8(17)/2023

SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy

Narzędzia nie rozwiążą problemów bezpieczeństwa

Artur Bicki: AI, algorytmy i przyszłość cyberbezpieczeństwa

Cyberbezpieczeństwo i jego słabe ogniwo - człowiek

Web 3.0 zmienia postrzeganie bezpieczeństwa cyfrowych wartości

Struktury Bezpieczeństwa w przedsiębiorstwach Czy naprawdę są potrzebne?

SPIS TREŚCI

SZANOWNI PAŃSTWO,

bezpieczeństwo i cyberbezpieczeństwo są obecnie nie tylko zagadnieniami technologicznymi, ale kluczowymi elementami strategii biznesowej każdej firmy.

Inwestycja w wykształcenie personelu, implementację skutecznych strategii i narzędzi oraz promowanie kultury bezpieczeństwa jest nie tylko mądra, ale wręcz niezbędna. Edukacja i świadomość są podstawą zapobiegania, a odpowiednio dobrane narzędzia i procesy mogą stanowić skuteczną ochronę przed coraz bardziej wyrafinowanymi atakami.

Sierpniowe wydanie "Security Magazine" dostarcza Państwu wiedzy, narzędzi i ekspertów, którzy mogą pomóc w zrozumieniu i zarządzaniu tym złożonym aspektem współczesnego świata. Wspólnie z najlepszymi specjalistami w dziedzinie, zgłębiamy tematykę od kwestii prawnych, poprzez analizę najnowszych technologii, aż po ludzki aspekt cyberbezpieczeństwa.

Bez względu na to, czy jesteście Państwo ekspertami w dziedzinie bezpieczeństwa, czy właścicielami firm, którzy chcą zrozumieć, jak skutecznie chronić swoje organizacje, nasz magazyn oferuje coś dla każdego.

Zapraszam do lektury!

Rafał Stępniewski


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

SECFENSE ZWYCIĘZCĄ W ECCC ASSESS-2-MARKET

Secfense zaprezentował swoje rozwiązanie User Access Security Broker podczas wydarzenia Access-2-Market w Katowicach. Narzędzie zdobyło uznanie europejskiej publiczności oraz jury złożonego z ekspertów branży cybersecurity. Secfense zwyciężył w konkursie, dzięki czemu weźmie udział w prestiżowym finale ESCO's CISO Choice Award.

Access-2-Market łączy mniejszych dostawców rozwiązań z zakresu cybersecurity z potencjalnymi użytkownikami tych aplikacji – dyrektorami bezpieczeństwa informacji, liderami biznesu, ale też inwestorami. Wydarzenie jest okazją dla innowatorów na dotarcie do nowych odbiorców, a dla biznesu – na odkrycie nowatorskich narzędzi, które pomogą zabezpieczyć kluczowe zasoby informacyjne przedsiębiorstw.

Ważną częścią polskiej edycji wydarzenia był konkurs, w którym udział wzięło 11 firm. Miały one szansę zaprezentować swoje rozwiązania z obszaru cyberbezpieczeństwa podczas pięciominutowych wystąpień ocenianych przez publiczność i jury złożone z CISO. Zwycięzcami tegorocznego konkursu zostały dwie firmy, w tym Secfense.

Secfense zaprezentował User Access Security Broker, czyli rozwiązanie, które umożliwia ochronę całej organizacji przy wykorzystaniu uwierzytelniania wieloskładnikowego (MFA) opartego na FIDO2 lub dowolnej innej metodzie uwierzytelniania. Jego wdrożenie nie wymaga kodowania i umożliwia dodanie MFA do dowolnej aplikacji w ciągu kilku minut. Dzięki zastosowaniu tego narzędzia firmy eliminują ryzyka związane z phishingiem, socjotechniką i kradzieżą uwierzytelnień.

Zapraszamy do dzielenia się z nami newsami 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"

SECFENSE ZWYCIĘZCĄ W ECCC ASSESS-2-MARKET

- Całe wydarzenie Access-2-Market poświęcone było rozwiązaniom z zakresu zarządzania tożsamością i dostępem oraz zarządzania ryzykiem i oceny tego ryzyka. To dziś priorytetowe tematy dla CISO, którzy coraz częściej szukają nowych narzędzi, które wzmocnią bezpieczeństwo ich firm w tych obszarach. Cieszymy się, że nasze innowacyjne podejście do wdrażania FIDO MFA i transformacji do passwordless, czyli bezpiecznego uwierzytelniania bez użycia haseł, zostało docenione. Wiemy, jak ważne jest dziś dla przedsiębiorstw zapewnienie bezpiecznego dostępu do ich aplikacji – pracownikom, użytkownikom, kontraktorom czy dostawcom – mówi **Krzysztof Góźdź, Sales Manager w Secfense.** Dzięki zwycięstwu w Katowicach Secfense został nominowany do konkursu ECSO's CISO Choice Award. Drugą firmą, która będzie reprezentowała Polskę podczas finałów, jest CDeX.

- Udział w konkursie finałowym pozwoli nam dotrzeć z informacją o naszym rozwiązaniu do potencjalnych odbiorców z całego świata. Nasze narzędzie jest w pełni przygotowane do wdrożeń w krajach z różnych regionów. Od kilkunastu miesięcy aktywnie działamy na międzynarodowych rynkach, korzystając z wiedzy i doświadczenia naszych zagranicznych doradców. Dzięki ECSO's CISO Choice Award będziemy mieli okazję opowiedzieć o przyszłości bez haseł jeszcze szerszej publiczności – dodaje **Tomasz Kowalski, współzałożyciel i CEO Secfense.**

Wydarzenie zostało zorganizowane przez Europejskie Centrum Kompetencji Cyberbezpieczeństwa, polskie Krajowe Centrum Kompetencji Cyberbezpieczeństwa, CYBERSEC FORUM/EXPO 2023, Instytut Kościuszki i klaster CyberMadeInPoland, a wspierane było przez projekt Europejskiej Wspólnoty Cyberbezpieczeństwa.

Zapraszamy do dzielenia się z nami newsami 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"

PATRONAT
SECURITY MAGAZINE

24. KONFERENCJA BRANŻY OCHRONY

POTENCJAŁ I ROLA SEKTORA PRYWATNEGO W SYSTEMIE BEZPIECZEŃSTWA NARODOWEGO

ZAREJESTRUJ SIĘ TUTAJ

28-29 września, w Hotelu Windsor w Jachrance, odbędzie się 24. Konferencja Branży Ochrony. Wydarzenie jest nieodłącznym elementem kalendarza ekspertów, przedsiębiorców i instytucji związanych z sektorem ochrony i zabezpieczeń w Polsce.

Tegoroczne spotkanie „Potencjał i Rola Sektora Prywatnego w Systemie Bezpieczeństwa Narodowego" to okazja, by zapoznać się z wystąpieniami ekspertów, panelami dyskusyjnymi, prezentacjami produktów oraz networkingu.

PIO, jako lider w branży ochrony, zrzesza około 180 firm, współpracujących z podmiotami prywatnymi i publicznymi. Organizacja odgrywa kluczową rolę w realizacji zadań ochronnych w Polsce, szczególnie na poziomie lokalnym.

Głównymi obszarami omawianymi podczas konferencji będą technologie dla narodowego bezpieczeństwa, współpraca z mieszkańcami i partycypacja społeczna w tworzeniu bezpiecznych przestrzeni, bezpieczeństwo społeczności, cyberbezpieczeństwo, oraz rola i potencjał branży ochrony dla bezpieczeństwa narodowego.

Konferencja jest adresowana do przedstawicieli władz, ośrodków bezpieczeństwa, jak również jednostek odpowiedzialnych za bezpieczeństwo oraz zarządzanie kryzysowe w sektorze prywatnym. Celem spotkania jest pokazanie potencjału branży ochrony oraz jej znaczącego wpływu na bezpieczeństwo na szczeblu narodowym.

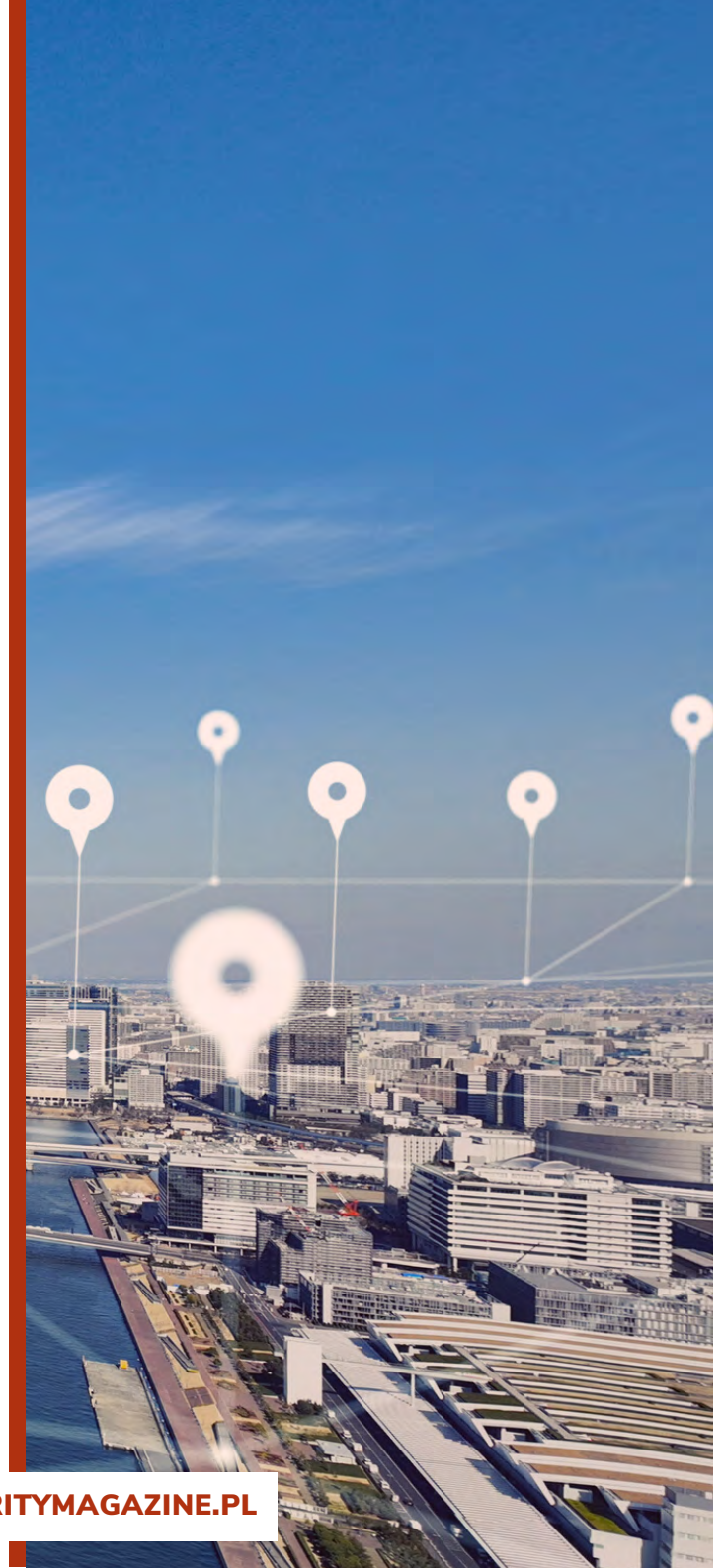
Partnerami konferencji są prestiżowe instytucje takie, jak Wojskowa Akademia Techniczna, Securex oraz Akademia WSB, a wsparcie merytoryczne zapewnia Centrum Prewencji Terrorystycznej, Agencja Bezpieczeństwa Wewnętrznego.

WIĘCEJ NA STRONIE PIO

CYBERBEZPIECZNY SAMORZĄD I NIS2 – SOC ROZWIĄZANIEM NIEDOBORU SPECJALISTÓW?

Łukasz Zajdel
Perceptus Sp z o. o.

Projekt Cyberbezpieczny Samorząd stał się faktem. Samorządy mogą wnioskować o środki na poprawę zabezpieczeń w oparciu o wskazówki, jakie przygotowało Ministerstwo dla kierowników i zespołów JST. Problem staje się o wiele poważniejszy z uwagi na sytuację niedoboru specjalistów w zakresie cyberbezpieczeństwa. Rozwój technologiczny w zakresie Security Operations Center (SOC) okazuje się najlepszym rozwiązaniem.



Projekt Cyberbezpieczny Samorząd ogłoszono 19 lipca. Samorządy mogą składać wnioski do 30 września, a realizacja projektu zakończy się 30 czerwca 2026 roku. W puli są prawie 2 mld zł.

To bardzo dobra wiadomość, ponieważ cyberataki na jednostki publiczne stały się w ostatnim roku niemal powszechne. Wojna w Ukrainie ma swoje odzwierciedlenie także w cyberprzestrzeni. Ataki na kluczową infrastrukturę informatyczną są coraz częstsze. Na pytanie, czy warto zbroić się w zabezpieczenia przeciw cyberatakom, odpowiedź może być tylko jedna: trzeba się zbroić.

Idea podniesienia poziomu zabezpieczeń zbiega się w czasie ze zbliżającym się wejściem w życie unijnego rozporządzenia NIS2, które reguluje szereg wymagań dotyczących cyberbezpieczeństwa.

JAKIE REGULACJE I DLA KOGO WPROWADZA NIS2?

Głównym celem dyrektywy jest podniesienie poziomu bezpieczeństwa cyfrowego, dzięki nałożeniu obowiązku wprowadzania środków skupiających się na zapobieganiu i reagowaniu na zagrożenia cybernetyczne.

Ważnym elementem jest katalog branż, które będą objęte szczególnym nadzorem. Wyróżnione zostały branże kluczowe i ważne.

Do kluczowych należą: sektor energii elektrycznej (w tym system ciepłowniczy i chłodniczy), ośrodki pozyskiwania ropy naftowej, gazu i wodoru, transport lotniczy, kolejowy, wodny i drogowy, bankowość, infrastruktura rynków finansowych, opieka zdrowotna, sektor zapewniających wodę pitną, ścieki, infrastruktura cyfrowa, administracja publiczna a także przestrzeń kosmiczna.

Dodatkowo pojawia się lista branż tzw. ważnych w kontekście cyberbezpieczeństwa. Zaliczać się do nich będą przedsiębiorstwa branż takich jak: usługi pocztowe i kurierskie, gospodarowanie odpadami, produkcja, wytwarzanie i dystrybucja chemikaliów, produkcja, przetwarzanie i dystrybucja żywności, produkcja w branżach wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro, produkcja komputerów, wyrobów elektronicznych i optycznych, produkcja urządzeń elektrycznych, produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana, produkcja pojazdów samochodowych, przyczep i naczep, dostawcy usług cyfrowych oraz badania naukowe.

Szeroki katalog sektorów dotyczyć będzie także o dostawców produkujących podzespoły i świadczących usługi dla wszystkich wspomnianych branż. Również dla administracji publicznej, w tym JST.

SEKTORY KLUCZOWE I WAŻNE WG NIS2

Akt prawny nie wprowadza zamkniętego katalogu zabezpieczeń, jakie ma wprowadzić jednostka samorządu lub firma komercyjnej, jednak pokazuje kierunki, w których powinny być realizowane działania. Są to:

- analiza ryzyka i polityki bezpieczeństwa systemów informatycznych,
- obsługa incydentów (zapobieganie, wykrywanie i reagowanie na incydenty),
- ciągłość działania i zarządzania kryzysowego,
- bezpieczeństwo łańcucha dostaw,

- bezpieczeństwo w pozyskiwaniu, rozwijaniu i utrzymywaniu sieci i systemów informatycznych (w tym obsługa i ujawniania podatności),
- procedury (testowanie i audyt) służące ocenie skuteczności środków zarządzania ryzykiem cyberbezpieczeństwa,
- wykorzystywanie kryptografii i szyfrowania,
- polityka kontroli dostępu.

Cyberbezpieczny Samorząd to projekt, który pozwala zabezpieczyć te wszystkie obszary w jednostkach samorządu terytorialnego. Ministerstwo Cyfryzacji przygotowało specjalną mapę drogową dla jednostek planujących kolejne kroki.

Obejmuje ona następujące obszary:

- Zarządzanie
- System Zarządzania Bezpieczeństwem Informacji
- Ochrona
- Zdarzenia i Monitoring
- Reagowanie
- Odtwarzanie
- Infrastruktura
- Telekomunikacja

Obszar: Zarządzanie – obejmuje przygotowanie kierownika Jednostki do zarządzania kwestiami związanymi z cyberbezpieczeństwem, jego przygotowanie, szkolenia, a także formalne aspekty, jak na przykład publikację Polityki Bezpieczeństwa Informacji czy zasady korzystania z Centrum Usług Wspólnych.

System Zarządzania Bezpieczeństwem Informacji obejmuje wskazówki dotyczące poprawnego, zgodnego z dobrymi praktykami przygotowania Polityki Bezpieczeństwa Informacji, a także procedury, sposoby reakcji na incydenty, strategia zarządzania ryzykiem również we współpracy z zewnętrznymi partnerami.

Kolejny obszar objęty wskazówkami to **Ochrona**. Tu mieści się zarówno zarządzanie uprawnieniami, jak również aspekty techniczne, dotyczące zabezpieczenia danych, tworzenia kopii zapasowych czy technologii ochronnych.

Zdarzenia i Monitoring definiują konieczność ciągłego monitorowania bezpieczeństwa jako kluczową dla zabezpieczenia infrastruktury IT, wymieniając w niej m.in. zapewnienie konieczności wykrywania poszczególnych rodzajów zagrożeń.

