowanie lub urządzenia, które służą do ochrony danych przed wyciekiem z systemu informatycznego. Działanie systemów DLP opiera się na monitorowaniu przepływu danych wewnątrz organizacji i wykrywaniu potencjalnych zagrożeń związanych z wyciekiem informacji. Systemy DLP mogą działać w różnych warstwach sieci, np. na poziomie aplikacji, protokołu lub warstwy transportowej.

Głównym zadaniem systemów DLP jest identyfikacja poufnych informacji, takich jak hasła, numery kart kredytowych, dane osobowe, tajemnice handlowe i inne poufne informacje, a następnie zapobieganie ich nieautoryzowanemu ujawnieniu.

Systemy DLP wykorzystują różne techniki, aby wykryć i zapobiec wyciekom danych, takie jak analiza treści, wykrywanie urządzeń, które są wpinane do sieci oraz monitoring ruchu sieciowego.

System DLP (Data Loss Prevention) jest zaprojektowany w celu zapobiegania utracie danych poprzez monitorowanie, kontrolowanie i ograniczanie ich przepływu w sieci. DLP może również monitorować dyski zewnętrzne, takie jak pendrive'y i dyski twarde, w celu zapobiegania wyciekom danych. Aby system DLP mógł monitorować dyski zewnętrzne, musi mieć dostęp do informacji o ich aktywności. Istnieją różne sposoby na to, jak można to zrobić.

Oto niektóre z nich:

- **Kontrola dostępu** - System DLP może zastosować zasady kontroli dostępu, które ograniczą dostęp do dysków zewnętrznych tylko do osób upoważnionych. To pozwoli na śledzenie, kto i kiedy korzysta z dysku.
- **Wymuszanie szyfrowania** - DLP może wymusić szyfrowanie danych przechowywanych na dyskach zewnętrznych. To pomoże zapobiec wyciekom danych w przypadku utraty dysku.
- **Kontrola zapisu** - System DLP może kontrolować, jakie dane są zapisywane na dyskach zewnętrznych. Można na przykład ograniczyć możliwość kopiowania danych z wrażliwymi informacjami.
- **Śledzenie aktywności** - DLP może monitorować aktywność na dyskach zewnętrznych, taką jak kopiowanie, usuwanie lub zmienianie plików. To pozwoli na wykrycie podejrzanych działań i szybką reakcję na nie.

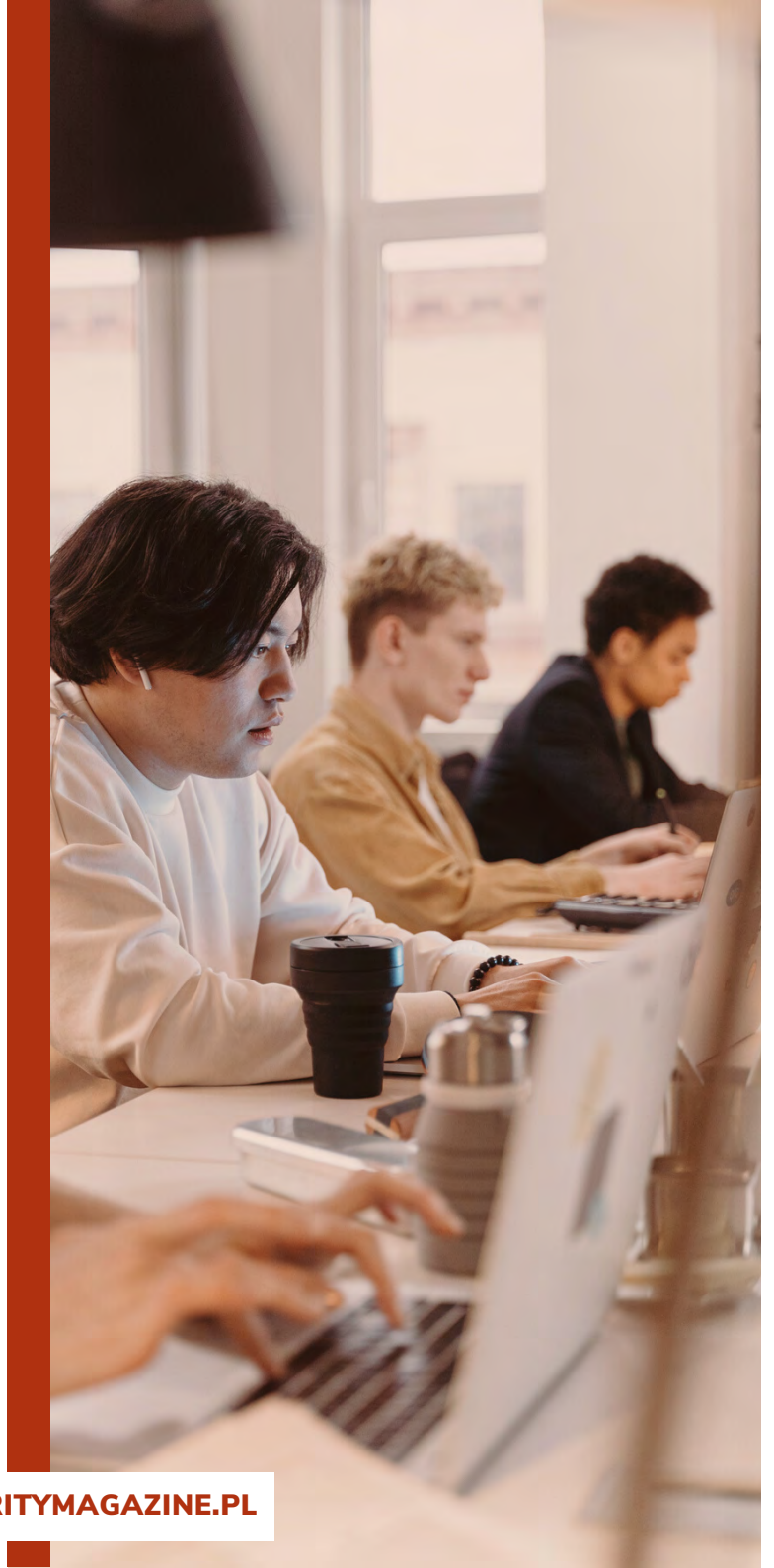
Wszystkie te metody mogą być wykorzystane wraz z oprogramowaniem do monitorowania aktywności na komputerze, co pozwoli na skuteczne monitorowanie dysków zewnętrznych oraz zapobieganie wyciekom danych.

NADAWANIE DOSTĘPÓW

System przyznawania uprawnień do systemów IT to proces zarządzania dostępem do systemów informatycznych, który ma na celu zapewnienie, że tylko uprawnione osoby mają dostęp do określonych zasobów systemowych. System ten obejmuje identyfikację użytkowników, autoryzację dostępu i monitorowanie działań użytkowników w systemie.

Proces ten zazwyczaj składa się z kilku etapów, które obejmują:

- **Identyfikację użytkownika** - Pierwszym krokiem jest potwierdzenie tożsamości użytkownika. W tym celu zazwyczaj wykorzystuje się login i hasło lub inne metody uwierzytelnienia, takie jak karty dostępowe lub biometryczne.
- **Autoryzację dostępu** - Następnym krokiem jest sprawdzenie uprawnień użytkownika oraz określenie, do których zasobów systemowych ma dostęp. To jest zwykle ustalane na podstawie roli użytkownika, stanowiska czy poziomu zaawansowania.
- **Przypisanie uprawnień** - W tym etapie definiuje się uprawnienia, jakie użytkownik ma mieć w systemie. To obejmuje zarówno



dostęp do określonych zasobów, jak i możliwość wykonywania określonych czynności, takich jak dodawanie, edytowanie lub usuwanie danych.

- **Monitorowanie działań** - Ostatnim krokiem jest monitorowanie działań użytkowników w systemie, w celu wykrycia nieuprawnionego dostępu lub podejrzanych działań. To pozwala na szybką reakcję na zagrożenia i zapobieganie naruszeniom bezpieczeństwa.