Reagowanie zawiera opis tego, jak powinien dzia-

łać system reagowania w sytuacji wykrycia incydentu bezpieczeństwa. **Odtwarzanie** wskazuje jasno, że plan odtwarzania powinien być na bieżąco aktualizowany o zgromadzone wnioski i doświadczenia.

Ostatnie dwie sekcje przygotowanego przez Ministerstwo Cyfryzacji planu analizy sytuacji w JST to **Infrastruktura** i **Telekomunikacja**. W tych obszarach technicznie opisano wskazówki w zakresie infrastruktury, która powinna być wykorzystana, by zapewnić lepsze zabezpieczenia samorządom.

SOC – JAK MOŻE POMÓC SAMORZĄDOM W REALIZACJI OBOWIĄZKÓW WYNIKAJĄCYCH Z DYREKTYWY NIS2?

SOC to usługa polegająca na zewnętrznym monitoringu infrastruktury IT. Eksperci z dziedziny cybersecurity obserwują sytuację 24/7, by ochronić systemy informacyjne, dane i infrastrukturę przed nieautoryzowanym dostępem, naruszeniami, podatnościami i innymi rodzajami ryzyka.

SOC stale monitoruje sieci, systemy i aplikacje organizacji za pomocą specjalistycznych narzędzi, takich jak systemy wykrywania włamań (IDS), platformy zarządzania informacjami i zdarzeniami dotyczącymi bezpieczeństwa (SIEM) oraz narzędzia do analizy logów. Dzięki temu możliwa jest analiza zdarzeń związanych z bezpieczeństwem oraz logów z różnych źródeł, takich jak zapory sieciowe, serwery, urządzenia sieciowe i urządzenia końcowe.

Wykryte zdarzenia i podatności są oceniane i analizowane w celu określenia ich nasilenia i potencjalnego wpływu na bezpieczeństwo całej infrastruktury jednostki samorządowej.

OGRANICZONE ZASOBY NA RYNKU – SOC ROZWIĄZUJE PROBLEM ZATRUDNIENIA I KOSZTÓW

W dobie ograniczonej ilości specjalistów z tego zakresu na rynku, SOC jest zdecydowanie najlep-szym rozwiązaniem:

- Pozwala ograniczać wydatki, które wiązałyby się z zatrudnieniem, a następnie regularnym szkoleniem specjalistów.
- Daje też dostęp do fachowców, których ilość na rynku jest ograniczona.
- Zapewnia zgodność procedur z wymaganiami i postępowanie zgodnie z najwyższym standardem świadczenia tego typu usług.

SOC PERCEPTUS

Perceptus realizuje procesy obsługi SOC dla klientów zgodnie ze standardem wyznaczanym przez normę ISO 27001. Doświadczenie w tym obszarze zespół specjalistów stale buduje od 2019 r. Dzięki temu firma Perceptus jest gotowa do wespierania zarówno klientów biznesowych, jak również jednostki samorządu terytorialnego w realizacji nowych wymagań.

Jako doświadczony integrator firma ta może zabezpieczyć też obszary techniczne, dostarczając najwyższej klasy sprawdzone rozwiązania (komplementarne rozwiązania z zakresu oprogramowania i infrastruktury sprzętowej) oraz szkoląc i edukując pracowników, by pomóc w zorganizowaniu kompletnego systemu zapewniającego cyberbezpieczne jutro.

- OH MY -

H @ C K

700 SPECJALISTÓW CYBERBEZPIECZEŃSTWA

Reprezentanci liderów branży fintech / IT,
m.in.: ACCENTURE, ALLEGRO, AVIVA, CERT Polska,
CSIRT KNF, EY, GSK, HSBC, IBM, ING, MICROSOFT,
NORDEA, ORANGE, Standard Chartered, T-MOBILE.

POKAŻ SIĘ!

NIECH POLSKA BRANŻA CYBERSECURITY CIĘ USŁYSZY

WYSTĄP NA SCENIE OMH 2023

KONFERENCJA POD PATRONATEM ZAUFANA TRZECIA STRONA.PL

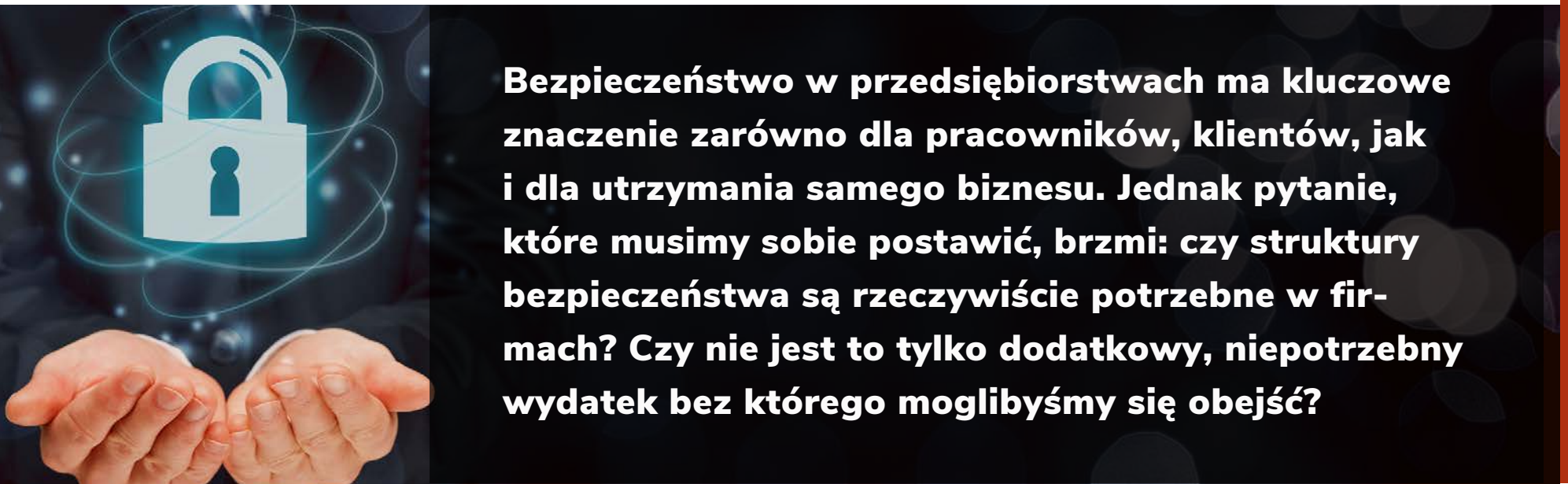
5.12.2023 / PGE Narodowy, Warszawa

CALL FOR PAPERS do 5 WRZEŚNIA 2023

BILETY DOSTĘPNE: www.omhconf.pl

STRUKTURY BEZPIECZEŃSTWA W PRZEDSIĘBIORSTWACH. CZY NAPRAWDĘ SĄ POTRZEBNE?

Tomasz Grzelak
Stay Safe Poland



Bezpieczeństwo w przedsiębiorstwach ma kluczowe znaczenie zarówno dla pracowników, klientów, jak i dla utrzymania samego biznesu. Jednak pytanie, które musimy sobie postawić, brzmi: czy struktury bezpieczeństwa są rzeczywiście potrzebne w firmach? Czy nie jest to tylko dodatkowy, niepotrzebny wydatek bez którego moglibyśmy się obejść?

Przyjrzymy się różnym aspektom bezpieczeństwa fizycznego i technicznego w przedsiębiorstwach, tak aby móc odpowiedzieć sobie na wszystkie nurtujące nas pytania i rozwiać wszelkie wątpliwości.

CZYM JEST BEZPIECZEŃSTWO?

To „stan braku zagrożeń, stan spokoju i pewności”*. Zagrożenia związane z bezpieczeństwem:

Ze względu na charakter:

- polityczne,
- gospodarcze,
- psychologiczno-socjologiczne,
- ekologiczne,
- ładu i porządku publicznego,
- militarne.

Ze względu na źródło pochodzenia:

- Zewnętrzne - działania kryminalne, nielegalna działalność nieuczciwej konkurencji lub klientów, siły natury.
- Wewnętrzne - działalność pracowników na szkodę firmy, czynniki zagrażające bezpieczeństwu w przypadku awarii.

* Włodarski A. Elementy Polityki Bezpieczeństwa Państwa, Tezy wykładów, Zarządzanie w stanach zagrożeń, Szkoła Główna Służby Pożarniczej, Warszawa 1999

Jak widać, obszar zagrożeń jest dość szeroki, dlatego pominiemy tak istotne kwestie jak cyberbezpieczeństwo czy bezpieczeństwo informacji, a skupimy się tylko na dwóch aspektach.

Pierwszym elementem, o którym należy wspomnieć jest bezpieczeństwo fizyczne. Pracownicy ochrony, patrole interwencyjne, osoby zarządzające oraz prowadzące szkolenia dla personelu w zakresie procedur bezpieczeństwa, stanowią podstawę zapewnienia ochrony przed zagrożeniami związanymi z działalnością przedsiębiorstwa. Wprowadzenie odpowiednich środków bezpieczeństwa fizycznego pomaga zmniejszyć ryzyko włamania, kradzieży, wandalizmu czy napaści. Dodatkowo dobrze przeszkoleni pracownicy są bardziej świadomi potencjalnych zagrożeń i potrafią reagować na nie w odpowiedni sposób.

Wdrożenie programów szkoleniowych w zakresach takich jak procedury bezpieczeństwa, ewakuacyjne czy pierwsza pomoc, z pewnością zwiększa poziom bezpieczeństwa w firmie.

Punkt drugi to oczywiście bezpieczeństwo techniczne, które w erze cyfrowej staje się równie ważne jak bezpieczeństwo fizyczne. Do najpopular-

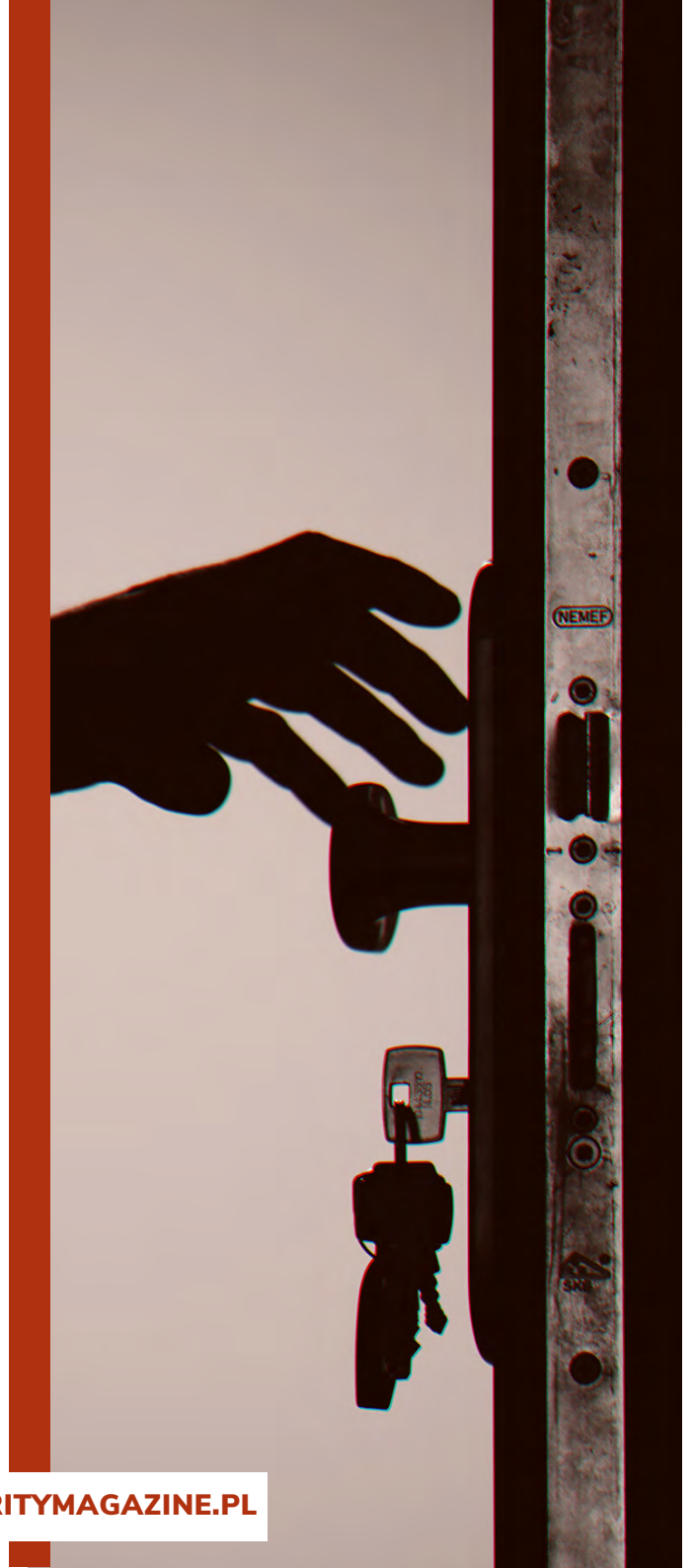
niejszych jego elementów należą:

- monitoring wizyjny: systemy monitoringu wizyjnego pozwalają na ciągłe monitorowanie obszaru firmy. To cenne narzędzie w śledzeniu aktywności niepowołanych osób i potencjalnych zagrożeń
- kontrola dostępu która umożliwia ograniczenie wstępu do określonych obszarów tylko dla uprawnionych pracowników
- systemy sygnalizacji włamania i napadu: alarmy i inne systemy sygnalizacyjne pomagają szybko reagować na potencjalne zagrożenia i przeciwdziałać im na wczesnym etapie. To kluczowe w minimalizacji ryzyka strat materialnych i ludzkich

Dodatkowo systemy te mogą być wykorzystywane przez inne działy w firmie:

Kamery w zakładach przemysłowych - monitorowanie linii produkcyjnych i identyfikacja problemów jak awarie, przegrzewanie maszyn lub nieprawidłowości w procesie produkcji, ewentualnie wczesne ostrzeganie o pojawieniu się dymu lub ognia w obiekcie.

Kamery w obiektach handlowych - liczenie osób, mapy ciepła pokazujące nam w których rejonach klienci zatrzymują się najczęściej i jakie działania marketingowe są najbardziej skuteczne.



Z kolei kontrola dostępu to idealne narzędzie do kontroli czasu pracy, zarządzania zatrudnieniem i efektywnością pracy. Dokładnie wiemy, ile czasu nasz pracownik spędził w pracy, a w przypadku rozwiązana umowy jednym kliknięciem możemy zablokować mu dostęp do obiektu bez obawy czy wtargnie na nasz teren.

To tylko kilka z licznych, dodatkowych możliwości systemów. Z pewnością będą one przydatne w niejednym przedsiębiorstwie. Szczególnie w dobie kryzysu ich dodatkowe zastosowanie powinno być interesujące dla inwestorów. Prawidłowo zaplanowany i wdrożony system zabezpieczeń może przynieść duże oszczędności firmom oraz zdecydowanie zwiększyć bezpieczeństwo w obiektach. Raz wydane fundusze będą przynosić oszczędności przez kilka następnych lat.

KTO POWINIEN ZAJMOWAĆ SIĘ WDRAŻANIEM WYMIENIONYCH RZECZY?

Niewątpliwie tworzenie struktur bezpieczeństwa w przedsiębiorstwie wymaga odpowiedniego zarządzania, a kluczowym elementem tego procesu jest zatrudnienie doświadczonej osoby która stanie na ich czele. Osoba ta odpowiada za wdrażanie, rozwijanie oraz monitorowanie strategii bezpieczeństwa oraz koordynację działań w tej dziedzinie. Istnienie takiego stanowiska stanowi fundament dla budowy bezpiecznej i stabilnej organizacji.

Główne zadania:

- planowanie strategii bezpieczeństwa: osoba ta analizuje ryzyko, identyfikuje potencjalne zagrożenia i tworzy plan działania, który obejmuje zarówno aspekty fizyczne, jak i techniczne bezpieczeństwa,

- tworzenie systemów bezpieczeństwa: odpowiada za wdrażanie i nadzór nad różnymi elementami struktur bezpieczeństwa, takimi jak monitoring wizyjny, systemy alarmowe i procedury bezpieczeństwa,
- zarządzanie personelem bezpieczeństwa: w zależności od wielkości przedsiębiorstwa, osoba ta może zarządzać zespołem specjalistów ds. bezpieczeństwa, współpracować z innymi działami firmy oraz nadzorować zewnętrzne podmioty świadczące dla nas usługi,
- monitorowanie skuteczności: regularnie ocenia skuteczność działań bezpieczeństwa, przeprowadza audyty i wprowadza niezbędne poprawki w celu ciągłego doskonalenia procesów bezpieczeństwa.

Jednakże, nie wszystkie przedsiębiorstwa mogą zatrudnić takiego specjalistę do spraw bezpieczeństwa na pełny etat, w szczególności tyczy się to tych mniejszych firm. Często obowiązki związane z zarządzaniem bezpieczeństwem powierzane są innym pracownikom, takim jak kierownicy administracji czy dyrektorzy innych działów.

To niesie ze sobą pewne zagrożenia takie jak:

- brak specjalistycznej wiedzy: ci pracownicy często nie posiadają odpowiedniego doświadczenia w zakresie bezpieczeństwa, co może wpłynąć na jakość i efektywność działań związanych z tą dziedziną,
- niedostateczna świadomość ryzyka: osoby te mogą nie dostrzegać wszystkich potencjalnych zagrożeń, co może skutkować niewłaściwą hierarchizacją działań i nieodpowiednim reagowaniem na incydenty,
- pozorne oszczędności: zarządzanie bezpieczeństwem wymaga odpowiedniego budżetu oraz inwestycji. Pracownicy niebędący specjalistami w tej dziedzinie mogą nie zrozumieć potrzeby wydatków w bezpieczeństwo i ograniczać budżet na te cele,
- brak rozwoju: bezpieczeństwo to dynamiczna dziedzina, wymagająca ciągłego doskonalenia oraz dostosowywania się do nowych zagrożeń. Osoby bez doświadczenia w tej dziedzinie mogą zapominać o tym aspekcie.

Wdrożenie struktur bezpieczeństwa może stanowić duże wyzwanie, szczególnie dla mniejszych przedsiębiorstw, które nie zawsze mają możliwość zatrudnienia osoby która będzie zarządzać tymi elementami. Jednak istnieją alternatywne rozwiązania, które pozwalają na zapewnienie odpowied-

niego poziomu bezpieczeństwa bez ponoszenia dużych kosztów. Audytorzy i firmy zewnętrzne to profesjonalne usługi, które mogą wspomóc przedsiębiorstwa w osiągnięciu wysokiego poziomu bezpieczeństwa za mniejsze pieniądze.

Audytorzy bezpieczeństwa to wyspecjalizowani eksperci, którzy niezależnie oceniają stan bezpieczeństwa w przedsiębiorstwie. Ich głównym zadaniem jest przeprowadzenie audytu bezpieczeństwa, który obejmuje analizę istniejących struktur, procedur oraz systemów bezpieczeństwa. Audytorzy identyfikują potencjalne zagrożenia i słabe punkty, a następnie rekomendują konieczne kroki w celu podniesienia poziomu.

Innym rozwiązaniem jest zatrudnienie firm zewnętrznych ds. bezpieczeństwa. To podmioty specjalizujące się w świadczeniu usług z zakresu bezpieczeństwa, które oferują wsparcie na wielu poziomach.

- **zarządzanie bezpieczeństwem:** firmy te mogą pełnić rolę Zewnętrznego Kierownika Bezpieczeństwa dla przedsiębiorstwa, oferując wsparcie w planowaniu, wdrażaniu i monitorowaniu bezpieczeństwa
- **outsourcing bezpieczeństwa**: przedsiębiorstwa mogą zlecić firmie zewnętrznej zarządzanie różnymi elementami bezpieczeństwa, takimi jak monitoring wizyjny, systemy alarmowe czy ochrona fizyczna
- **szkolenia z bezpieczeństwa:** firmy zewnętrzne często oferują specjalistyczne szkolenia z zakresu bezpieczeństwa dla pracowników, co zwiększa świadomość zagrożeń i umiejętności reagowania na nie
- **konsultacje:** pełnienie roli doradcy, dostarczając wiedzy i doświadczenia w zakresie bezpieczeństwa

Bezpieczne przedsiębiorstwo to stabilne przedsiębiorstwo, gotowe stawić czoła wyzwaniom współczesnego rynku.


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

ZMIENIA SIĘ USTAWA O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA

Redakcja
SECURITY MAGAZINE

Zmienią się dotychczasowe przepisy związane z cyber-bezpieczeństwem? Projekt nowelizacji ustawy ma roz-szerzyć obowiązki nakładane na firmy. Które z branż obejmie? Co dokładnie zawiera nowelizacja ustawy?

PROJEKT NOWELIZACJI TRAFIA DO SEJMU

Rządowy projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UKSC) trafił w końcu do sejmu. Jednak wdrożenie przepisów w życie niekoniecznie będzie takie proste. Prace nad nowelizacją będą przeniesione z powodu skierowania jej do wysłuchania publicznego. To ma mieć miejsce 11 września 2023 r. Warto podkreślić, że to już 13 propozycja tego aktu.

Obecnie obowiązujący tekst UKSC został wprowadzony z powodu konieczności wprowadzenia unijnej dyrektywy NIS. Jednak w trakcie prac nad nowelizacją UKSC opublikowano dyrektywę NIS 2, która zastępuje swoją poprzedniczkę i ma być zaimplementowana do 17 października 2024 r.

Równolegle do prac nad nowelizacją UKSC trwa proces ustanowienia prawa komunikacji elektronicznej (PKE). To ma zastąpić obecnie obowiązujące prawo telekomunikacyjne. PKE ma dotyczyć głównie przedsiębiorców komunikacji elektronicznej. Ci według propozycji nowelizacji UKSC mają zostać włączeni do krajowego systemu cyberbezpieczeństwa. Propozycje PKE i nowelizacji UKSC są ze sobą powiązane. Wielokrotnie w projekcie nowelizacji UKSC odnosi się do PKE. W uzasadnieniu projektu wskazano również, że oba akty powinny wejść w życie w tym samym czasie. Nie mamy jednak pewności w jakiej dokładnie formie i kiedy oba te projekty wejdą w życie. A to ze względu na NIS 2 oraz kończącą się kadencję rządu.

NA CZYM POLEGA USTAWA UKSC?

Projekt nowelizacji UKSC nakłada na przedsiębiorców komunikacji elektronicznej szereg obowiązków związanych z cyberbezpieczeństwem.

Przewiduje się, że będą oni musieli systematycznie szacować ryzyko wystąpienia sytuacji szczególnego zagrożenia, jak i podejmować środki techniczne czy organizacyjne zapewniające poufność, integralność, dostępność oraz autentyczność przetwarzanych danych, zgodnie z poziomem bezpieczeństwa odpowiednim do zidentyfikowanego ryzyka.

Tego typu firmy będą również musiały dokumentować podejmowane działania w ramach cyberbezpieczeństwa oraz obsługi incydentów bezpieczeństwa. Mowa tutaj np. o zgłaszaniu incydentów i współpracy z organami cyberbezpieczeństwa. Co w przypadku niewywiązania się z takich obowiązków? Nowelizacja przewiduje karę, która może wynieść do 3% rocznego przychodu ukaranej organizacji. Z kolei osoby kierujące taką firmą naruszającą obowiązki mogą być obłożone karą pieniężną do 300% miesięcznego wynagrodzenia.

Nowelizacja UKSC przewiduje również rozszerzenie katalogu podmiotów publicznych podlegających obowiązących w zakresie cyberbezpieczeństwa. Obejmować to ma zarówno podmioty administracji publicznej na różnych szczeblach, jak i instytucje sektora finansowego, opieki zdrowotnej oraz inne sektory krytyczne dla funkcjonowania państwa.
Są to np. Państwowe Gospodarstwo Wodne Wody Polskie, Polski Fundusz Rozwoju, Polska Agencja Rozwoju Przedsiębiorczości, uczelnie i szkolnictwo wyższe itd.

Nowelizacja UKSC ma również na celu usprawnienie reakcji na incydenty cyberbezpieczeństwa. Projekt zakłada utworzenie CSIRT INT i CSIRT Telco, które mają działać na rzecz jednostek organizacyjnych podległych właściwemu ministerstwu czy na potrzeby przedsiębiorstw telekomunikacyjnych. Powołane zostanie również Operacyjne Centrum Bezpieczeństwa, która ma na celu zastąpić dotychczasowe struktury odpowiedzialne za cyberbezpieczeństwo operatorów usług kluczowych. Podzieli się ono na wewnętrzne i zewnętrzne, czyli będzie pełnić funkcje u operatorów, jak i zlecać pełnienie tej funkcji.

Według planowanej nowelizacji UKSC, operatorzy usług kluczowych będą musieli mieć w swojej infrastrukturze właśnie rzeczone Centrum Operacyjne Bezpieczeństwa. Będą one wówczas odpowiedzialne za kilka ważnych funkcji, takich jak zarządzanie bezpieczeństwem, tworzenie i aktualizacja dokumentacji związanej z cyberbezpieczeństwem oraz obsługa incydentów. Co więcej, personel pracujący w tych centrach będzie musiał posiadać poświadczenie bezpieczeństwa osobowego do obsługi in-

formacji o klauzuli „poufne”. To ważne kroki mające na celu wzmocnienie ochrony systemów i danych w kraju.

W ramach nowelizacji powołany zostanie osobny podmiot, czyli Operator Strategicznej Sieci Bezpieczeństwa (OSSB). Organizacja ta ma oferować usługi telekomunikacyjne i zapewinać cyberbezpieczeństwo najważniejszym organom Polski, a także zarządzać strategiczną siecią bezpieczeństwa. Wybrana zostaine przez premiera z organizacji spełniających określone kryteria. Musi to być jednoosobowa spółka Skarbu Państwa, przedsiębiorca telekomunikacyjny i zapewniać odpowiednie wykonywanie zadań operatora strategicznej sieci bezpieczeństwa.

OSSB będzie korzystać z częstotliwości państwowych, chyba że zaistnieje konieczność wykorzystania tych cywilnych. Wówczas prezes Urzędu Komunikacji Elektronicznej (UKE) będzie miał możliwość nałożenia na organizację, który posiada rezerwację częstotliwości cywilnych, obowiązku udostępnienia ich OSSB. Istnieją jednak obawy dotyczące zgodności tego rozwiązania z prawem Unii, w szczególności z Europejskim kodeksem łączności elektronicznej, który określa warunki dostępu do częstotliwości oraz wyjątki od zasady swobodnego dostarczania sieci i świadczenia usług telekomunikacyjnych. To jednak nie są jedyne kontrowersje związane z UKSC.

KONTROWERSJE PRZY NOWELIZACJI UKSC

Jednak niektóre organizacje pozarządowe i eksperci z dziedziny cyberbezpieczeństwa wyrażają swoje obawy dotyczące nowelizacji UKSC. Krytycy podkreślają, że obowiązki i sankcje finansowe nakładane na podmioty mogą być zbyt restrykcyjne, zwłaszcza dla sektora MMŚP.

Istnieje również obawa, że brak odpowiednich środków finansowych i technologicznych może utrudnić spełnienie nowych wymagań.

Ustawa przewiduje też rozszerzenie uprawnień „ministra właściwego do spraw informatyzacji". Nowa regulacja umożliwi mu przeprowadzanie postępowań mających na celu uznanie danego podmiotu za dostawcę wysokiego ryzyka. W rezultacie, minister będzie mógł wydać decyzję administracyjną, która uzna dostawcę sprzętu lub oprogramowania za podmiot stanowiący poważne zagrożenie dla obronności, bezpieczeństwa państwa, porządku publicznego lub życia i zdrowia ludzi. Jeśli taka decyzja zapadnie, to szczególnie narażone organizacje, takie jak dostawcy usług cyfrowych czy operatorzy usług kluczowych lub niektóre przedsiębiorstwa telekomunikacyjne nie będą mogły korzystać z usług firmy usankcjonowanej przez ministra.

Ma to się tyczyć też organizacji, których tyczy się ustawa o zamówieniach publicznych. W praktyce oznacza to, że takie podmioty nie będą mogły kupować produktów, oprogramowania czy usług od konkretnego, usankcjonowanego dostawcy. Dodanie nowej przesłanki wykluczenia wykonawcy z postępowania budzi wątpliwości związane ze zgodnością z unijnym prawem zamówień publicznych. Niektóre wątpliwości w tej kwestii wyraził Minister ds. Unii Europejskiej podczas konsultacji dotyczących projektu nowelizacji UKSC.

Wprowadzone zostaną też zmiany w ustawie PZP. Zostanie w niej wskazany dodatkowy powód odrzucenia oferty wykonawcy. Zgodnie z nowymi przepisami, oferta zostanie odrzucona, jeśli obejmuje produkt, usługę lub proces z dziedziny technologii informacyjno-komunikacyjnych (ICT), które zostały określone w decyzji o uznaniu organizacji za

dostawcę wysokiego ryzyka.

W ramach nowelizacji UKSC przewiduje się również utworzenie krajowego systemu certyfikacji cyberbezpieczeństwa. Będzie to program mający na celu ocenę i certyfikację produktów, usług i procesów związanych z cyberbezpieczeństwem. Certyfikacja ta ma na celu zapewnienie wysokiego poziomu bezpieczeństwa i ochrony danych.

Nowelizacja UKSC stawia również duży nacisk na współpracę międzynarodową w dziedzinie cyberbezpieczeństwa. Projekt zakłada intensyfikację współpracy z innymi państwami, organizacjami międzynarodowymi i sektorem prywatnym w celu wymiany informacji, dobrych praktyk i wspólnego działania przeciwko cyberzagrożeniom. Współpraca ta ma na celu zwiększenie skuteczności działań i ochronę przed transgranicznymi atakami.

ZMIANY W DEFINICJI CYBERBEZPIECZEŃSTWA

Jedną z ważnych zmian wprowadzanych przez nowelizację UKSC jest nowa definicja cyberbezpieczeństwa. Jej celem jest dostosowanie terminologii do innych przepisów prawnych, w tym unijnych regulacji.

Zgodnie z nową definicją, cyberbezpieczeństwo oznacza działania mające na celu ochronę systemów informacyjnych, użytkowników tych systemów i innych podmiotów przed zagrożeniami związanymi z cyberprzestrzenią.

Natomiast pojęcie cyberzagrożeń, które również zostało wprowadzone przez nowelizację, odnosi się do wszelkich potencjalnych okoliczności, zdarzeń lub działań, które mogą spowodować szkodę, zakłócenia lub negatywny wpływ na systemy informacyjne, użytkowników i inne podmioty.

Warto zauważyć, że obecne brzmienie definicji cyberbezpieczeństwa w nowelizacji UKSC nie jest w pełni dostosowane do terminologii używanej w innych unijnych aktach prawnych, takich jak rozporządzenie DORA czy dyrektywa NIS 2.

W ramach nowelizacji UKSC przewiduje się również utworzenie krajowego systemu certyfikacji cyberbezpieczeństwa. Będzie to program mający na celu ocenę i certyfikację produktów, usług i procesów związanych z cyberbezpieczeństwem. Certyfikacja ta ma na celu zapewnienie wysokiego poziomu bezpieczeństwa i ochrony danych.

Zmienia się ustawa o krajowym systemie cyberbezpieczeństwa

Przepisy wynikające z nowelizacji UKCS mają wejść po upływie 6 miesięcy od dnia ogłoszenia. To oznacza, że musi upłynąć pewien okres po opublikowaniu zmian, zanim zaczną one obowiązywać.

Czas oczekiwania na wejście w życie ustawy został jednak niedawno wydłużony. Wcześniej proponowano okres 30 dni, ale teraz zdecydowano się na 6 miesięcy. Ta zmiana ma na celu dostosowanie nowelizacji UKSC do innych aktów prawnych, takich jak PKE.

ZAMÓW

AUDYT BEZPIECZEŃSTWA

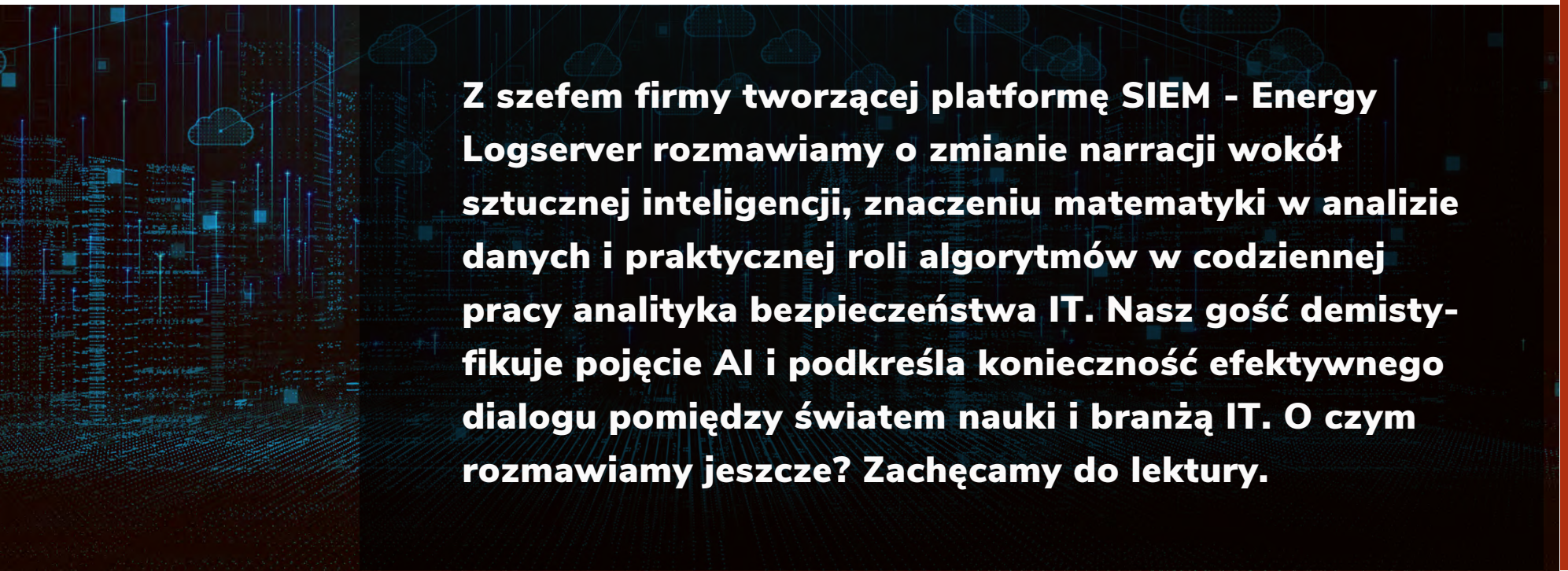
I PRZEKONAJ SIĘ,
JAK OPTYMALIZACJA
PRZETWARZANIA DANYCH
MOŻE DAĆ
CI PRZEWAGĘ
KONKURENCYJNĄ

DOWIEDZ SIĘ WIĘCEJ!