By zwiększyć bezpieczeństwo systemu, ważne jest, aby system przyznawania uprawnień był ściśle kontrolowany oraz monitorowany przez specjalistów ds. bezpieczeństwa IT. Powinno się również regularnie przeglądać i aktualizować listę użytkowników oraz ich uprawnień, aby zapewnić, że tylko uprawnione osoby mają dostęp do systemów IT.

SYSTEMY IAM

IAM to skrót od ang. Identity and Access Management, czyli zarządzania tożsamością i dostępem. Jest to kompleksowy system służący do zarządzania użytkownikami, ich tożsamościami oraz kontrolowania dostępu do zasobów systemowych.

Systemy IAM są wykorzystywane w celu zapewnienia bezpieczeństwa i ochrony danych w organizacjach. Dzięki nim można kontrolować, kto ma dostęp do określonych zasobów, jakie mają one uprawnienia i w jakim zakresie. Dzięki temu można zminimalizować ryzyko naruszenia poufności danych,

kradzieży danych lub innych niepożądanych działań.

Systemy IAM pozwalają na zarządzanie identyfikatorami użytkowników, takimi jak loginy i hasła, ale też na zarządzanie dostępem do aplikacji, systemów i innych zasobów. Użytkownicy są identyfikowani przez unikalne tożsamości, które są przechowywane w systemie. Dzięki temu można kontrolować dostęp do różnych zasobów, takich jak pliki, foldery, aplikacje, bazy danych i inne.

Funkcjonowanie systemów IAM opiera się na kilku podstawowych elementach:

- **Autentykacja** - potwierdzenie tożsamości przez system, np. przez wpisanie loginu i hasła.
- **Autoryzacja** - przypisanie uprawnień do określonych zasobów w systemie na podstawie tożsamości użytkownika.
- **Zarządzanie tożsamościami** - proces zarządzania tożsamościami użytkowników, np. tworzenie i usuwanie kont użytkowników, nadawanie uprawnień, itp.
- **Audytowanie** - rejestrowanie działań użytkowników w systemie, np. logowanie do systemu, próby logowania, operacje na plikach i folderach itp.

Systemy IAM pozwalają na zintegrowanie różnych aplikacji i systemów w jednym miejscu, co ułatwia zarządzanie dostępem użytkowników i redukuje koszty administracyjne. Dodatkowo, zapewniają bezpieczeństwo danych przez kontrolowanie dostępu do zasobów i audytowanie działań użytkowników.

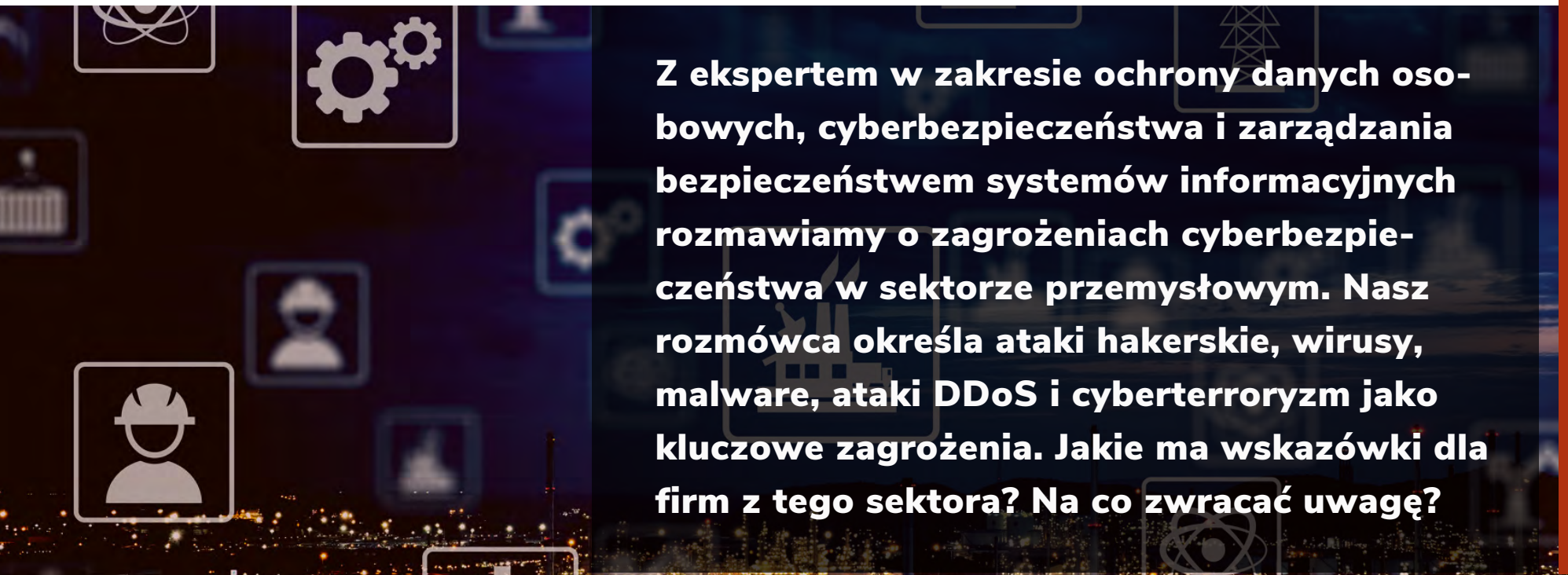
PODSUMOWANIE

Cyberprzestrzeń z uwagi na szybki rozwój jest wykorzystywana w wielu celach. Mając na uwadze katalog usług, to znajduje się w niej ogromna ilość danych, nie tylko danych osobowych. Mowa tutaj często o informacjach prawnie chronionych (tajemnice przedsiębiorstwa). Co za tym idzie, jest wiele osób zainteresowanych posiadaniem tej wiedzy, w celu wykorzystywania do własnych celów. Jak widać wiele jest możliwości, co do podwyższania poziomu bezpieczeństwa danych w organizacji. Nie można zapominać, że proces ten jest ciągły i powinien on być weryfikowany i usprawniany w miarę potrzeb.


Organizujesz wydarzenie związane
z bezpieczeństwem w firmie
lub nowymi technologiami?
Sprawdź ofertę
PATRONATU
MEDIALNEGO
SECURITY MAGAZINE
Napisz do nas:
redakcja@securitymagazine.pl

JAK ZADBAĆ O CYBER-BEZPIECZEŃSTWO W PRZEMYŚLE?

Dariusz Chmielewski
Aegis Security Sp. z o.o.



Z ekspertem w zakresie ochrony danych osobowych, cyberbezpieczeństwa i zarządzania bezpieczeństwem systemów informacyjnych rozmawiamy o zagrożeniach cyberbezpieczeństwa w sektorze przemysłowym. Nasz rozmówca określa ataki hakerskie, wirusy, malware, ataki DDoS i cyberterroryzm jako kluczowe zagrożenia. Jakie ma wskazówki dla firm z tego sektora? Na co zwracać uwagę?

Jakie są najważniejsze zagrożenia dla systemów przemysłowych w zakresie cyberbezpieczeństwa?

Dariusz Chmielewski: Systemy przemysłowe (ang. Operational Technology – OT) stanowią specyficzna grupę zasobów informatycznych, które są w szczególny sposób narażone na ataki cybernetyczne. Systemy te są podłączone do urządzeń przemysłowych i bezpośrednio sterują ich pracą. Złożoność procesów produkcyjnych jest coraz większa, a sieci informatyczne odgrywają kluczową rolę w zarządzaniu tymi procesami. Istnieje wiele rodzajów ataków, które mogą wystąpić na systemy przemysłowe, takie jak SCADA (ang. Supervisory Control and Data Acquisition) lub systemy sterowania.