Polityka® Bezpieczeństwa

ARTUR BICKI: AI, ALGORYTMY I PRZYSZŁOŚĆ CYBERBEZPIECZEŃSTWA

Artur Bicki
Energy Logserver



Z szefem firmy tworzącej platformę SIEM - Energy Logserver rozmawiamy o zmianie narracji wokół sztucznej inteligencji, znaczeniu matematyki w analizie danych i praktycznej roli algorytmów w codziennej pracy analityka bezpieczeństwa IT. Nasz gość demistyfikuje pojęcie AI i podkreśla konieczność efektywnego dialogu pomiędzy światem nauki i branżą IT. O czym rozmawiamy jeszcze? Zachęcamy do lektury.

Tematem naszej rozmowy jest zastosowanie sztucznej inteligencji w obszarze bezpieczeństwa IT. Zastanawiam się jednak, jak powinniśmy zacząć?

Artur Bicki: Sztuczna inteligencja to fascynujące zagadnienie, ale zacznijmy może od jej definicji. Pracując jako architekt systemu SIEM zmuszony jestem do rozmowy o konkretach. Na początek proponuję abyśmy zmienili nasz temat na „zastosowania algorytmów matematycznych w analizie danych".

Czy to aż taka różnica ?

A.B.: Dla analityka danych to bardzo ważne. Dziś zagadnienie „sztucznej inteligencji" traci na wartości. Z jednej strony dopiero budujemy nasze doświadczenie w tym obszarze, a z drugiej mam wrażenie, że wzmianki o sztucznej inteligencji będziemy niebawem szukać w opisie składu produktów spożywczych.

Dziś, jeżeli coś nie posiada wzmianki AI, oznacza to tylko przeoczenie działu marketingu. Każdy system informatyczny w swoim opisie bazuje na „Inteligencji". Nie mamy jasności, co się kryje pod tym zagadnieniem. Czy AI to czarna skrzynka, do której wrzucimy nasze nierozwiązane kwestie czy też jest to zbiór żartów i domniemywań, którymi co i rusz częstuje nas Chat GPT.

W takim razie jak powinniśmy rozmawiać?

A.B.: Interesują nas algorytmy przetwarzania danych.

Podchodząc na poważnie do tego zagadnienia, przede wszystkim musimy wykazać się spokojem i opanowaniem wobec medialnej burzy dotyczącej AI. Nie jesteśmy świadkami wiekopomnych odkryć, a jedynie świat IT w końcu do swojej pracy doprosił grono profesorów matematyki. Świat nauki zaszedł dużo dalej niż nam się wydaje. Mam wrażenie, że w kolorowym świecie IT zapomnieliśmy o fundamentach wiedzy, jakimi są statystyka, uczenie maszynowe czy nawet matematyczna analiza i algebra. W tych obszarach naukowcy pracują od setek lat.

Czy to znaczy, że brakuje nam wiedzy?

A.B.: Chyba brakuje nam świadomości, że ta wiedza istnieje. Charakterystyczne jest, że specjaliści danych obszarów nie komunikują się ze sobą. W praktyce, naukowcom pracującym nad algorytmami uczenia maszynowego brakuje praktyki oraz samych danych. Analogicznie, świat IT posługuje się hasłami związanymi z AI, jednak ich wiedza w tym obszarze nie wychodzi poza umiejętność policzenia średniej wartości za dany okres czasu. Widzimy wyraźnie, że podstawą sukcesu jest dialog pomiędzy zespołami reprezentującymi świat nauki oraz świat danych maszynowych.

Co wynika z takiego dialogu?

A.B.: W swojej pracy architekta Energy Logserver współpracuję z profesorami Wydziału Matematyki i Nauk Informacyjnych Politechniki Warszawskiej. Spotykamy się raz w tygodniu, aby omówić dane z którymi pracują nasi wdrożeniowcy. Zaskakujące jest to, że konsultacje z profesorem matematyki mogą trwać tak krótko. Przedstawiamy nasz problem zauważony w danych i już pada odpowiedź, jaki algorytm należy zastosować i z jakimi parametrami.

Czy dziś środowiska programistyczne nie posiadają gotowych funkcji analitycznych, z których możecie korzystać?

A.B.: Oczywiście że tak. Projekty typu Sparc, Pandas, SciKit, czy programy matematyczne są wyposażone we wszystkie możliwe metody analizy. Tylko, że to trochę, jak z siecią internet. Aby coś znaleźć, musimy wiedzieć, czego szukamy.

Co zatem jest dziś najważniejszym wyzwaniem analitycznym, dla którego szukacie algorytmów?

A.B.: Największa potrzebą, którą widzimy na rynku, jest udzielenie wsparcia analitykowi bezpieczeństwa IT. Jego praca bez wsparcia analizy danych nie może być efektywnie wykonana. Żyjemy dziś w świecie pełnym technologii informatycznych. Niewiele osób wie, że każde kliknięcie myszki w aplikacji bankowej, użycie kasy w sklepie czy zebranie punktów lojalnościowych znaczy wygenerowanie dziesiątek linijek tekstu tworzących historię tego zdarzenia. W skali kraju firmy zmuszone są do analizy petabajtów linijek logów, których nikt nie da rady przeglądać.
W swoim produkcie pracę w obszarze analizy zdarzeń kierujemy głównie na automatyczną detekcję anomalii. To zagadnienie okazuje się bardzo szerokie.

Możemy to omówić?

A.B.: Przede wszystkim musimy ustalić, co jest przedmiotem analizy. We wdrożeniach systemów bezpieczeństwa SIEM kolekcjonujemy zdarzenia, jednak wśród nich są liczby i słowa. Ten podział na wstępie oznacza zupełnie inne podejście i zastosowanie innych algorytmów. Musimy rozróżnić przypadki takie jak: detekcja anomalii dla pojedynczej wartości liczbowej, dla wielu liczb naraz, oraz anomalie w tekście.

Czy nie możemy tych danych analizować łącznie?

A.B.: Nie, to są zupełnie odrębne gałęzie nauki. Już detekcja anomalii dla wartości liczbowych stawia przed nami wyzwania. Dla pojedynczej wartości analizujemy rozkład danych w czasie. Szukamy cech powtarzalności i na tej podstawie budujemy model zachowania. Inaczej musimy pracować z wieloma sygnałami na raz, bo interesuje nas nie tylko zmiana wartości, ale również analiza relacji próbki z pozostałymi sygnałami. Wprowadzamy współczynnik korelacji Pearsona i dopiero na tak modelowanych danych możemy analizować odstępstwa od normy.

Te podejścia mają zastosowanie dla danych liczbowych. Co w takim wypadku z tekstem?

A.B.: Matematyka nie analizuje słów i liter. Możemy je jednak policzyć i stworzyć zapis prawdopodobieństwa wystąpienia danej frazy w zbiorze. Dzięki temu łatwo zwracamy uwagę operatorowi co w zdarzeniach jest unikalne i nie zdarzyło się nigdy dotąd. Doświadczony operator IT dobrze zna typowe komunikaty maszyn. Analogicznie, można pokusić się o stworzenie słownika, który będzie związany z konkretną technologią. Ataki, które widzimy jako nowe wpisy, zostaną automatycznie rozpoznane.

Czy to jedyna metoda pracy ze zdarzeniami tekstowymi?

A.B.: Nie. Dla tekstu możemy zastosować trik i zamienić tekst na liczbę. W momencie, gdy posiadamy zbiór liczby utworzony na bazie logów, możemy w tych liczbach szukać podobieństwa oraz różnic. Sięgając po mechanizmy klasteryzacji danych, możemy wykorzystać algorytm, który najzwyczajniej w świecie połączy nam liczby blisko siebie w grupy. To prosty zabieg, jednak odbywa się on bez nadzoru. Nowością jest fakt, że dzięki temu nasze logi możemy zacząć rysować. Okazuje się, że grupa kropek obok siebie to logi o bardzo zbliżonej treści. Analizując taki obraz, możemy zauważyć punkty, które nie pasują do żadnej z grup. To na te zdarzenia będziemy kierowali uwagę operatora.

Te podejścia są bardzo ciekawe i nowatorskie. Co zatem nas czeka jeszcze?

A.B.: Nam jako producentowi systemu SIEM zarysowuje się wizja utworzenia rynku dotyczącego modeli danych. Analogicznie, jak na przykładzie Chat GPT, widzimy, że algorytmika 1:1 polega na danych.

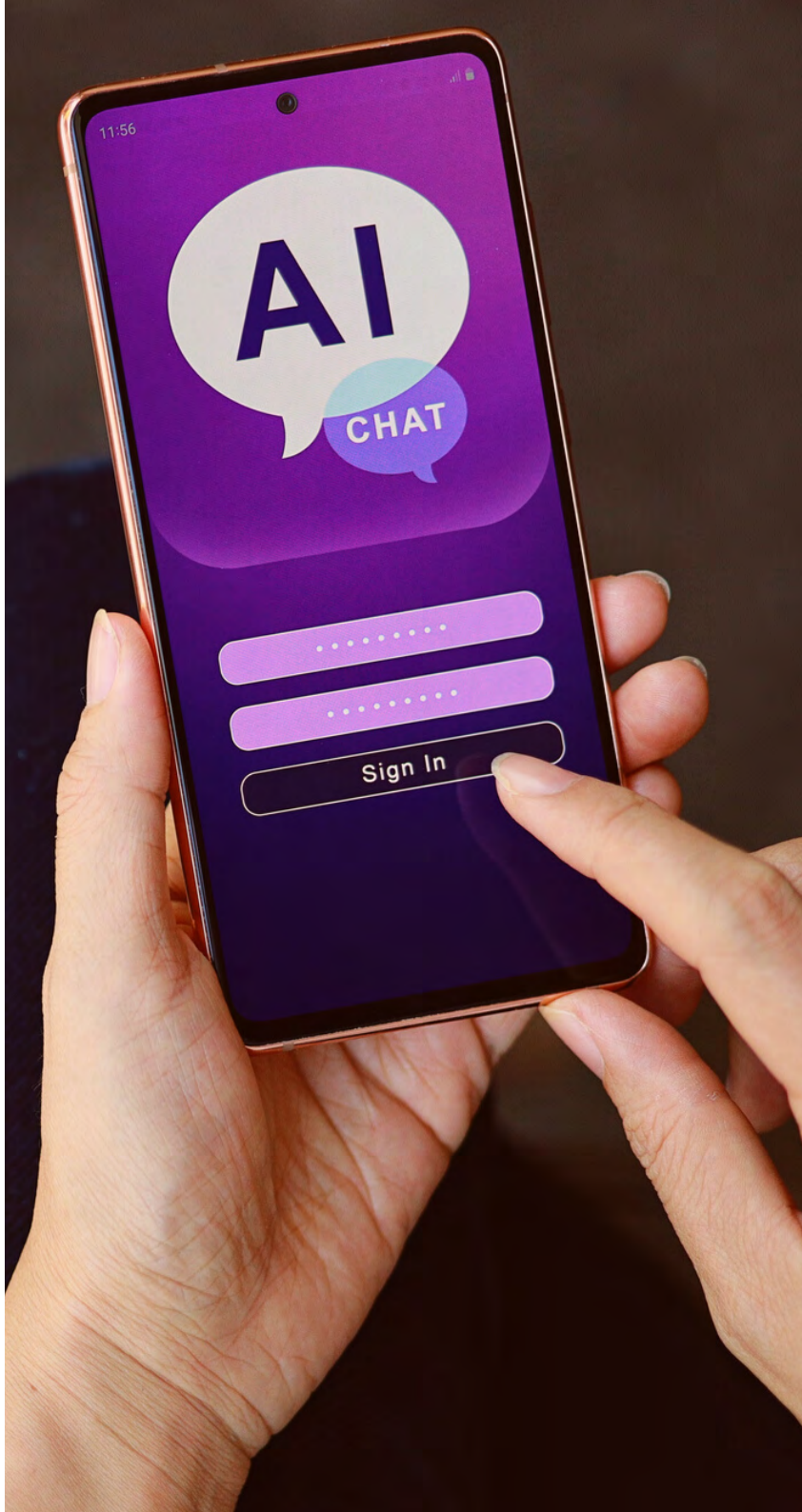
Odpowiedzi nauczonej maszyny będą proporcjonalne do ilości przetworzonej wiedzy. Jako producent mamy możliwość współpracować z klientami, tworząc dla nich modele zachowania sieci, modele rozkładu logów firewall, baz danych i innych powtarzalnych elementów infrastruktury. Dziś społeczność IT Security wymienia się wiedzą dotyczącą wektorów ataków. Dla nas oczywisty kierunek to wymiany wiedzy w postaci wytrenowanych modeli danych.

Czy zastosowanie modelowania danych i opisanych algorytmów nie uśpi czujności operatorów?

A.B.: Tu nie ma w ogóle takiego problemu. Przypomnę, że ręczna analiza milionów wpisów jest technicznie niemożliwa. Bez narzędzi wspomagających dział bezpieczeństwa po prostu działa na domysłach, a jego praca jest bardzo nieefektywna. Wprowadzenie matematycznych algorytmów zdecydowanie poprawi bezpieczeństwo organizacji.

Cieszę się, że rynek zabezpieczeń cechuje tak dogłębna świadomość problemu i dążenie do stałego rozwoju. Dla nas użytkowników to ważne. Dziękuję za rozmowę.

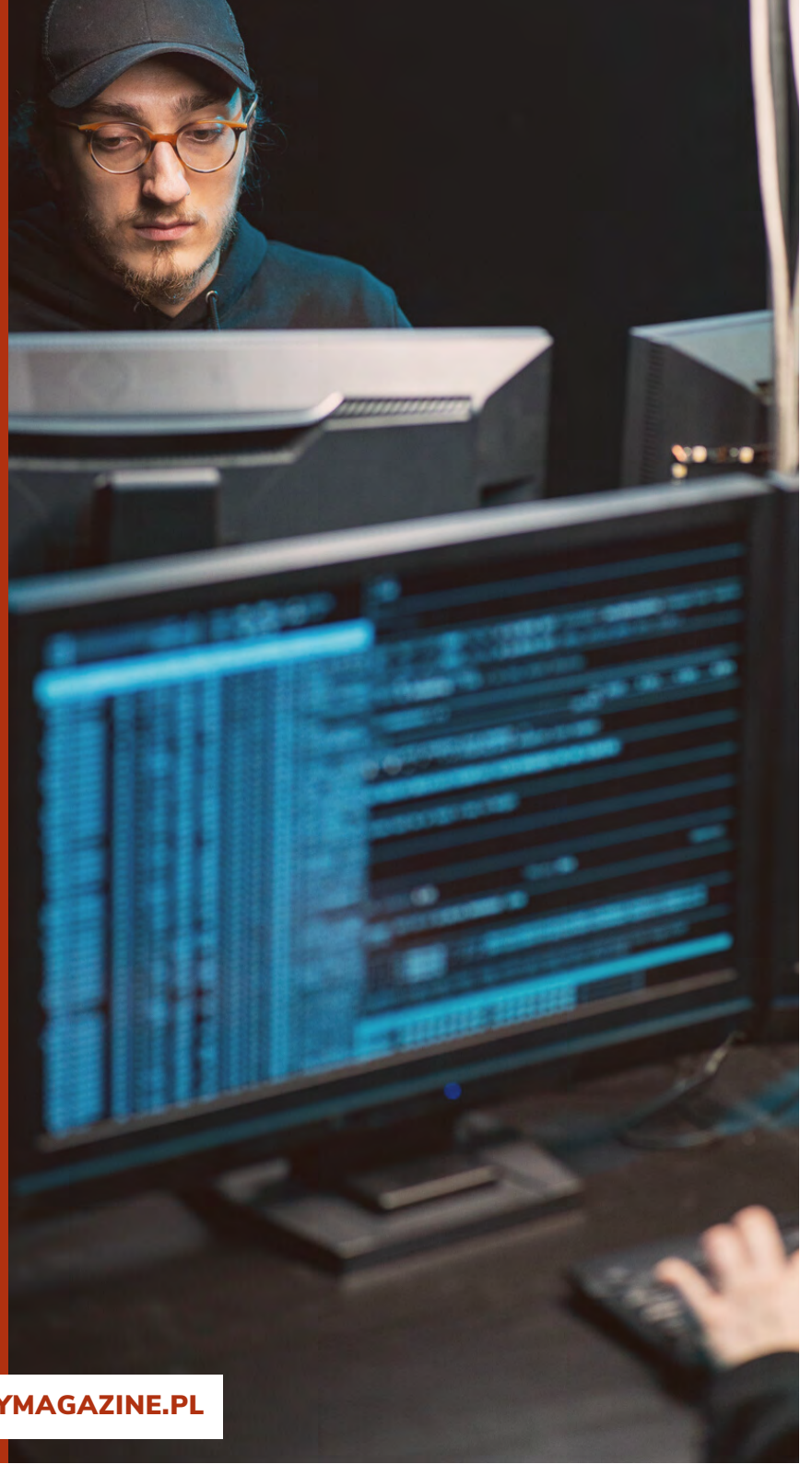
A.B.: Również dziękuję.




Rzetelny Regulamin®
Kompleksowa obsługa prawna Twojego e-commerce

CO ZROBIĆ, ABY TWOJA FIRMA NIE ZOSTAŁA ZASZYFROWANA?

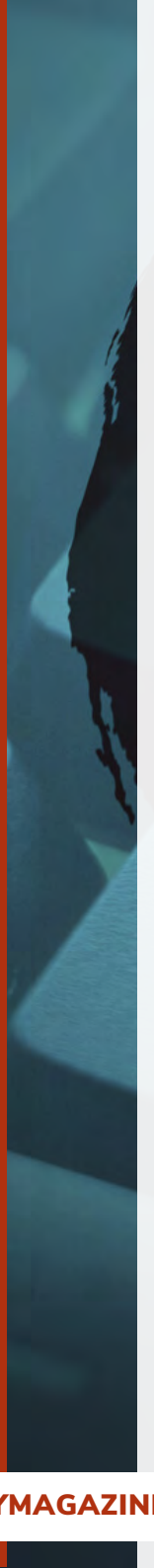
Najpopularniejszymi formami ataków na organizacje są nadal ransomware, malware, phishing, smishing czy DoS. Nazwy te przyprawiają o ból głowy już nie tylko osoby z działów IT sektorów szczególnie narażonych na cyberataki (jak wynika z raportu ENISY: administracja publiczna i dostawcy usług cyfrowych), ale również przedstawicieli innych branż. Dlaczego? Bo dziś to kwestia czasu, kiedy organizacja zostanie zaszyfrowana i jak duże będą tego skutki.



TROCHĘ DANYCH

Średni koszt ataku w Polsce w 2021 r. wynosił 1,49 mln zł, a składały się na niego i koszty związane z przestojem w działalności, kwestie operacyjne, utracona wiarygodność i zamówienia, a także kary za niewłaściwe zabezpieczenie danych (za: Sophos). W Polsce w 2022 roku aż 58% badanych firm zarejestrowała przynajmniej jeden incydent polegający na naruszeniu bezpieczeństwa, a 1/3 odnotowała wzrost intensywności cyberataków na swoje systemy – wynika z raportu „Barometr cyberbezpieczeństwa", przeprowadzonego na zlecenie KPGM w lutym 2023 roku.

Światowe dane są jeszcze bardziej porażające, gdyż – jak podaje Sophos – 94% firm padło ofiarą cyberataku, 75% miało trudności ze znalezieniem źródeł tych incydentów, a średni czas potrzebny na wykrycie, zbadanie i zareagowanie na alert wynosił nawet 9 lub 15 godzin (odpowiednio: dla organizacji zatrudniających od 100 do 3000 pracowników i 3001 do 5000 osób). Szacuje się, że globalny koszt cyberprzestępstw w 2023 r. osiągnie 11 trylionów dolarów, a w 2027 –niemal 24 trylionów dolarów (za: State of Cybersecurity Resilience 2021, firmy Accenture). Jak zatem skutecznie przygotować się na potencjalny cyberatak i ochronić swoją organizację przed utratą drogocennych danych?



W BACKUPIE TKWI SIŁA

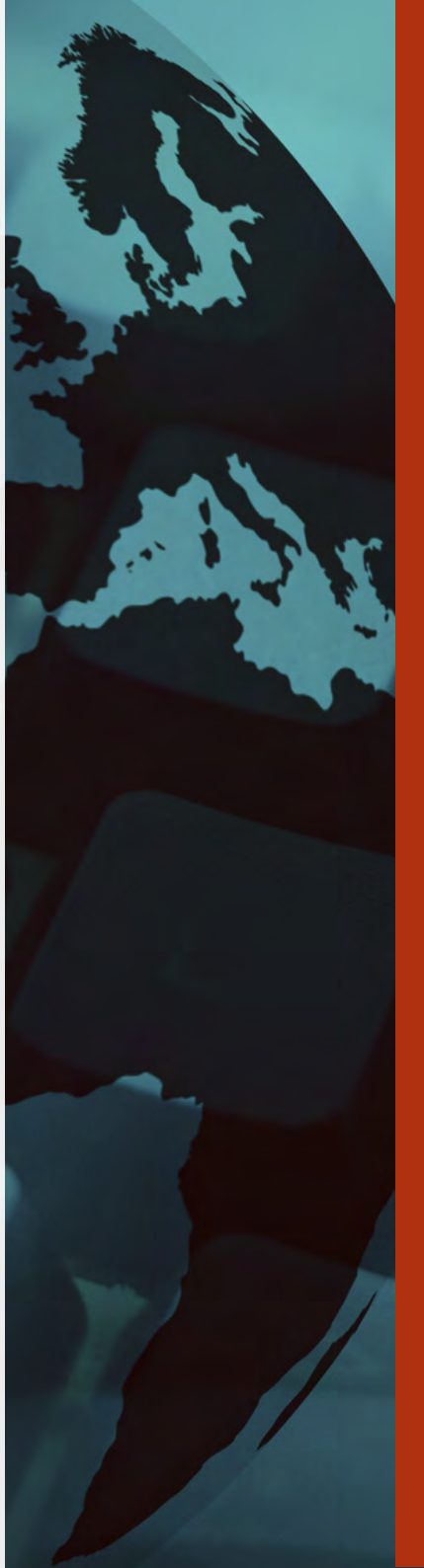
Podstawowym krokiem, który należy podjąć w ramach zabezpieczenia organizacji przed atakami ransomware, jest niewątpliwie zabezpieczenie infrastruktury poprzez firewalle, antywirusy, szyfrowanie SSL i tworzenie kopii zapasowych. FBI w dokumencie „Ransomware prevention and response for CISOs" przekonuje, że to właśnie backup może być najlepszą metodą na odzyskanie danych.

Należy jednak pamiętać, aby mieć zaktualizowane oprogramowanie i by tworzyć kopie danych regularnie, zabezpieczać je i upewnić się, że są one oddzielone od środowiska produkcyjnego warstwą logiczną. Warto również sprawdzać integralność zabezpieczanych danych i testować proces odtworzenia. Takie testy powinny być przeprowadzane przynajmniej raz do roku, gdyż pozwalają na analizę wrażliwych punktów i sprawdzają, czy w razie ataku zaplanowany proces zadziała.

Ekspert Dell Technologies, Kamil Grzesik, podkreśla jednak że *„odpowiedzią na dzisiejsze wyzwania związane z cyberbezpieczeństwem organizacji jest przede wszystkim wielopoziomowa, holistyczna strategia, obejmująca swoim zakresem standardy bezpieczeństwa, wytyczne, zasoby ludzkie, procesy biznesowe i rozwiązania technologiczne".*

CYFROWY BUNKIER PEŁEN... KAMIENI!

- Dziś mówi się o tym, że dane są jednym z najważniejszych surowców XXI wieku. Ich integracja, udostępnianie, analiza i ochrona są fundamentem funkcjonowania i rozwoju organizacji. Nasi klienci coraz częściej zgłaszają się z prośbą o wypracowanie elastycznego, skalowalnego i dającego 100% pewności rozwiązania do zarządzania i zabezpieczenia danych. Jako Platynowy Partner Dell Technologies możemy zaoferować m.in. Cyfrowy Bunkier – mówi **Rafał Brudnicki, właściciel firmy Servers24.pl**, zajmującej się doradztwem i dostawami sprzętu i rozwiązań IT dla biznesu.

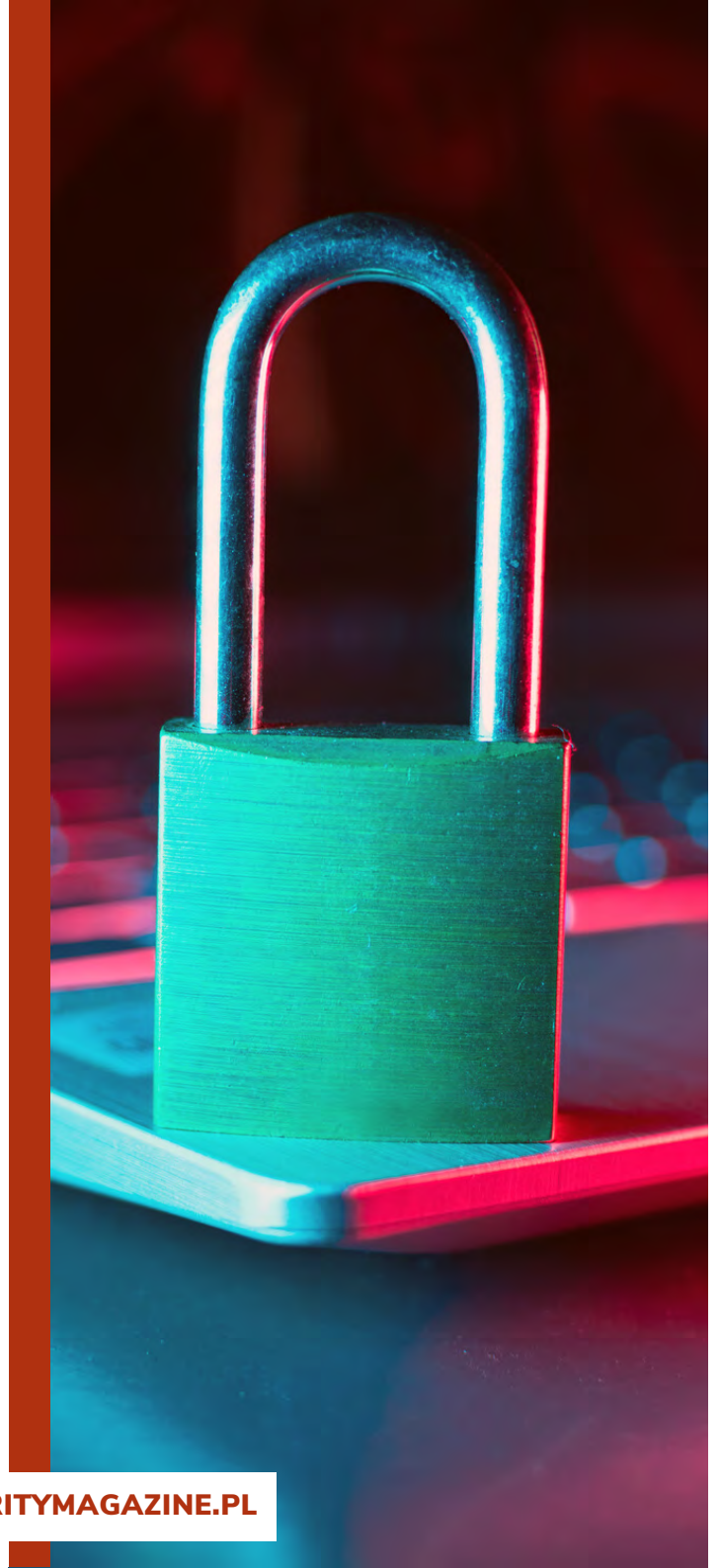


- Systemy pamięci masowej z deduplikacją EMC Data Domain rewolucjonizują dziedziny tworzenia kopii zapasowych, archiwizowania i odzyskiwania sprawności po awarii przez stosowanie bardzo szybkiej deduplikacji przed zapisem. Sprawdzają się zarówno na potrzeby małych, zdalnych lokalizacji, jak i wysoce skalowalnych systemów zabezpieczania kopii zapasowych i danych archiwalnych w centrach danych dużych korporacji – dodaje.

Czym jest Cyfrowy Bunkier? Dell PowerProtect Cyber Recovery to narzędzie, które zapewnia sprawdzoną, nowoczesną i inteligentną ochronę w celu izolowania krytycznych danych, przyspieszenia ich odzyskiwania i identyfikowania podejrzanych działań. A w praktyce? - *Założeniem Cyfrowego Bunkra jest to, aby dane, które trafią do niego, były w pełni bezpieczne i gwarantowały ich odtworzenie w świecie produkcyjnym, w jak najkrótszym czasie* – podkreśla Kamil Grzesik. - *Cyfrowy Bunkier gwarantuje nie tylko odzyskanie danych, które zostały zamrożone, zamienione w <<kamienie>>, ale też ochronę danych oraz wykrywanie zagrożenia na jego wczesnym stadium* – dodaje ekspert.

Podstawowa architektura PowerProtect Cyber Recovery opiera się głównie na elementach:

- **Izolacji danych fizycznych (AirGap)** – jest to logiczna i fizyczna izolacja danych zabezpieczanych od środowiska produkcyjnego, która ma chronić przed niepowołanym dostępem. Dzięki temu firma ma pewność, że w każdej sytuacji będzie w stanie swoje dane odzyskać.
- **Niezmienności czyli gwarancji,** iż – podczas ataku ransomware – dane organizacji pozostaną w niezmienionej formie. Wszystkie dane w Cyfrowym Bunkrze są jak „kamienie", co oznacza, że nie da się ich zaszyfrować, nadpisać czy usunąć, nawet posiadając hasło administratora. Daje to gwarancję odzyskania ich w 100% i w niezmienionej formie.
- **Analityce**, która pomaga kontrolować na bieżąco co dzieje się z danymi organizacji. Środowisko jest stale monitorowane za pomocą oprogramowania do zarządzania Cyfrowym Bunkrem, które odpowiada za synchronizację kopii, przesyłanie danych, zabezpieczenie ich retention lockiem oraz stałą analizę. Wyznaczony użytkownik otrzymuje raporty m.in. dotyczące tego, jak wygląda zajętość i wydajność.



DANE Z WIRUSEM? NIE W TYM PRZYPADKU!

Ważnym uzupełnieniem Cyfrowego Bunkra jest CyberSense. - *Jest to oprogramowanie, które wykorzystuje uczenie maszynowe i umożliwia szybką detekcję ataku oraz szybkie odtworzenie po ataku. Działa na kilku płaszczyznach: analizy danych, które są w Cyfrowym Bunkrze, pod kątem sygnatur wirusów, zagrożeń, luk bezpieczeństwa. Pliki badane są również pod kątem zawartości, sygnałów szyfrowania, etc.* – tłumaczy **Kamil Grzesik z Dell Technologies**.

Oznacza to, że program analizuje metadane plików, ale też ich zawartość. Dzięki temu nie ma możliwości, aby – w razie potrzeby odtworzenia danych organizacji – system został zainfekowany przez niewyczyszczone dane.

LET'S TALK ABOUT IT!

Zamiast w razie cyberataku zastanawiać się, czy płacić okup przestępcy, warto już dziś podjąć stosowne kroki w celu ochrony danych. W naszych czasach nie należy lekceważyć pytań o cyberbezpieczeństwo swojej organizacji i przygotowanie pracowników na wypadek zaszyfrowania. Ważne jest, aby weryfikować, sprawdzać, zastanawiać się, rozważać i testować różne scenariusze.

Firma Servers24.pl we współpracy z Dell Technologies jest w stanie pomóc klientowi w zdefiniowaniu potrzeb, zaprojektowaniu, przetestowaniu (Proof of Concept) oraz wdrożeniu systemu ochrony danych, dzięki czemu najbardziej wyszukane ataki cyfrowe nie będą w stanie uniemożliwić odtworzenia krytycznych danych organizacji.

Polityka® Bezpieczeństwa

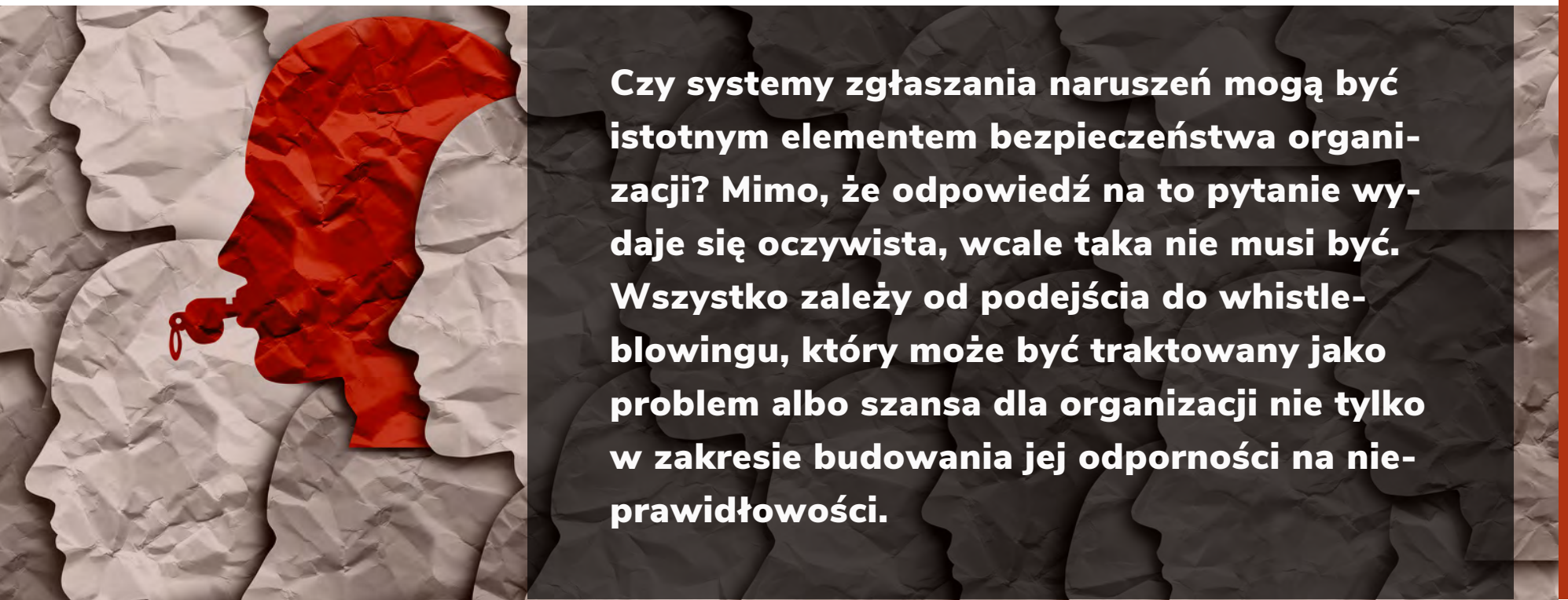
ANALIZA FORMALNA WYCIEKU DANYCH

MASZ 72 GODZINY NA POWIADOMIENIE UODO O INCYDENCIE

SPRAWDŹ OFERTĘ

WHISTLEBLOWING. ISTOTNY ELEMENT SYSTEMU BEZPIECZEŃSTWA

Rafał Hryniewicz
E-nform



Czy systemy zgłaszania naruszeń mogą być istotnym elementem bezpieczeństwa organizacji? Mimo, że odpowiedź na to pytanie wydaje się oczywista, wcale taka nie musi być. Wszystko zależy od podejścia do whistleblowingu, który może być traktowany jako problem albo szansa dla organizacji nie tylko w zakresie budowania jej odporności na nieprawidłowości.