Najważniejsze zagrożenia dla systemów przemysłowych to ataki hakerskie, podczas których hakerzy próbują uzyskać nieautoryzowany dostęp do systemów przemysłowych, aby dokonać kradzieży poufnych informacji lub zniszczyć dane. Wirusy i złośliwe oprogramowanie (malware), które może zostać wprowadzone do systemów przemysłowych, powodując uszkodzenia w systemie lub kradzież danych. Ataki DDoS (ang. Distributed Denial of Service) polegające na przeładowaniu systemu zapytaniami, które pochodzą z wielu różnych źródeł mające na celu zablokowanie dostępu do systemów przemysłowych, przez co uniemożliwiają ich normalne funkcjonowanie, a także cyberterroryzm, czyli ataki cybernetyczne mogące być również stosowane w celu dokona-

nia zamachów terrorystycznych, które mogą mieć poważne konsekwencje zarówno dla bezpieczeństwa ludzi i infrastruktury przemysłowej. Ważne jest, aby pamiętać, że zagrożenia te są stale zmieniające się i ewoluujące, więc należy być w stałej gotowości do przeciwdziałania nowym zagrożeniom.

Jakie są najważniejsze sposoby ochrony systemów przemysłowych przed atakami i zagrożeniami związanymi z cyberbezpieczeństwem?

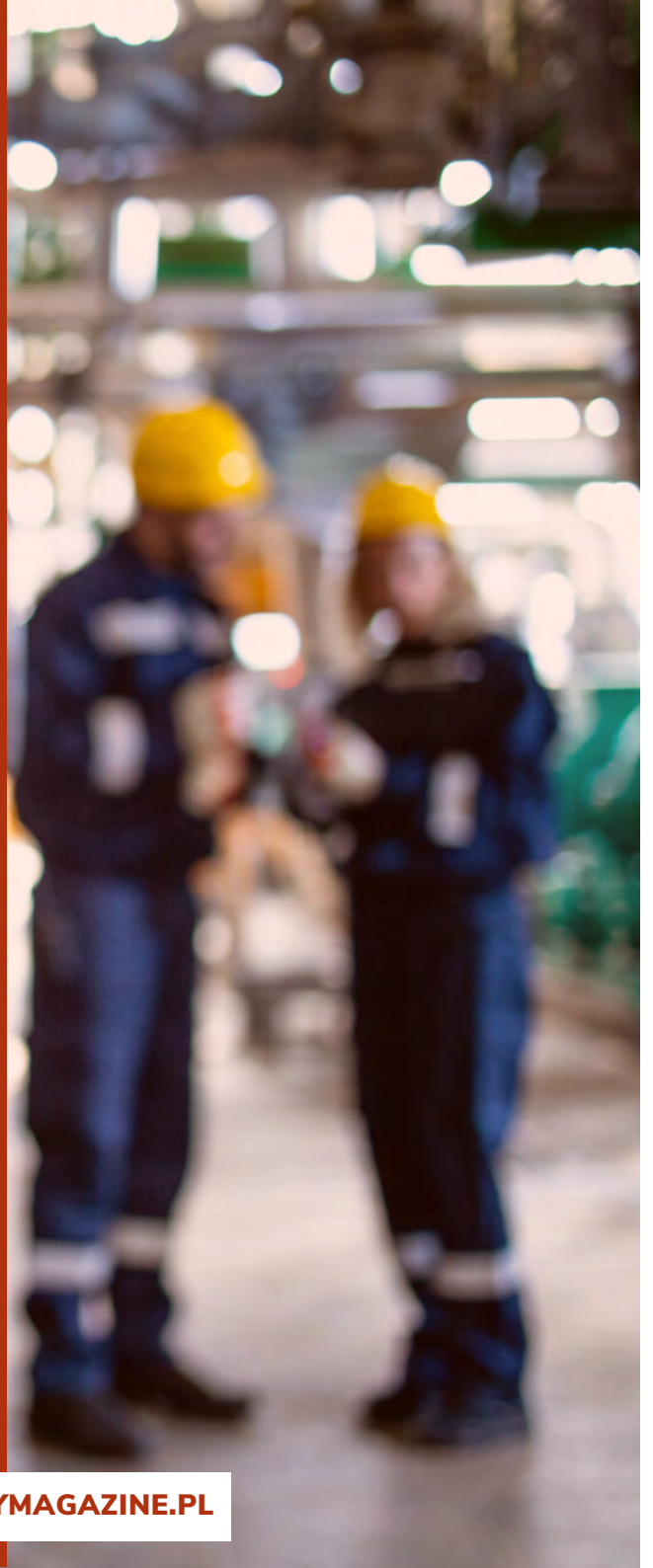
D.C.: Należy zastosować odpowiednie oprogramowanie zabezpieczające, czyli wdrożyć odpowiednie narzędzia do wykrywania i eliminowania zagrożeń związanych z cyberbezpieczeństwem, takie jak antywirusy, zapory ogniowe (firewall), systemy wykrywania intruzów (IDS) czy systemy zapobiegające utracie danych (DLP). Konieczne jest systematyczne aktualizowanie oprogramowania w celu usunięcia znanych podatności i uzupełnienia luk w systemach bezpieczeństwa.

Częstym problemem charakterystycznym dla systemów przemysłowych, jest to, że często wykorzystują one stare wersje oprogramowania, które albo nie są aktualizowane na bieżąco, albo wręcz takie aktualizacje nie są dostępne ze względu na zakończenie wsparcia oprogramowania przez producenta (np. stosowany na dużą skalę w systemach przemysłowych system operacyjny Windows XP, który stracił wsparcie producenta już w 2014 roku).

Nie należy zapominać o szkoleniach pracowników. Ważne jest, aby pracownicy byli świadomi zagrożeń związanych z cyberbezpieczeństwem i wiedzieli, jak rozpoznawać podejrzane zachowania lub ataki hakerskie. Należy również zwracać uwagę na to, aby nie udostępniali oni poufnych informacji lub haseł osobom trzecim. Wdrożenie odpowiedniej dokumentacji w tym polityk i procedur bezpieczeństwa, które określają wymagania dotyczące bezpieczeństwa systemów przemysłowych, takie jak wymagania dotyczące haseł, kontroli dostępu i monitorowania sieci.

Bardzo dużo zakładów przemysłowych stosuje słabe uwierzytelnienia i domyślne hasła. Ważna jest kryptografia, która powinna być stosowana do zabezpieczenia danych i zapewnienia poufności i integralności przesyłanych informacji w systemach przemysłowych.

Konieczne jest również regularne tworzenie bezpie-



cznych kopii zapasowych danych, aby zapobiec ich utracie w przypadku ataku lub awarii systemu.

Koszt utraty ważnych informacji może być znacznie wyższy niż koszt wykonania regularnej kopii zapasowej. Dlatego warto stosować zasadę 3-2-1 backupu i regularnie wykonywać kopie zapasowe swoich danych.

Zabezpieczać je hasłami i oprogramowaniem antywirusowym. Przypominam, iż zasada 3-2-1 to standardowy sposób tworzenia kopii zapasowych, który zapewnia ochronę danych przed utratą, uszkodzeniem lub kradzieżą. Zgodnie z tą zasadą, należy mieć co najmniej trzy kopie danych, przechowywane na dwóch różnych nośnikach. Jedna z tych kopii powinna być przechowywana poza siedzibą firmy.

Jakie są przykłady ataków na systemy przemysłowe, które miały miejsce na świecie?

D.C.: Zacznę może od malware Stuxnet, który był jeden z najbardziej znanych ataków złośliwego oprogramowania na systemy przemysłowe. Miał on miejsce w 2010 roku i był ukierunkowany na systemy sterowania przemysłowego w irańskiej elektrowni jądrowej. Stuxnet został zaprojektowany w taki sposób, aby infekować komputery i systemy sterowania przemysłowego przez wykorzystanie podatności w oprogramowaniu.

W 2017 roku miał miejsce atak złośliwego oprogramowania Triton i był skierowany na systemy kontroli bezpieczeństwa w elektrowni gazowej

w Arabii Saudyjskiej.

Atak ten miał na celu zakłócenie procesu kontroli bezpieczeństwa, co mogło doprowadzić do katastrofalnych konsekwencji. Industroyer to zaawansowany malware, który został użyty w ataku na elektrownię w Ukrainie w 2016 roku. Atak ten spowodował przerwy w dostawach energii elektrycznej i wody dla 225 tys. ludzi.

NotPetya to złośliwe oprogramowanie, które zo-stało użyte w ataku na firmy przemysłowe na Ukrainie w 2017 roku, a następnie rozprzestrzeniło się na cały świat. Atak ten miał na celu zablokowanie dostępu do danych i systemów komputerowych. Atak Dragonfly w 2011 roku był skierowany na systemy przemysłowe w sektorze energetycznym w USA i Europie. Atak ten miał na celu pozyskanie poufnych informacji i naruszenie bezpieczeństwa krytycznych systemów przemysłowych.

A jak to wygląda w Polsce?

D.C.: Jeśli chodzi o nasz kraj i ataki na polskie systemy przemysłowe to wymienię atak ransomware, który był w 2018 roku na jedną z elektrowni, który spowodował przerwę w pracy systemów informatycznych. Atak nie wpłynął na bezpieczeństwo elektrowni, ale zmusił do wstrzymania niektórych systemów, co wywołało zakłócenia w jej pracy.

Inny atak to ten na sieć ciepłowniczą w 2016 roku. Sieć ciepłowni-

cza była atakowana przez hakerów, którzy chcieli przejąć kontrolę nad systemem sterującym i zmienić ustawienia temperatury.

Atak ten został na szczęście ograniczony i nie wpłynął na bezpieczeństwo pracy sieci ciepłowniczej. Kolejny atak przeprowadziła w 2019 roku znana grupa hakerów na jednego z liderów branży energetycznej, kradnąc poufne informacje dotyczące kontraktów i dostawców. Te ataki pokazują, że polskie systemy przemysłowe są również narażone na zagrożenia związane z cyberbezpieczeństwem. Dlatego ważne jest, aby firmy działające w sektorze przemysłowym w Polsce dbały o bezpieczeństwo swoich systemów OT.

Jakie standardy cyberbezpieczeństwa dedykowane są systemom przemysłowym?

D.C.: Normy ISA/IEC 62443 stanowią propozycję zintegrowanego środowiska, które odpowiada na obecnie znane oraz prawdopodobne rodzaje podatności w układach sterowania systemami automatyki przemysłowej. Norma definiuje szereg wymagań dotyczących bezpieczeństwa systemów przemysłowych, w tym klasyfikację ryzyka, zarządzanie ryzykiem, architekturę bezpieczeństwa, zarządzanie zdarzeniami bezpieczeństwa i inne.

Kolejnym standardem jest grupa norm EN-IEC 61508 dotycząca niezawodności sprzętu elektrycznego i elektronicznego związanych z bezpieczeństwem. Wdrożenie tych standardów zapewnia ochronę przed cyberatakami.

Ciągłość działania jest kluczowym zagadnieniem dla bezpiecznego i niezawodnego funkcjonowania firm z branży przemysłowej. Pomocą w zarządzaniu ciągłością działania jest norma ISO 22301. Przedsiębiorstwa powinny przygotować plany awaryjne na wypadek nagłych sytuacji, takich jak awarie sprzętu czy cyberataki. Plany te powinny określać procedury postępowania oraz role i odpowiedzialności pracowników w czasie awarii.

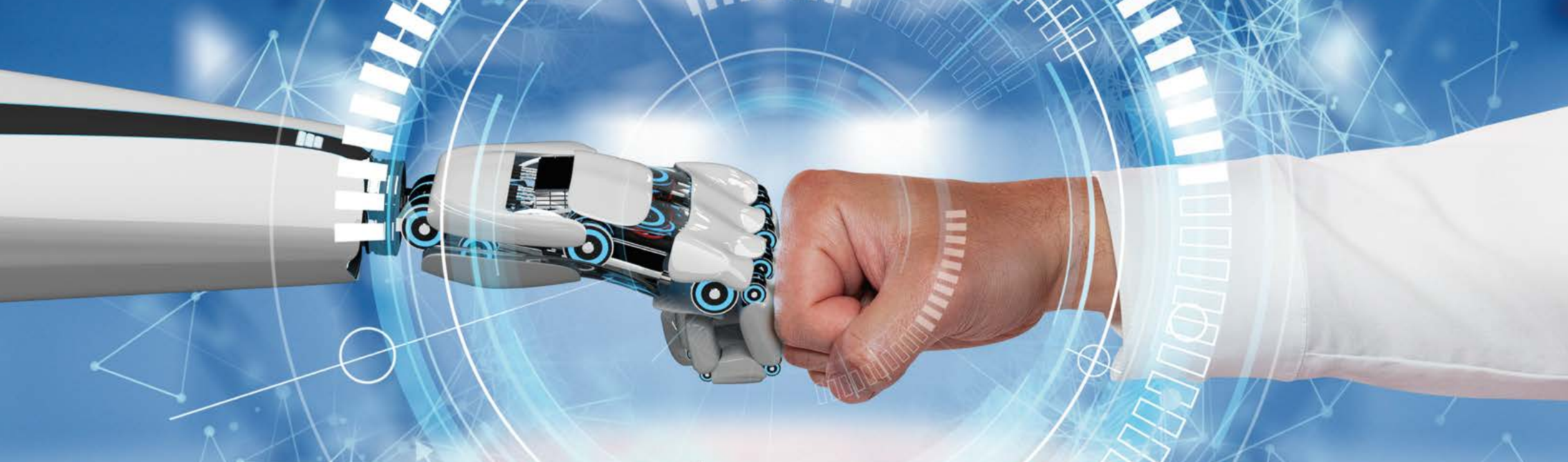
Jakie systemy pomogą w ochronie sieci przemysłowych?

D.C.: Aby nie doprowadzać do konieczności uruchomienia planów awaryjnych warto wyposażyć się w najnowocześniejsze rozwiązania zapewniające ciągłość działania i odtwarzania awaryjnego. Rozwiązania takie bazują na zabezpieczeniu kopii systemów w chmurach obliczeniowych i umożli-

wiają uruchamianie środowisk na żądanie. Dodatkowo zabezpieczają wykonywane kopie bezpieczeństwa przed ich zaszyfrowaniem szkodliwym oprogramowaniem – ransomware. Innym ważnym rozwiązaniem jest zastosowanie zabezpieczenia punktów styku z siecią oraz uruchomienie systemów detekcji. Systemy IDS (ang. Intrusion Detection System) analizują ruch sieciowy, aby wykryć podejrzane działania i ostrzec przed potencjalnymi atakami. Z kolei systemy NDR (ang. Network Detection and Response) posiadają funkcje, które umożliwiają wykrywanie i analizowanie zagrożeń, nieprawidłowych zachowań i ryzykownych aktywności w całej sieci, w tym poprzez analizę ruchu sieciowego oraz monitorowanie komunikacji w czasie rzeczywistym.

Systemy przemysłowe powinny również być regularnie aktualizowane, aby zagwarantować ochronę przed najnowszymi zagrożeniami. Regularne testy penetracyjne i skanowanie podatności mogą znacząco przyczynić się do bezpieczeństwa i zapewnić ciągłość działania systemów przemysłowych.

Dziękuję za rozmowę.