TYTUŁEM WSTĘPU

Zanim przejdziemy do omówienia roli whistleblowingu w systemie bezpieczeństwa organizacji, warto wyjaśnić co się kryje za tymi pojęciami. Poprzez pojęcie whistleblowingu należy w uproszczeniu rozumieć zgłaszanie przez osoby związane z daną organizacją (zazwyczaj pracowników) naruszeń, do których doszło w tej organizacji lub które miały miejsce w związku z jej działalnością. Osoby zgłaszające często nazywa się sygnalistami i tym terminem będziemy się posługiwali w dalszej części niniejszego artykułu.

Natomiast system bezpieczeństwa organizacji to zaprojektowane i skoordynowane wewnętrznie przedsięwzięcia m.in. na płaszczyźnie organizacyjnej, technicznej i prawnej (proceduralnej) umożliwiające podmiotowi realizację w sposób bezpieczny i skuteczny jego krótko- i długoterminowych celów.

Widząc te dwie definicje trudno nie zauważyć istotnych korelacji między nimi. Niewątpliwie whistleblowing może wpisywać się w działania organizacji mające na celu zwiększenie jej bezpieczeństwa w drodze do realizacji wyznaczonych celów. Jednakże zakres wpływu whistleblowingu na owo bezpieczeństwo nie jest już taki oczywisty, tym bardziej że w Polsce na whistleblowing bardzo często spogląda się głównie przez wąski pryzmat wymagań prawnych i wynikających z nich sankcji. Pochylmy się więc po kolei nad poszczególnymi obliczami whistleblowingu mogącymi wzmacniać, a nawet współtworzyć system bezpieczeństwa organizacji.

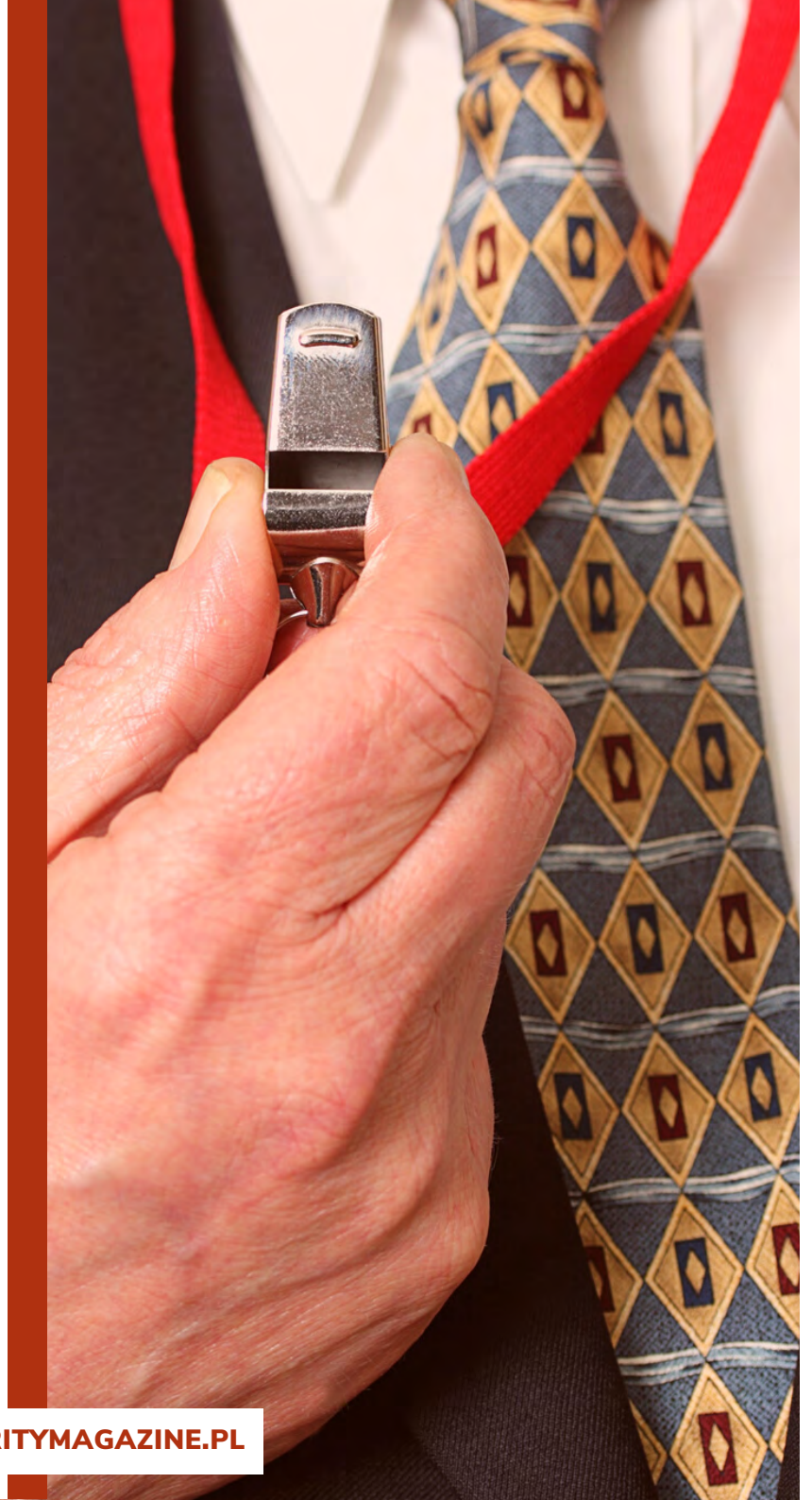
WHISTLEBLOWING JAKO ELEMENT SYSTEMU ZGODNOŚCI Z WYMAGANIAMI PRAWA

Zgodnie z przepisami dyrektywy Parlamentu Europejskiego i Rady 2019/1937

w sprawie ochrony osób zgłaszających naruszenia prawa Unii (tzw. Dyrektywa o sygnalistach) wiele podmiotów w Polsce będzie obowiązanych, pod groźbą sankcji, do wdrożenia i respektowania wymagań tego europejskiego aktu prawnego. Co do zasady wszystkie prawne podmioty publiczne (z ewentualnymi wyłączeniami przewidzianymi polską ustawą implementującą), a także prawne podmioty prywatne, zatrudniające co najmniej 50 pracowników, będą musiały stworzyć warunki do skutecznego przyjmowania i wyjaśniania zgłoszeń o naruszeniach prawa oraz do skutecznej ochrony sygnalistów. Wdrożenie systemu whistleblowingowego zgodnego z wymaganiami prawnymi będzie więc warunkiem koniecznym do uniknięcia przewidzianych prawem sankcji. W tym kontekście warto również wspomnieć, że sektor finansowy w Polsce już od kilku lat posiada konkretne regulacje w obszarze anonimowego zgłaszania naruszeń prawa i standardów etycznych.

SKUTECZNE UJAWNIANIE NARUSZEŃ

Praktyka, jak i badania zagadnienia pokazują, że systemy whistleblowingowe w porównaniu z innymi mechanizmami wykrywczymi stanowią **najskuteczniejsze narzędzie do detekcji nadużyć w organizacji**. Z ostatniego (2022 r.) raportu z badań nad tematyką nadużyć przeprowadzonych przez Association of Certified Fraud Examiners wynika, że skuteczność whistleblowingu w wykrywaniu nieprawidłowości w organizacji określono na poziomie 42%, co zdeklasowało inne środki detekcyjne, takie jak audyt wewnętrzny (16%), nadzór przełożonych (12%) czy audyt zewnętrzny (4%). Co więcej, z przytoczonych badań ACFE wynika również, że organizacje z systemami whistleblowingowymi **znacznie szybciej i częściej wykrywały naruszenia** niż organizacje bez takich mechanizmów oraz **ponosiły dwukrotnie mniejsze straty**. Idąc za tymi danymi można dojść do oczywistego wniosku, że skuteczne systemy whistleblowingowe nie tylko pomagają ograniczać straty wynikające z uszczuplenia majątku czy też utraconych korzyści. Takie systemy - co powinno być istotne dla wielu organizacji – wspierają także organizację w ochronie jej wizerunku wewnętrznego (zapobieganie utraty zaufania ze strony pracowników), jak i zewnętrznego (przeciwdziałanie utraty zaufania ze strony kontrahentów, udziałowców, czy też akcjonariuszy).



SKUTECZNA IDENTYFIKACJA ZAGROŻEŃ I PODATNOŚCI

Nie jest tajemnicą, że przeciwdziałanie nieprawidłowościom jest bardziej racjonalne i skuteczniejsze od ich zwalczania. Taki sposób podejścia wymaga jednak działań proaktywnych, a przede wszystkim wiedzy i dobrej znajomości organizacji oraz jej procesów. Rzetelnie i odpowiedzialnie wdrożone systemy whistleblowingowe mogą pomóc w skutecznej identyfikacji różnego rodzaju podatności czy też zagrożeń, których materializacja mogłaby spowodować szkody w organizacji na różnych płaszczyznach jej funkcjonowania.

Szybkie ujawnianie obszarów ryzyka i racjonalne zarządzanie nimi pozwala nie tylko na unikniecie strat materialnych czy też wizerunkowych, ale także na wyeliminowanie dodatkowych kosztów związanych z „obsługą" nieprawidłowości, do której ostatecznie mogłoby dojść.

Co istotne, informacja o takich zagrożeniach czy podatnościach (np. w systemach kontroli) może wynikać bezpośrednio ze zgłoszenia sygnalisty, świadomego, że organizacja takich informacji potrzebuje, jak również pośrednio, jako wynik analizy treści zgłoszenia (wnioskowanie z opisu problemu o jego przyczynach i związanych z tym podatnościach lub lukach w procesach).

WHISTLEBLOWING – PROBLEM CZY SZANSA DLA BEZPIECZEŃSTWA ORGANIZACJI?

Bazując na doświadczeniach z whistleblowingiem w Polsce, można pokusić się o stwierdzenie, że dla większości organizacji sektora prywatnego oraz publicznego podstawową motywacją do wdrożenia systemów whistleblowingowych będzie konieczność dostosowania się do wymagań prawa krajowego w obszarze ochrony sygnalistów.

Efektem pośrednim takich implementacji może być zaś wzmocnienie systemu bezpieczeństwa organizacji dzięki możliwości szybszej detekcji naruszeń lub zagrożeń. Wyrażenie „może być" jest tu kluczowe, bowiem część podmiotów obowiązanych do wdrożenia takich rozwiązań może je traktować nie jako istotny element systemu przeciwdziałania nadużyciom lecz jako tzw. „generator problemów', którymi organizacja będzie musiała się zajmować, w tym angażować w ten proces część swoich zasobów. Nie da się ukryć, że przy skutecznie działających systemach zgłaszania naruszeń, decydenci niejednokrotnie będą musieli wychodzić ze swojej strefy komfortu i podejmować nierzadko trudne decyzje (np. personalne).

Nie trzeba chyba jednak nikogo przekonywać, że zarządzanie problemem na jego wczesnym etapie jest znacznie bardziej racjonalne, efektywne i bezpieczne dla organizacji niż mierzenie się z nim, kiedy się rozrośnie i skomplikuje.

Dla racjonalnie myślącej i działającej osoby zarządzającej danym podmiotem, whistleblowing to niezwykle cenne i skuteczne źródło informacji, które może istotnie przyczynić się podniesienia bezpieczeństwa organizacji w znacznie szerszym kontekście.

WHISTLEBLOWING W SYSTEMIE BEZPIECZEŃSTWA ORGANIZACJI – SZERSZA PERSPEKTYWA

Jeżeli potraktujemy whistleblowing jako cenne źródło informacji o organizacji, to nic nie stoi na przeszkodzie by wykorzystać jego mechanizmy do budowania systemowego bezpieczeństwa rozumianego znacznie szerzej niż „tylko" przeciwdziałanie nadużyciom i zagrożeniom. Wykorzystanie funkcjonującego w organizacji systemu whistleblowingowego do przekazywania innych istotnych dla niej informacji, może budować jej bezpieczeństwo na różnych płaszczyznach.

Na przykład, dzięki informacjom o (a) nieracjonalnych kosztach (np. zawyżone wydatki), (b) nieefektywnych procesach wewnętrznych (np. produkcyjnych) czy też (c) pomysłach lub usprawnieniach możemy wzmacniać bezpieczeństwo ekonomiczne i organizacyjne podmiotu, w tym zabezpieczać jego ciągłość działania.

Na poziomie zarządczym systemy whistleblowingowe mogą istotnie wspierać procesy decyzyjne zarówno o charakterze operacyjnym czy też strategicznym. Natomiast na poziomie wykonawczym tego typu rozwiązania pozwalają budować zaangażowanie pracowników oraz zaufanie do organizacji, która wsłuchuje się w ich głosy. Systemy whistleblowingowe mogą stanowić także pewnego rodzaju wentyl bezpieczeństwa dla pracowników, pozwalając im wyrazić swoje niezadowolenie lub frustracje, co minimalizuje ryzyko utraty wizerunku organizacji w wyniku wywlekania jej wewnętrznych spraw na światło dzienne.

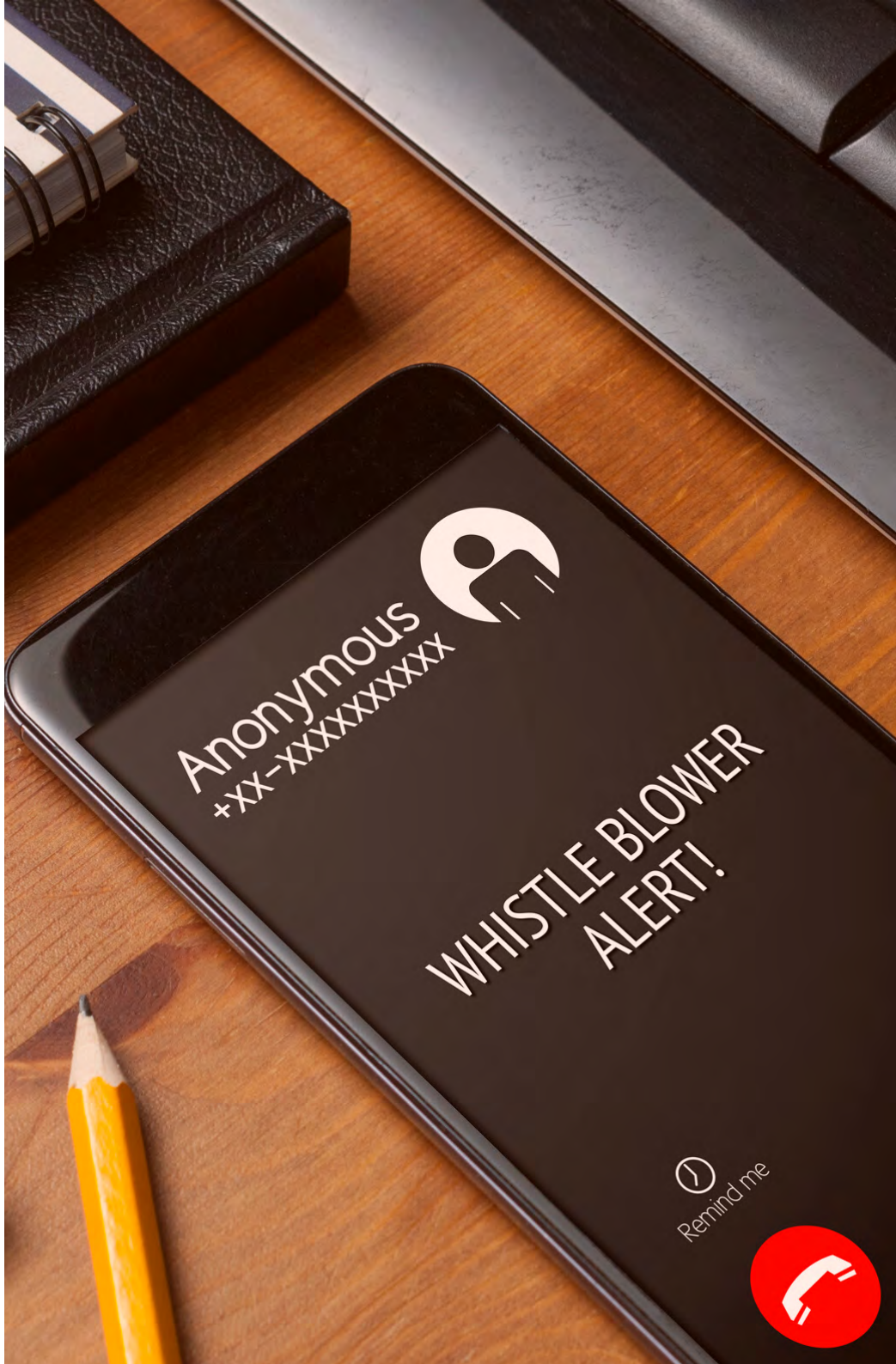
Z takiej perspektywy whistleblowing może wzmacniać bezpieczeństwo kadrowe podmiotu, które jest często fundamentem zapewnienia ciągłości działania poszczególnych procesów.