engave

Razem zbudujemy
TWOJĄ FIRMĘ
jutra

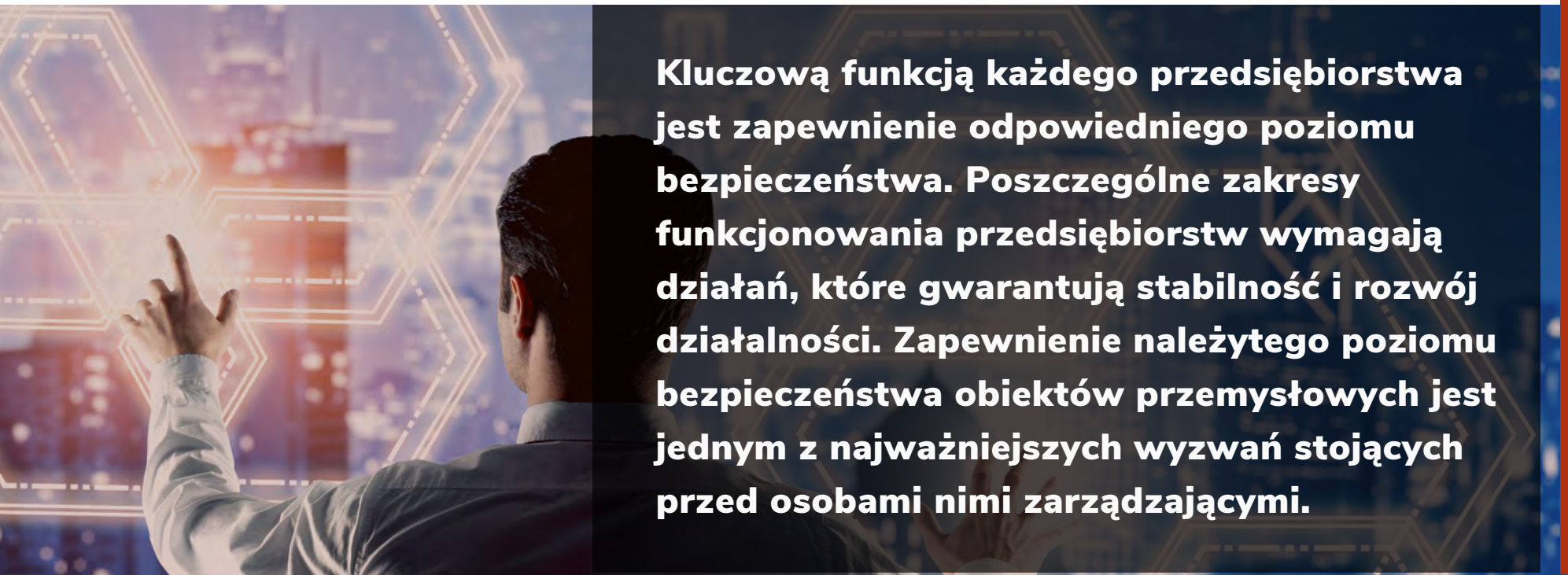
Sprawdź

APLIKACJE I SYSTEMY DLA BIZNESU | USŁUGI DLA IT | DORADZTWO BIZNESOWE

#PlayTechTogether

ZARZĄDZANIE BEZPIECZEŃSTWEM JAKO PROGRAM W UJĘCIU PROJEKTOWYM

Dariusz Mrugowski
ENGAVE S.A.



Kluczową funkcją każdego przedsiębiorstwa jest zapewnienie odpowiedniego poziomu bezpieczeństwa. Poszczególne zakresy funkcjonowania przedsiębiorstw wymagają działań, które gwarantują stabilność i rozwój działalności. Zapewnienie należytego poziomu bezpieczeństwa obiektów przemysłowych jest jednym z najważniejszych wyzwań stojących przed osobami nimi zarządzającymi.

DEFINICJE I ISTOTA

Od sprawności reagowania na dynamicznie zachodzące zmiany oraz podejmowania działań w zakresie zapewnienia odpowiedniego poziomu bezpieczeństwa jak również stosownych procedur zależy prawidłowe funkcjonowanie danej organizacji a czasem nawet jej istnienie. Czym więc jest bezpieczeństwo i jak sprawić, aby jego poziom był optymalny w dynamicznie zmieniającej się rzeczywistości?

Rozważania nad pojęciem, definicją i istotą bezpieczeństwa należy rozpocząć od stwierdzenia, że mają one tak długą historię, jak długa jest historia ludzkości. Człowiek od początku swojego istnienia dążył do przetrwania, a co za tym idzie do zapewnienia sobie niezbędnego minimum bezpieczeństwa. Można wyróżnić wiele definicji bezpieczeństwa, a co najistotniejsze, każda z nich jest prawidłowa, gdyż wspólnie odnoszą się one do ogólnego stanu poczucia braku zagrożeń. Wszystkie definicje bezpieczeństwa mają wspólny mianownik — jest ono stanem istniejącym w danym momencie. Stan ten nie jest stały ani dany raz na zawsze – tak jak pokój.

REALIZACJA CELÓW STRATEGICZNYCH

XXI wiek przynosi coraz to nowsze rodzaje zagrożeń - zarówno o znaczeniu globalnym, jak i lokalnym. W dobie powszechnego dostępu do nowoczesnych technologii oraz ich dynamicznego rozwoju obecnie zagrożenia, które jeszcze kilka lat temu zdawały się być pieśnią przyszłości, są coraz bardziej realne.

Obecnie zarówno wiele firm prywatnych, jak i instytucji państwowych stara się zapanować nad wyzwaniami i zagrożeniami poprzez wdrażanie systemów oraz rozwiązań pozwalających na zarządzanie ryzykiem np. wdrażając standardy

ISO. Przedsiębiorstwa mające dobrze opracowaną strategię zarządzania ryzykiem o wiele lepiej są w stanie chronić siebie i skutecznie skalować swoją działalność.

Dążenie przedsiębiorstwa do utrzymania odpowiedniego poziomu bezpieczeństwa jest długotrwałym i wielofalowym procesem, jednak w wielu przypadkach przejawia się ono przez tworzenie i zarządzanie projektami, które w swej naturze mogą mieć charakter programu. Według definicji przyjętej w standardach IPMA program to zbiór określonych i powiązanych ze sobą wzajemnie projektów i innych zadań, które wspólnie realizują określone cele operacyjne w ramach jednej nadrzędnej strategii. Już z samej definicji wynika konieczności posiadania określonych celów operacyjnych, których realizacja przybliża dane przedsiębiorstwo do osiągnięcia celów strategicznych. W przypadku obiektów przemysłowych, bezpieczeństwo zazwyczaj realizowane jest dwojako poprzez nieustający proces monitorowania zagrożeń i zdarzeń jak również równolegle realizowane projekty mające na celu rozwój systemów bezpieczeństwa.

Powyższe zadania często realizowane są równolegle, jednak w wielu przypadkach nie są one ze sobą w żaden sposób powiązane co skutkować może generowaniem wyższych kosztów realizacji prowadzonych zadań. Realizowanie projektów bez jasno sprecyzowanych celów jest jak prowadzenie samochodu z zawiązanymi oczami — być może uda się dotrzeć do celu, jednakże będzie to okupione bólem i licz-

nymi ofiarami w ludziach.

REALIZOWANIE PLANOWANYCH DZIAŁAŃ W RAMACH JEDNEGO PROGRAMU

Optymalną formą zarządzania bezpieczeństwem obiektów przemysłowych, jest realizowanie planowanych działań w ramach jednego programu - spójnego z obraną strategią bezpieczeństwa.

Można w tym miejscu wymieniać wiele działań o znaczeniu strategicznym dla obiektów przemysłowych, jednakże wszystkie zmierzają w tym samym celu, tj. zapewnieniu przedsiębiorstwu optymalnych warunków do wzrostu poprzez minimalizację ryzyka wynikającego z możliwości zaistnienia zdarzeń nieprzewidywalnych. Jak więc reagować w chwili wystąpienia zdarzenia niemożliwego do przewidzenia?

Przede wszystkim należy wspierać swoje działania doświadczeniem osób o odpowiednich kompetencjach, ponieważ jeśli nie można liczyć na profesjonalne wsparcie to dynamika zdarzeń kryzysowych, może okazać się bolesnym lub kosztownym w skutkach przeżyciem dla firmy.

Niestety, nie wszystkie firmy mogą pozwolić sobie na zatrudnianie profesjonalistów w każdej dziedzinie, w której, stwierdzono możliwość zaistnienia zdarzeń mogących mieć negatywne skutki dla funkcjonowania obiektu przemysłowego.

Wynika to zarówno z faktu ograniczonej ilości specjalistów jak również kosztów ich zatrudnienia. Alternatywnym rozwiązaniem jest korzystanie z usług firm zewnętrznych, posiadających odpowiednio bogate zaplecze specjalizacyjne oraz stosowną gamę rozwiązań technologicznych i infrastrukturalnych.

AGILE, KANBAN

Zapewnienie optymalnego poziomu bezpieczeństwa obiektów przemysłowych i infrastruktury IT jest tematem wielowymiarowym, wymagającym ciągłego doskonalenia jak również działań na podstawie odpowiednio dobrane metodyki i procedur. Dlatego też przy dynamicznie zmieniającej się rzeczywistości społeczno-politycznej, globalnej oraz technologi-

cznej, niezbędne jest zwinne reagowanie na zmiany. W wielu przypadkach możliwe jest stosowanie metodyk zwinnych w zarządzaniu bezpieczeństwem — takich jak np. Agile lub Kanban.