Oczywiście, można zarzucać, że takie podejście znacznie wykracza poza ramy klasycznego whistleblowingu. To prawda, ale mechanizmy systemów whistleblowingowych, m.in. takie jak bezpieczne i anonimowe kanały komunikacji, proces zarządzania zgłoszeniem czy przyjęte zasady ochrony osób dokonujących zgłoszeń mogą stanowić fundament dla otwartego oraz bezpiecznego dialogu budującego nie tylko bezpieczeństwo organizacji.

PODSUMOWANIE

Nie ulega wątpliwości, że whistleblowing jako źródło cennych informacji może być fundamentem systemu bezpieczeństwa organizacji. Ale to, w jaki sposób organizacja będzie go wykorzystywała w zakresie podnoszenia jej szeroko rozumianego bezpieczeństwa, będzie przede wszystkim pochodną nastawienia kierownictwa do tego zagadnienia. Jeżeli decydenci będą traktowali to narzędzie jako zło konieczne, to nie będzie ono skuteczne nawet w przeciwdziałaniu nieprawidłowościom. Natomiast na tych, dla których whistleblowing stanowi szansę dla doskonalenia organizacji, z pewnością czekają niemałe wyzwania.

Wdrożenie skutecznego systemu whistleblowingowego nastawionego na szeroki zakres informacji to proces często złożony, żmudny i czasochłonny, wymagający zaangażowania oraz uczciwego i konsekwentnego działania. Jednakże potraktowanie takiego systemu jako inwestycji w szeroko pojęte bezpieczeństwo organizacji może jej przynieść ogromne korzyści.



Rzetelny® Regulamin

DYREKTYWA OMNIBUS

DOSTOSUJ Z NAMI SWÓJ SKLEP
DO NOWYCH PRZEPISÓW

SPRAWDZAM OFERTĘ

SECURITYMAGAZINE.PL

INSIDER THREAT, CZYLI NAJCIEMNIEJ POD LATARNIĄ

Grzegorz Dobromiński
Secito – Security Hub

Czy zastanawiasz się, jak bardzo nieuczciwy pracownik może zaszkodzić Twojej firmie? Wzrost incydentów bezpieczeństwa o 44,3% w 2021 roku, z pracownikami jako źródłem zagrożenia, pokazuje, że zagrożenie jest realne i rośnie. Jak skutecznie zarządzać ryzykiem wewnętrznym?

W kwietniu 2022 roku Gartner opublikował „Market Guide for Insider Risk Management Solutions” w którym informuje, że ilość incydentów bezpieczeństwa, których źródłem byli pracownicy, wzrosła o 44,3% w roku 2021 w stosunku do roku 2020. Badane organizacje wydały średnio 34% więcej na walkę z zagrożeniami wewnętrznymi w roku 2021, niż miało to miejsce w 2020. Ośrodek badawczy Ponemon Institute, opublikował w 2022 roku raport „Cost of Insider Threats Global Report” w którym podaje kolejne twarde liczby. W 278 badanych organizacjach (na terenie Europy), odnotowano ponad 6800 incydentów tego typu, a średni koszt ich obsługi rocznie, wyniósł ponad 15 milionów dolarów.

MINIMALIZACJA RYZYKA

Większość takich zdarzeń wynika z zaniedbania czy błędów (56% według Ponemon Institute). 18% jest powiązane z kradzieżą poświadczeń użytkownika. Jednak aż 26% wynika z działań o podłożu kryminalnym. Podejmując temat zarządzania ryzykiem wewnętrznym (ang. Insider Risk Management), powinniśmy działać kompleksowo. Do rozwiązań technologicznych, konieczne jest dołożenie środków organizacyjnych i prawnych.

ROZWIĄZANIA ORGANIZACYJNE

Zacznijmy od bardziej „miękkich” środków bezpieczeństwa. Kwestie organizacyjne, np. umowy, szkolenia i przekazywanie informacji o kulturze organizacji, mogą zniechęcić potencjalnego oszusta do podejrzanych działań.

HR

Proces rekrutacji - to tu zaczyna się weryfikacja osoby, pod kątem referencji, doświadczenia czy luk w życiorysie. Na tym etapie możemy uzyskać pierw-

sze informacje na temat tego, czy danej osobie możemy zaufać.

Umowy i klauzule

Po pomyślnie zakończonym procesie rekrutacji, kolejne elementy zabezpieczenia wprowadzić możemy na polu zawieranych umów. To etap, na którym zawierane są umowy o poufności (NDA) i jeśli jest to uzasadnione, o zakazie konkurencji. W przypadku tych drugich, upewnijmy się, że umowa będzie skuteczna i możliwa do wyegzekwowania, choćby z uwagi na ustalony czas jej trwania czy wynagrodzenia po ustaniu zatrudnienia.

Polityki bezpieczeństwa i procedury

Gdy jesteśmy przy onboardingu, do akcji wchodzą polityki bezpieczeństwa, procedury i regulaminy. Zapoznajemy osobę z zasadami jakie panują w organizacji. Warto pamiętać, aby przekazać informacje o tym, co stanowi tajemnicę przedsiębiorstwa. To szalenie istotny element, w przypadku ewentualnego konfliktu. Dokumenty te, powinny podlegać przeglądom, aktualizacjom a osoby, które zobligowano do ich przestrzegania, cyklicznie uświadamiane co do ich zapisów.

Gdy planujemy prowadzić działania mające na celu np. monitorowanie aktywności pracownika, pamiętajmy też o tym, aby uprzedzić go o tym, choćby w ramach polityki bezpieczeństwa.

Szkolenia

Przed realizacją zadań służbowych, warto pracownika przeszkolić. Szkolenia z cyberbezpieczeństwa, ochrony danych osobowych, etyki i zasad postępowań są istotnym elementem, za pomocą którego możemy zaakcentować nacisk, jaki kładziemy na ochronę informacji. Warto takie szkolenia przeprowadzać cyklicznie oraz weryfikować ich skuteczność np. testami socjotechnicznymi.

Analiza zachowania

Warto zwrócić uwagę na kwestie behawioralne. Takie zachowania jak praca w nietypowych godzinach, częste spory z pracownikami, nagła zmiana statusu finansowego, spadek wydajności czy częste opuszczanie pracy, mogą wzbudzić podejrzenia. Same w sobie mogą oznaczać, na przykład, zmiany w życiu prywatnym pracownika, ale w połączeniu z sygnałami z urządzeń czy systemów, o których poniżej, otrzymujemy szerszy kontekst, pozwalający na wyciągnięcie konkretnych wniosków.

ROZWIĄZNIA TECHNICZNE

Przejdźmy do rozwiązań technicznych. Będziemy mieli tutaj systemy analizujące zachowania i działania pracowników, rozwiązania ułatwiające zarządzanie alarmami czy wreszcie rozwiązania sprzętowe, łączące w sobie wiele funkcjonalności.

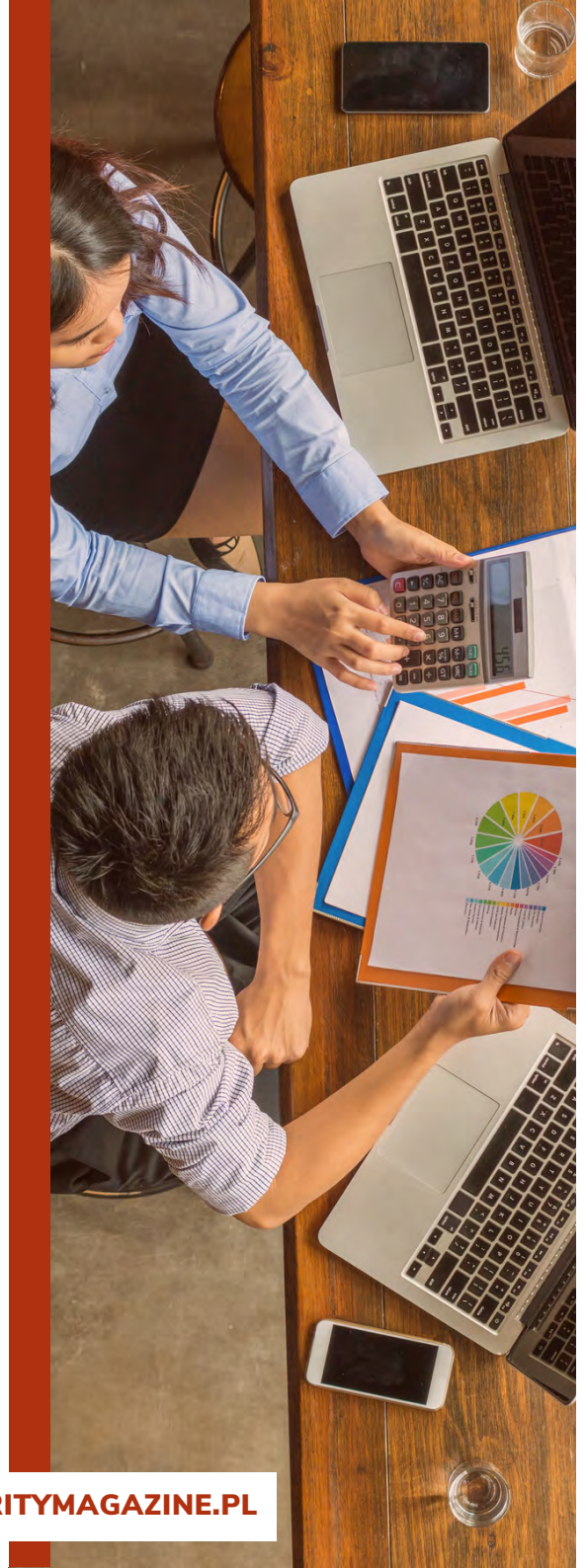
DLP

Jako podstawę weryfikowania aktywności użytkowników, warto zastosować rozwiązania analizujące operacje wykonywane na danych, takie jak np. DLP (Data Loss Prevention). Podnoszą one poziom bezpieczeństwa przed kradzieżą danych czy przypadkowym wyciekiem.

Bazują w głównej mierze na ciągłej analizie działań podejmowanych przez użytkownika, zgodnie z ustalonymi politykami.

SIEM

W sukurs rozwiązaniom DLP, idą systemy SIEM (Security Information and Event Management). Dzięki połączeniu funkcji takich, jak zbieranie i przechowywanie logów, gromadzeniu danych związanych z bezpieczeństwem z wielu źródeł (zapory firewall, serwery, routery, antywirusy) oraz monitorowaniu, analizie, wizualizacji i korelacji zdarzeń, stają się centralnym systemem bezpieczeństwa.



Systemy tego typu, generują alarmy zgodnie z zasadami jakie skonfigurujemy i znacznie ułatwiają zarządzanie informacjami, zwłaszcza w bardziej rozbudowanych środowiskach.

Monitoring i kontrola

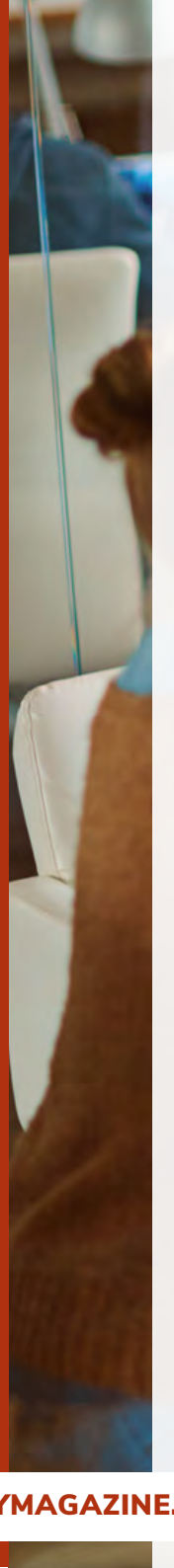
Nie możemy zapomnieć o monitorowaniu i kontroli dostępu do danych, które znajdują się w posiadaniu firmy. Dobrą praktyką jest stosowanie polityki minimalnych uprawnień, czyli dostępu tylko do wymaganych informacji. Należy również mieć oko na nieudane próby uzyskania dostępu do danych, do których osoba nie powinna się dostać.

UTM

Monitorować należy również ruch sieciowy, na okoliczność nietypowych zachowań takich jak niestandardowe ilości pobieranych czy wysyłanych danych, połączenia z podejrzanymi usługami, adresami. Te oraz wiele innych zadań, realizują urządzenia typu UTM (ang. Unified Threat Management). Podobnie podejrzane mogą być na przykład nienaturalne godziny aktywności. Jak mawia przysłowie – gdy kota nie ma, myszy harcują.

Inne płaszczyzny, które należy uwzględnić

Pod uwagę należy wziąć również takie kwestie jak praca zdalna, która może być polem do nadużyć i oszustw, a także aktywność pracowników z wykorzystaniem usług w chmurze czy bezpieczeństwo i monitoring urządzeń mobilnych. Innymi systemami na które warto zwrócić uwagę są m.in. PAM (Privileged Access Management), UEBA (User and Entity Behavior Analytics) czy IAM (Identity and Access Management).



ŚRODKI PRAWNE

Czy uda nam się zbudować system w 100% odporny na zagrożenie, jakim jest nieuczciwy pracownik? Nigdy. Warto jednak pracować nad tym, aby w ramach możliwości, maksymalizować swoje szanse w tym starciu. Gdy już dojdzie do incydentu, a taka osoba wykradnie firmowe dane, przekaże dostęp do systemów osobie nieupoważnionej czy np. dopuści się fraudu, organizacja musi być w stanie udowodnić, że podjęła kroki dążące do tego, by ryzyko minimalizować. Udowodnić, że zasoby które uległy upublicznieniu bądź trafiły w ręce konkurencji, stanowiły tajemnicę przedsiębiorstwa.

Pamiętajmy również o przepisach prawnych, które chronią firmy, takich jak, na przykład:

- **Art. 100 § 2 pkt 4 Kodeksu pracy**, który traktuje o tym, że pracownik zobowiązany jest dbać o dobro zakładu pracy, chronić jego mienie oraz zachować w tajemnicy informacje, których ujawnienie mogłoby narazić pracodawcę na szkodę.
- **Zgodnie z art. 122 Kodeksu pracy**, nieuczciwy pracownik ponosi odpowiedzialność odszkodowawczą w pełnej wysokości, bez ograniczeń kwotowych.
- **Ustawa z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji,** uznaje za taki czyn m.in. przekazanie, ujawnianie lub wykorzystanie cudzych informacji stanowiących tajemnicę przedsiębiorstwa albo ich nabycie od osoby nieuprawnionej, o ile zagraża lub narusza interes przedsiębiorcy.

PODSUMOWANIE

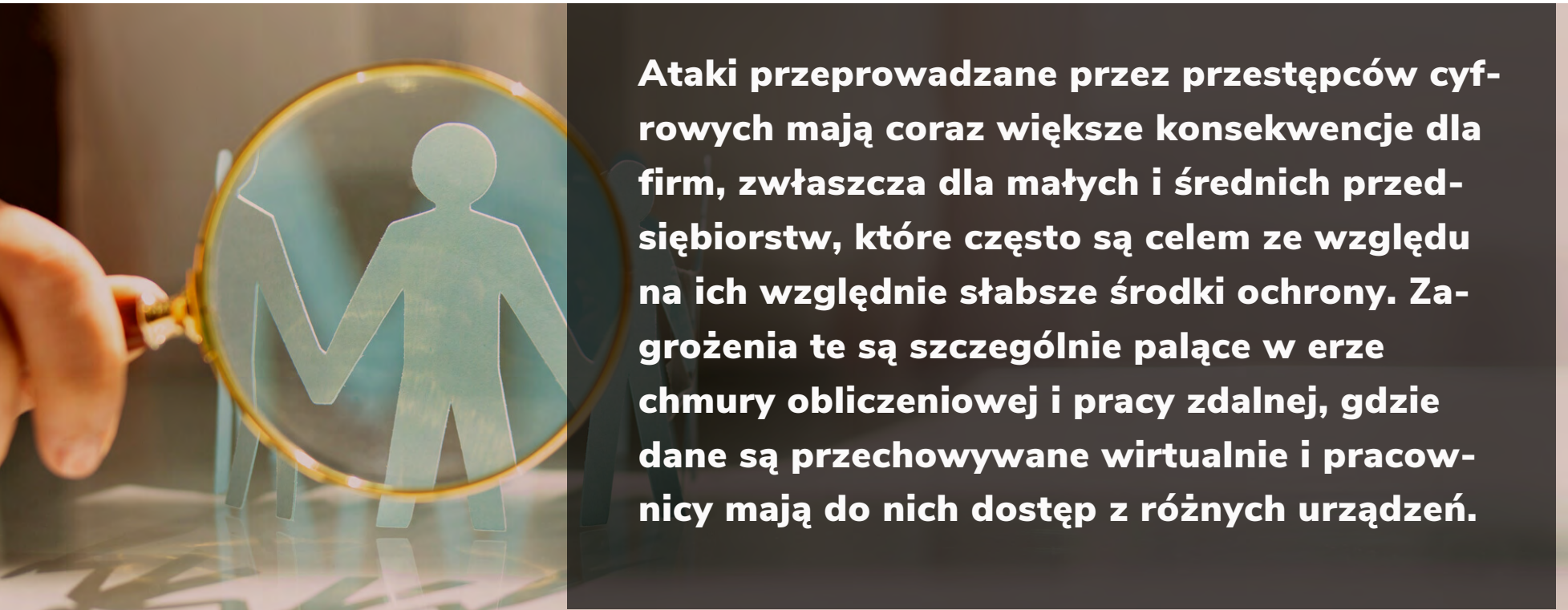
Z perspektywy organizacji, mamy zatem przynajmniej trzy płaszczyzny, na których możemy zabezpieczyć się przed nieuczciwym pracownikiem. Przybliżyłem je począwszy od organizacyjnych, przez techniczne które budzą największe zainteresowanie, a na prawnych skończywszy. Niemniej jednak, nie należy kwestii prawnych traktować jako najmniej ważnych. Gdy przysłowiowe mleko już się rozleje, to właśnie na tym polu rozegra się batalia.