Zwinne postępowanie w tematyce związanej z bezpieczeństwem łączy się z koniecznością dynamicznych działań wymagających oraz szybkich i skutecznych rozwiązań. Największym wyzwaniem w każdej kwestii dotyczącej bezpieczeństwa zawsze jest czas reakcji i podjęcia stosownych działań.

Posiadając umowy SLA z operatorem infrastruktury lub usług, przedsiębiorstwo może zapewnić sobie swego rodzaju gwarancję na dostępność do kluczowych usług, takich jak np. backup danych, utrzymanie i zarządzanie infrastrukturą, utrzymanie systemów wykorzystywanych do pracy zdalnej, monitorowanie sieci, utrzymanie systemów zarządzania bezpieczeństwem informacji (Information Security Management System, ISMS).

W nowoczesnych systemach zabezpieczeń, stosowanych w obiektach przemysłowych, wykorzystuje się technologię IP oraz PoE, co często pozwala obniżyć koszty inwestycji. Jednak często zapomina się o pozostałych elementach infrastruktury, które mogą również generować ryzyko dla bezpieczeństwa. Wiele inwestycji realizowanych jest w oparciu o cenę, a nie o jakość czy bezpieczeństwo, co jest w mojej ocenie, błędnym podejściem. Bezpieczeństwo zawsze będzie wyłącznie kosztem dla przedsiębiorstwa, jednak można rozsądnie ten koszt optymalizować.

Dobrym przykładem może tu być wykorzystywanie urządzeń odnowio-nych w klasie A+ lub A, wraz z gwarancją dostawcy. Jest to zarówno ekonomiczne jak i ekologiczne, ponieważ wykorzystując ponownie urządzenia klasy enterprice (np. serwery, switche zarządzalne, itp.) można ograniczyć koszty inwestycji zachowując wysoką jakość urządzeń.

W dobie coraz bardziej skomplikowanych zagrożeń, jakie stają przed bezpieczeństwem obiektów przemysłowych i infrastruktury IT, wykorzystanie nowoczesnych technologii (takich jak backup danych, usługi Cloud, disaster recovery czy outsourcing usług IT) oraz podejścia zwinnego w projektowaniu i zarządzaniu bezpieczeństwem, staje się niezbędne. Dzięki temu organizacje mogą zwiększyć swoją odporność na zagrożenia oraz szybciej i sprawniej reagować na ewentualne incydenty.

Warto również zauważyć, że program zarządzania bezpieczeństwem w ujęciu projektowym może przynieść wiele korzyści, dzięki czemu organizacje mogą skutecznie zidentyfikować zagrożenia i podjąć odpowiednie działania, aby minimalizować ich wpływ. W dalszej kolejności monitorowanie skuteczności działań pozwala na ciągłe doskonalenie procesów i reagowanie na zmieniające się warunki.

KLUCZOWA ROLA BEZPIECZEŃSTWA W ROZWOJU ORGANIZACJI

Podsumowując, w dzisiejszych czasach bezpieczeństwo obiektów przemysłowych i infrastruktury IT jest jednym z kluczowych czynników, które wpływają na rozwój organizacji. Strategiczne podejście do kwestii związanych z bezpieczeństwem jest tak szerokie, że przekrojowo dotyka każdego aspektu funkcjonowania firmy, a co za tym idzie również jej pracowników. To właśnie pracownicy są kluczowym zasobem w sytuacji kryzysowej, dlatego w pierwszej kolejności należy zadbać o budowanie świadomości w zakresie ryzyk i prawidłowego postępowania.

DOŁĄCZ DO GRONA EKSPERTÓW "SECURITY MAGAZINE"

EKSPERCI WYDANIA

DANIEL KAMIŃSKI
Właściciel
AlertControl

Pasjonat nowoczesnych usług monitoringu alarmów oraz zdalnie zarządzanych systemów bezpieczeństwa. Regularnie śledzi trendy branżowe, bierze udział w międzynarodowych targach i utrzymuje kontakt z wiodącymi producentami rozwiązań bezpieczeństwa. Swoją wiedzą dzieli się na łamach czasopism branżowych, konferencji oraz szkoleń.

KRZYSZTOF ANDRIAN
Prezes Zarządu
Concept Data

Na rynku ICT od ponad 20 lat. Wcześniej zarządzał zespołami i projektami oraz realizował strategie sprzedaży dla m.in.: Softbank, IBM Polska, Tieto Poland. W latach 2011-2014 zbudował i kierował nowym działem usług IT Contracting w Hays Polska.

DOMINIK ROZDZIAŁOWSKI
Dyrektor
Departament Cyberbezpieczeństwa
Ministerstwa Obrony Narodowej

Dyrektor Departamentu Cyberbezpieczeństwa Ministerstwa Obrony Narodowej. W latach 2016-2018 - dyrektor Biura do Walki z Cyberprzestępczością KGP w Warszawie. Wykładowca akademicki w SGH, Akademii WSB Dąbrowa Górnicza, Krajowej Szkole Sądownictwa i Prokuratury. Biegły sądowy z zakresu m.in. informatyki i przestępczości komputerowej.

TOMASZ GRZELAK
CEO
Stay Safe Poland

Security manager z wieloletnim doświadczeniem w międzynarodowym biznesie. Specjalizuje się w obszarze handlu i logistyki, z osiągnięciami w innowacyjnych projektach technologicznych i organizacyjnych. Specjalista w zakresie negocjacji, zarządzania oraz bezpieczeństwa fizycznego i korporacyjnego.

EKSPERCI WYDANIA

MAGDALENA CELEBAN
Właściciel
ODO Szkolenia

Wykładowca, szkoleniowiec, praktyk z zakresu ochrony danych osobowych. Pełni funkcję inspektora ochrony danych zarówno w podmiotach publicznych, jak również w sektorze prywatnym. Z wieloletnim doświadczeniem z zakresu bezpieczeństwa przetwarzania danych osobowych.

JAKUB GORAL
Architekt bezpieczeństwa
Energy Logserver

Ekspert w zakresie systemów zarządzania informacjami i zdarzeniami bezpieczeństwa informatycznego. Odpowiada za strategię wdrożenia i rozwój produktu Energy SOAR. Ma szerokie kompetencje w obszarze projektowania i wdrażania systemów SIEM oraz zarządzania podatnościami.

ALEKSANDRA KORNECKA
Inżynier ds. cyberbezpieczeństwa

Inżynier ds. cyberbezpieczeństwa (security awareness, SecOps, CloudSec, SSDLC), lubiąca pracować i z maszynami, i z ludźmi. W IT od 2013 roku (testowanie, konsulting jakości, cyberbezpieczeństwo), magister kognitywistyki, prelegentka konferencji oraz meetupów w Polsce i zagranicą, mentorka, sprinterka.

DARIUSZ CHMIELEWSKI
Prezes Zarządu
Aegis Security Sp. z o.o.

Ekspert z zakresu ochrony danych osobowych, cyberbezpieczeństwa oraz zarządzania bezpieczeństwem systemów informacyjnych. Audytor wiodący systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001. Zarządzał licznymi projektami z obszaru bezpieczeństwa IT.

EKSPERCI WYDANIA

MATEUSZ JAKUBIK
Oficer Bezpieczeństwa Informacji
iSecure Sp. z o.o.

Doktorant na Wydziale Prawa i Administracji UJ w Krakowie, tam zajmuje się tematyką ODO oraz prywatności. Bierze czynny udział w pracach podgrup ds. ram polityki, ds. badań, innowacyjności i wdrożeń oraz ds. umiejętności cyfrowych w zespole eksperckim Ministerstwa Cyfryzacji ds. programu działań w zakresie AI.

DARIUSZ MRUGOWSKI
Head of Product Development
ENGAVE S.A.

Ekspert ds. bezpieczeństwa obiektów przemysłowych oraz zarządzania projektami, posiadający ponad 10-letnie doświadczenie w zarządzaniu projektami inwestycyjnymi o łącznej wartości 60+ mln PLN netto.

KATALOG FIRM

AEGIS
SECURITY

AEGIS SECURITY SP. Z O.O.

ul. Cybernetyki 19B
02-677 Warszawa, Polska

Dane kontaktowe
+48 600 825 051
kontakt@aegissecurity.pl

Specjalizacje

cyberbezpieczeństwo | socjotechnika | audyty | testy penetracyjne | compliance | akredytacja POZ | socjotechnika | zarządzanie IT | RODO

Jesteśmy grupą specjalistów działających na rynku bezpieczeństwa informacji od wielu lat. Od początku działalności Spółka zakładała stworzenie miejsca, gdzie klienci będą mogli odnaleźć odpowiedzi na najtrudniejsze pytania z zakresu cyberbezpieczeństwa oraz bezpieczeństwa informacji.

Dbamy o to, aby współpracujący z nami klienci, pozostawali bezpieczni oraz świadomi rozwoju zagrożeń wynikających z pracy w cyberprzestrzeni, która stała się nieodłączną częścią funkcjonowania każdego przedsiębiorstwa.

Oferujemy kompleksowe rozwiązania IT dla biznesu, audyty bezpieczeństwa, testy penetracyjne i socjotechniczne, doradztwo oraz szkolenia z zakresu cyberbezpieczeństwa, a także przygotowanie do certyfikacji systemów zarządzania oraz usługi w zakresie ochrony danych osobowych.

Jesteśmy członkiem klastra #CyberMadeInPoland, którego celem jest kształtowanie i rozwój bezpiecznej cyberprzestrzeni w Polsce. Należymy do Mazowieckiego Kluczowego Klastra ICT, w którego szeregach budujemy świadomość cyber na terenie kraju i we współpracy z zagranicznymi organizacjami.

Dobierając rozwiązania do portfolio naszych usług, wsłuchujemy się w potrzeby naszych klientów. Poniżej znajdziecie Państwo listę usług skategoryzowaną według poszczególnych obszarów zabezpieczeń uznawanych za najważniejsze dla naszych klientów.

- Testowanie sieci i aplikacji
- Zarządzanie incydentami i podatnościami
- Bezpieczeństwo brzegu sieci
- Klasyfikacja i kontrola aktywów
- Ochrona antywirusowa
- Ochrona przed wyciekami danych
- Zarządzanie tożsamością i dostępem
- Platforma cyberbezpieczeństwa
- Weryfikacja procedur i pracowników
- Wdrażanie systemów zarządzania
- Ochrona danych osobowych
- Bezpieczeństwo chmury
- Zapewnienie zgodności z regulacjami
- Akredytacja POZ

KATALOG FIRM

ALERTCONTROL

Daniel Kamiński
ul. Przyrodnicza 7E
05-126 Michałów-Grabina

Dane kontaktowe
+ 48 784 646 386
alertcontrol@alertcontrol.pl

Specjalizacje

doradztwo	procedury	nadajniki	aplikacje
audyty	alarmy	odbiorniki	projekty
szkolenia	monitoring	programy	wsparcie

AlertControl od 2010 roku zajmuje się doradztwem w zakresie systemów bezpieczeństwa technicznego. Głównymi klientami firmy są agencje ochrony oraz klienci korporacyjni. Naszą specjalnością są centra monitoringu oraz zdalnie zarządzane zabezpieczenia techniczne.

Specjalizujemy się w poszukiwaniu innowacyjnych rozwiązań z obszaru zabezpieczeń technicznych. Na bieżąco śledzimy rynki europejskie i światowe w poszukiwaniu rozwiązań, które dają naszym klientom przewagę konkurencyjną.

Bierzemy udział w konferencjach, międzynarodowych targach oraz utrzymujemy kontakt z producentami. Z tego względu możemy dzielić się zdobytym doświadczeniem z firmami, które nie mogą utrzymywać działów badań i rozwoju usług zabezpieczeń technicznych.

Kierujemy swoją ofertę do firm, które chcą ponosić mniejsze koszty na utrzymanie, modernizację i rozwój swoich systemów bezpieczeństwa. Posiadamy międzynarodowe doświadczenie w obszarze zabezpieczeń technicznych oraz wdrażamy innowacyjne rozwiązania w zakresie usług monitorowania.

Nasze usługi:

- **Doradztwo** – jest jedną z najczęściej oferowanych przez nas usług. Współpracują z nami firmy, które szukają rozwiązania niestandardowego problemu, po tym, gdy rekomendowane przez dostawców zabezpieczeń technicznych rozwiązania nie sprawdziły się.
- **Audyty** – Centrum Monitoringu na zgodność z normami PN-EN 50518 dotyczącymi konstrukcji, wyposażenia oraz procedur alarmowego centrum odbiorczego to nasza specjalność.
- **Kierowanie projektami** - częstą praktyką jest wynajmowanie naszej firmy do wykonania działań naprawczych wskazywanych w zaleceniach raportu z audytu.
- **Szkolenia** - jednym z elementów wdrożeń są szkolenia personelu. Prowadzimy zarówno szkolenia okresowe z procedur i regulaminów, jak również szkolenia produktowe.

KATALOG FIRM

CONCEPT DATA

CONCEPT DATA SA

Concept Data SA
ul. Piękna 24/26A
00-549 Warszawa

Dane kontaktowe
@ info@conceptdata.pl

Specjalizacje

- cyberbezpieczeństwo
- service desk
- cyfrowy dostęp
- ruch sieciowy
- automatyzacja
- polityki bezpieczeństwa

Concept Data to zespół konsultantów z wieloletnim doświadczeniem w zakresie rozwoju i wdrażania rozwiązań IT wspierających biznes. Naszym głównym celem jest pomaganie klientom w efektywnym oraz zgodnym ze standardami i wymogami bezpieczeństwa zarządzaniu przedsiębiorstwami.

Dla firm, z którymi współpracujemy, jesteśmy przede wszystkim partnerem. Słuchamy ich potrzeb, analizujemy sytuację, poznajemy kontekst biznesowy oraz oczekiwania technologiczne. Dopiero na podstawie tych informacji proponujemy odpowiednie usługi i produkty.

Wspólnie przechodzimy przez proces wdrożenia i związanych z nim zmian. Służymy naszym doświadczeniem i wiedzą, którą pogłębiamy każdego dnia, co potwierdzają liczne certyfikaty od naszych partnerów technologicznych.

Z pasją podążamy za trendami świata IT, dzięki czemu możemy spełnić oczekiwania różnych organizacji z wielu branż.

Realizujemy projekty dla klientów z wielu sektorów, m.in. bankowego, ubezpieczeniowego, telekomunikacyjnego, energetycznego i FMCG. Oferujemy rozwiązania IT największych i cenionych na świecie producentów (w tym SailPoint, CyberArk, Tufin, Gigamon, Imperva, BMC, Broadcom).

Doradzamy w ich wyborze, wdrażamy, integrujemy z funkcjonującymi już w firmach systemami, w końcu szkolimy oraz przeprowadzamy testy.

Specjalizujemy się głównie w obszarach:

- cyberbezpieczeństwa i zarządzania politykami bezpieczeństwa
- zarządzania tożsamością cyfrową i dostępem do kluczowych informacji przedsiębiorstwa
- automatyzacji procesów biznesowych
- zarządzania wydajnością w warstwie aplikacyjnej i bazodanowej
- ochroną kluczowych zasobów informacyjnych przedsiębiorstw.

KATALOG FIRM

engave

ENGAVE S.A.

ul. Czarodzieja 16
03-116 Warszawa, Polska

Dane kontaktowe
+48 22 863 13 90
@ biuro@engave.pl

www

Specjalizacje

chmura | backup | aplikacje | procesy | cyberbezpieczeństwo | outsourcing | szkolenia | integracja | digitalizacja | serwis | testy | architektura

Technologia zmieniła sposób konkurowania w biznesie i nie ma już miejsca dla firm, które nie są gotowe na cyfrową przemianę.

Jednak wiemy, że dla wielu przedsiębiorstw jest to cały czas zbyt trudne zadanie. Dlatego nie tylko oferujemy nasze wsparcie i pomoc w przeprowadzeniu Twojej firmy przez proces cyfrowej zmiany w sposób, który zagwarantuje ci bezpieczeństwo na najwyższym poziomie.

Jako lider w dziedzinie cyberbezpieczeństwa, oferujemy zakres usług i rozwiązań, które pomagają chronić przed zagrożeniami związanymi z atakami cybernetycznymi. Wspieramy naszych klientów w ochronie danych osobowych, systemów transakcyjnych oraz infrastruktury IT.

Dzięki naszemu doświadczeniu i wiedzy, pomogliśmy wielu klientom z różnych branż. Są to między innymi: ZUS, NFZ, Wody Polskie, Hubix, Man Truck & Bus.

Nasze rozwiązania obejmują backup as a service (BaaS), archiwizację, a także rozwiązania z zakresu disaster recovery. Nasze usługi backupu i archiwizacji umożliwiają klientom utworzenie kopii zapasowych danych w czasie rzeczywistym i archiwizację wiadomości e-mail.

W przypadku wystąpienia sytuacji awaryjnej, nasze rozwiązania disaster recovery pomagają przywrócić systemy i dane do stanu sprzed awarii. To oznacza minimalizację strat wynikających z niedostępności danych lub systemów.

Jeśli szukasz rozwiązania, które pomaga w zapewnieniu bezpieczeństwa Twojej firmy, skontaktuj się z nami już dziś!

Jesteśmy gotowi pomóc w rozwiązaniu najtrudniejszych problemów, z jakimi możesz się spotkać.

KATALOG FIRM

ENERGY LOGSERVER

EMCA SOFTWARE SP. Z O.O.

ul. Wiejska 20
00-490 Warszawa, Polska

Dane kontaktowe
@ sales@energylogserver.com

Specjalizacje

cyberbezpieczeństwo | **cloud monitoring** | **APM** | **infrastruktura** | **compliance** | **log management**

EMCA Software Sp. z o.o. to dostawca oprogramowania z zakresu cyberbezpieczeństwa. Firma powstała w 2018 roku. Należy do grupy kapitałowej EMCA, obecnej na polskim rynku od ponad 30 lat. W swoich biurach w Warszawie i w Katowicach zatrudnia ponad 30 ekspertów, którzy w każdej chwili gotowi są służyć Klientom swoją wiedzą i doświadczeniem. Dzięki współpracy międzynarodowej z ponad 40 Partnerami swoje usługi świadczy na rynkach Europy, Azji, Afryki i Ameryki Północnej.

EMCA Software Sp. z o.o. tworzy rozwiązania, które w sposób efektywny oraz ekonomiczny identyfikują i przetwarzają cenne informacje. W portfolio firmy znajdują się najnowocześniejsze technologicznie, elastyczne i skalowalne, autorskie produkty opierające się na analizie danych, sztucznej inteligencji i automatyzacji procesów.

Są to:
Energy Logserver – nowatorski system, który dzięki komponentom SIEM, Log Management i Network Probe umożliwia centralizację zdarzeń w systemie informatycznym i zapewnia precyzyjne przechowywanie, analizowanie i zarządzanie danymi.

Energy SOAR - zaawansowana, biznesowa platforma, która pozwala szybko, a także efektywne reagować na zdarzenia w systemach poprzez identyfikację, badanie i automatyzację procesów biznesowych i informatycznych. Jej hiperautomatyzacja polega na zorganizowanym wykorzystaniu wielu technologii, narzędzi lub systemów.

Inwestycje w innowacyjność i rozwój wiedzy są sednem przedsięwzięć EMCA Software. W 2023 r. firma została beneficjentem programu badawczo-rozwojowego realizowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego, w ramach poddziałania „1.1.1. Badania przemysłowe i prace rozwojowe realizowane przez przedsiębiorstwa” Programu Inteligentny Rozwój. Projekt pn.: „Empowered AI in Energy Logserver – moduł AI do algorytmicznego odkrywania wiedzy zgromadzonej w zdarzeniach systemów informatycznych jako odpowiedź na wyzwania w dziedzinie Cybersecurity” był jednym z najwyżej ocenionych w ramach konkursu Szybka Ścieżka „Innowacje cyfrowe”.

KATALOG FIRM

STAY SAFE POLAND

Ul. Witkacego 25/87
95-100 Zgierz, Polska

Dane kontaktowe
+48 504 826 547
kontakt@staysafepoland.pl

Specjalizacje

- przeciwdziałanie kradzieżom
- kontrola dostępu
- zarządzanie bezpieczeństwem
- audyty
- CCTV
- bezpieczeństwo fizyczne
- zarządzanie kryzysowe
- systemy alarmowe
- bezpieczeństwo biznesu

Stay Safe Poland to firma konsultingowo-doradcza z wieloletnim doświadczeniem w dziedzinie bezpieczeństwa fizycznego. Zajmujemy się zwiększaniem bezpieczeństwa przy użyciu technologii, doradztwa i szkoleń. Oznacza to współpracę z gronem pracowników oraz pracę na poziomie strategicznym.

Dzięki naszym kompetencjom, autorskim metodom pracy, połączonymi z najlepszymi praktykami obowiązującymi w branży jesteśmy w stanie zapewnić kompleksowe rozwiązania dla Twojej firmy lub domu. To od naszych klientów zależy, jak będzie wyglądać nasza usługa. W zależności od ustaleń przyjmiemy rolę wykonawczą, doradczą lub szkoleniową. Zakres współpracy zostaje ustalony po analizie i określeniu potrzeb tak aby osiągnąć wspólny efekt, który sobie założyliśmy. Nasz zespół przeanalizuje zgłoszenie, problem i wskaże najlepsze rozwiązanie. Szeroki wachlarz naszych usług sprawia, iż Twoja firma lub dom będą należycie zabezpieczone w każdym aspekcie. Już nie musisz martwić się o straty, Ty zajmij się swoim biznesem, my zajmiemy się jego bezpieczeństwem.

Sprawdź w czym możemy Ci pomóc:

Audyty:
- Tajemniczy klient
- Tajemniczy pracownik
- Audyt bezpieczeństwa firmy
- Audyt bezpieczeństwa domu

Doradztwo
- Business Resilience
- Doradztwo biznesowe
- Zarządzanie kryzysowe
- Interim Security Manager
- Doradztwo zakupowe w domu
- Zarządzanie ciągłością działania

Szkolenia
- Bezpieczeństwo biznesu
- Systemy antykradzieżowe
- Kradzieże, sposoby postępowania

Zainteresowany współpracą? Umów na bezpłatną konsultację!

ZOBACZ WYDANIA

Wydanie 1/2022

POBIERZ

Wydanie 2/2022

POBIERZ

Wydanie 3/2022

POBIERZ

Wydanie 4/2022

POBIERZ

Wydanie 5/2022

POBIERZ

Wydanie 6/2022

POBIERZ

Wydanie 7/2022

POBIERZ

Wydanie 8/2022

POBIERZ

Wydanie 9/2022

POBIERZ

Wydanie 1(10)/2023

POBIERZ

Wydanie 2(11)/2023

POBIERZ

Wydanie 3(12)/2023

POBIERZ

WYDAWCA

Wydawca:

Rzetelna Grupa sp. z o.o.

al. Jana Pawła II 61 lok. 212
01-031 Warszawa

KRS 284065
NIP: 524-261-19-51
REGON: 141022624
Kapitał zakładowy: 50.000 zł
Sąd Rejonowy dla m. st. Warszawy I XIII Wydział Gospodarczy
Magazyn wpisany do sądowego Rejestru dzienników i czasopism.

Redaktor Naczelny: Rafał Stępniewski

Redaktor prowadzący: Monika Świetlińska
Redakcja: Damian Jemioło, Anna Petynia-Kawa
Projekt, skład i korekta: Monika Świetlińska

Współpraca i kontakt: redakcja@securitymagazine.pl

SECURITYMAGAZINE.PL