Czy może być ona skuteczna? Tak. Moje doświadczenie jako świadka w postępowaniach sądowych, prowadzonych przeciwko nieuczciwym pracownikom pokazuje, że można i trzeba. Jakość zebranych dowodów przez organizację i odpowiednio prowadzona dokumentacja, mogą mieć kluczowe znaczenie.


Polityka ®
Bezpieczeństwa
SZKOLENIA
Z OCHRONY DANYCH
OSOBOWYCH
SPRAWDŹ OFERTĘ

CYBERBEZPIECZEŃSTWO I JEGO SŁABE OGNIWO – CZŁOWIEK

Jarosław Gniado
ENGAVE S.A.



Ataki przeprowadzane przez przestępców cyfrowych mają coraz większe konsekwencje dla firm, zwłaszcza dla małych i średnich przedsiębiorstw, które często są celem ze względu na ich względnie słabsze środki ochrony. Zagrożenia te są szczególnie palące w erze chmury obliczeniowej i pracy zdalnej, gdzie dane są przechowywane wirtualnie i pracownicy mają do nich dostęp z różnych urządzeń.

Ataki cybernetyczne mogą spowodować ogromne straty finansowe dla przedsiębiorstw. Koszty związane z naprawą uszkodzonych systemów, odtwarzaniem danych, płaceniem okupów lub nawet opłacaniem kar nałożonych przez organy regulacyjne mogą być ogromne. Poza stratami finansowymi, ataki te prowadzą również do poważnych konsekwencji związanych z utrata reputacji. Gdy firma staje się ofiarą ataku, zaufanie jej klientów może zostać zachwiane, co prowadzi do utraty zarówno obrotów jak i wiarygodności na rynku. Dodatkowo, naruszenie przepisów dotyczących ochrony danych osobowych może prowadzić do konsekwencji prawnych, takich jak kary grzywny lub procesy sądowe.

Każde przedsiębiorstwo posiada cenne zasoby, których utrata lub uszkodzenie może mieć poważne skutki. Dane klientów, informacje biznesowe, poufne informacje handlowe i strategie marketingowe, kanały komunikacji z klientami oraz środki finansowe to tylko kilka przykładów takich zasobów. Cyberatak może prowadzić do utraty tych cennych aktywów, co może wpłynąć na trwałość działalności firmy.

Aby skutecznie chronić się przed cyberatakami, firmy powinny opracować kompleksowe strategie cyberbezpieczeństwa, które obejmują ochronę danych, infrastruktury, łańcuchów dostaw oraz przestrzeganie przepisów i regulacji. Najważniejsze jest jednak regularne szkolenie pracowników i przeprowadzanie testów świadomości, aby zapobiegać cyberatakom i minimalizować ryzyko wynikające z ludzkich błędów. W dzisiejszym cyfrowym świecie przedsiębiorstwa stają się coraz częściej ofiarami cyberprzestępców. Cyberataki są motywowane różnymi czynnikami, a ich konsekwencje mogą być katastrofalne.

MOTYWY CYBERPRZESTĘPCÓW

Jakie motywy mają najczęściej hakerzy atakujący firmy? Wiadomo, że pieniądze. Cyberprzestępczość to gigantyczny „przemysł". Straty firm i osób fizycznych – czyli dochody z cyberprzestępczości wyniosły w 2022 roku na całym świecie 110 mld dolarów, a w Polsce - 4,8 mld zł. Ale nie tylko pieniądze są motywatorem ataku, to również szantaż, sabotaż, kradzież poufnych informacji, szukanie słabych punktów, osłabienie reputacji, szpiegostwo przemysłowe, wandalizm.

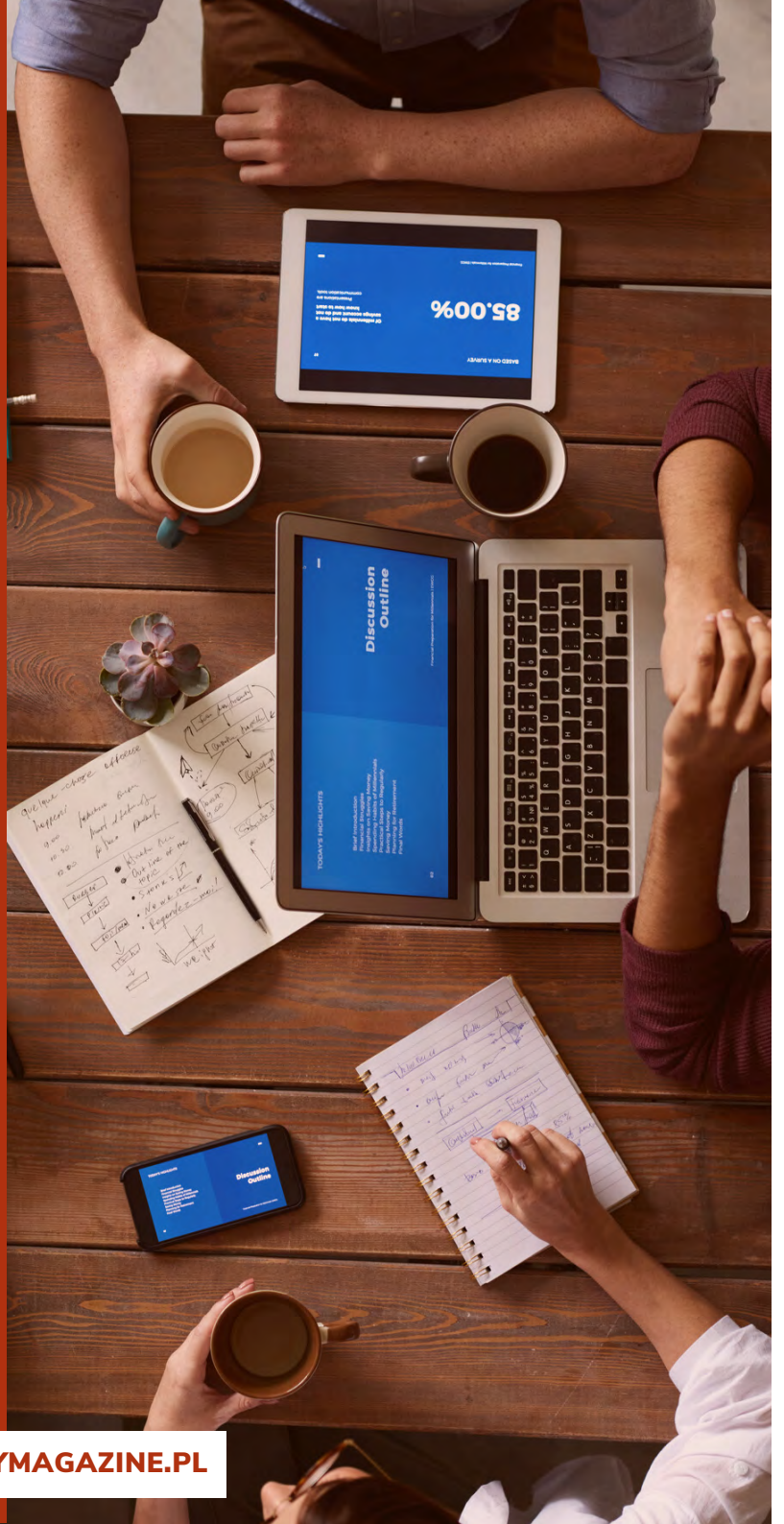
Niezależnie od motywów cyberataków, ich skutki dla firm i pracowników mogą być poważne oraz długotrwałe. Dlatego musimy być świadomi różnych sposobów, którymi cyberprzestępcy mogą atakować firmy. Poniżej przedstawiamy najczęstsze metody ataku na firmy:

- atak poprzez człowieka,
- atak poprzez łącze internetowe,
- atak poprzez podrzucenie zainfekowanego nośnika danych,
- kradzież lub "wypożyczenie" firmowego komputera,
- skrzynka pocztowa (e-mail),
- instalacja oprogramowania prywatnego na służbowym urządzeniu,
- nasłuchiwanie firmy.

Pracownicy mają istotny wpływ na ochronę danych, zarówno jako pierwsza linia obrony, jak i potencjalne źródło zagrożeń.

Cyberbezpieczeństwo to nie tylko kwestia narzędzi i technologii, ale także rola i postawa pracowników w firmie. W kontekście bezpieczeństwa sieciowego grupy pracowników odgrywają różne role. Specjaliści od cyberbezpieczeństwa opracowują procedury i politykę bezpieczeństwa, zarządzają oprogramowaniem, dbają o fizyczne zabezpieczenia sprzętu oraz kontrolują dostęp do danych.

Pracownicy szeregowi, choć nie posiadają takiej wiedzy technicznej jak specjaliści od cyberbezpieczeństwa, również są kluczowymi uczestnikami w procesie cyberbezpieczeństwa. To właśnie oni codziennie korzystają z systemów informatycznych i mają bezpośredni dostęp do danych firmy. Niestety, to także wśród pracowników można znaleźć słabe punkty, które mogą być wykorzystane przez cyberprzestępców.



SŁABE PUNKTY

Jednym z najczęstszych słabych punktów jest brak świadomości i odpowiedniego szkolenia pracowników w zakresie cyberbezpieczeństwa. Wielu z nich może nie zdawać sobie sprawy z potencjalnych zagrożeń, jakie mogą wynikać z nieodpowiedniego korzystania z technologii. Otwieranie podejrzanych załączników e-mailowych, klikanie w podejrzane linki czy udostępnianie poufnych informacji na niewłaściwych platformach - to tylko kilka przykładów błędnych praktyk, które mogą otworzyć furtkę dla ataków cybernetycznych.

Ponadto, brak odpowiednich polityk bezpieczeństwa i procedur w firmie może również stanowić słaby punkt. Jeśli pracownicy nie są świadomi oczekiwanych standardów dotyczących bezpieczeństwa danych i nie mają jasnych wytycznych, jak postępować w przypadku podejrzenia ataku, może to prowadzić do błędnych decyzji i potencjalnych naruszeń bezpieczeństwa.

Musimy też mieć świadomość, że zadbanie o cyberbezpieczeństwo nie jest jednorazowym zadaniem, ale procesem ciągłym. Wraz z rozwojem technologii i ewolucją zagrożeń cybernetycznych, firmy muszą regularnie aktualizować swoje strategie i narzędzia, aby nadążyć za zmieniającym się krajobrazem cyfrowych zagrożeń. To wymaga zaangażowania wszystkich pracowników i utrzymania wysokiej świadomości w tym zakresie.

Choć technologia odgrywa istotną rolę w ochronie przed cyberatakami, to człowiek nadal pozostaje jednym z najważniejszych czynników ryzyka. Bez odpowiedniej świadomości i zaangażowania pracowników, żadne narzędzia ani systemy nie będą w stanie zapewnić pełnej ochrony przed atakami cybernetycznymi. Dlatego tak istotne jest budowanie kultury bezpieczeństwa w firmach, w której każdy pracownik rozumie znaczenie cyberbezpieczeństwa i podejmuje odpowiednie działania celem ochrony danych i zasobów przedsiębiorstwa.

WZMACNIANIE ŚWIADOMOŚCI I SZKOLENIA - KLUCZ DO CYBERBEZPIECZEŃSTWA

Podnoszenie świadomości pracowników w zakresie cyberbezpieczeństwa jest kluczowe dla ochrony przed atakami.

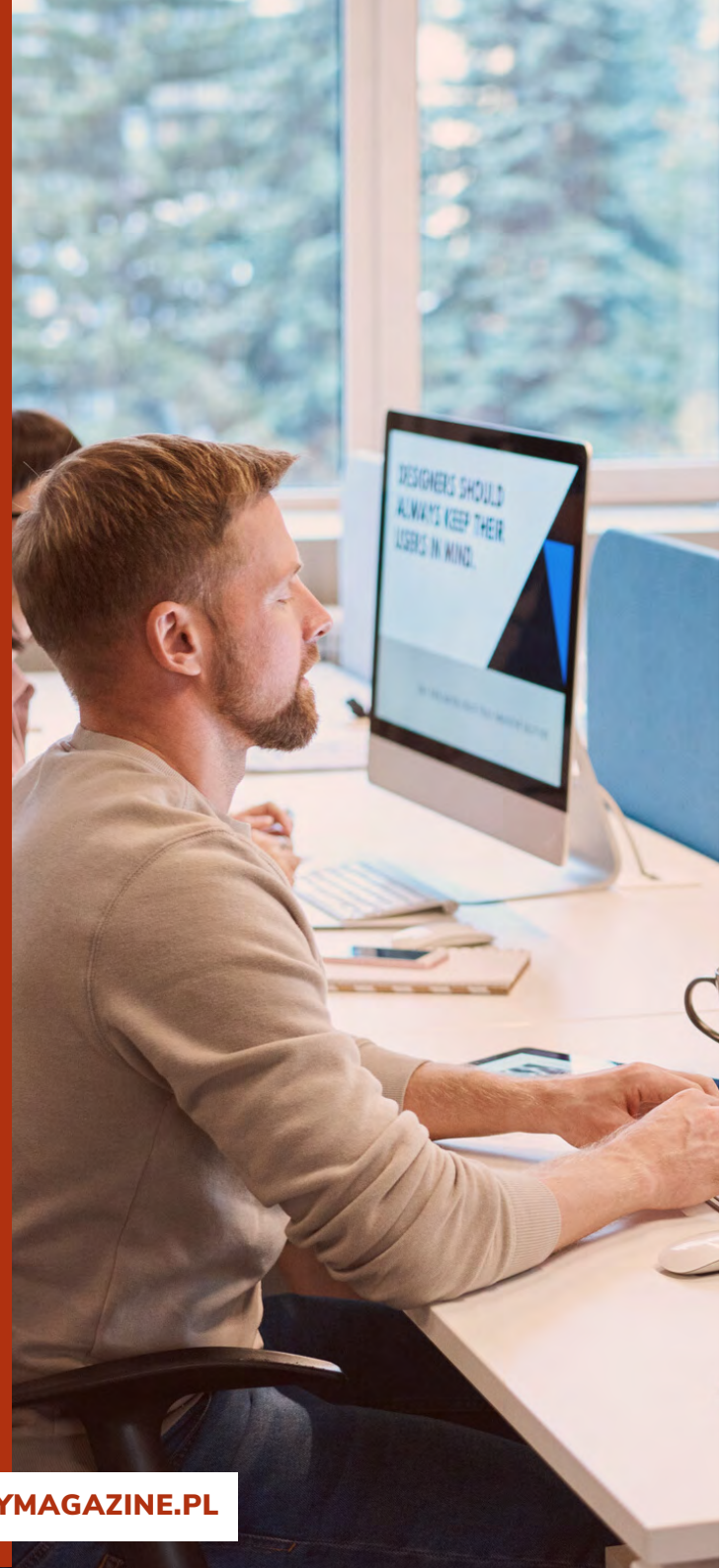
Jednym z najważniejszych elementów w zapewnianiu skutecznej ochrony przed cyberatakami jest odpowiednie szkolenie pracowników. Brak świadomości w zakresie potencjalnych zagrożeń i nieodpowiednie praktyki są częstymi słabymi punktami w firmach. Stąd trzeba zainwestować w programy szkoleniowe, które pomogą pracownikom zrozumieć znaczenie cyberbezpieczeństwa i nauczyć ich dobrych praktyk w codziennym korzystaniu z technologii.

APLIKACJE VROWE. ROZWIĄZANIE W SZKOLENIACH Z CYBERBEZPIECZEŃSTWA

Wykorzystanie aplikacji VRowe w procesie szkoleniowym może przynieść liczne korzyści i wzmocnić efektywność nauki.

W ostatnich latach pojawiło się wiele innowacyjnych narzędzi, które wspierają proces szkoleniowy z cyberbezpieczeństwa. Jednym z nich są aplikacje VRowe, wykorzystujące technologię wirtualnej rzeczywistości. Dzięki nim pracownicy mają możliwość praktycznego uczenia się wirtualnych scenariuszy, które odzwierciedlają rzeczywiste zagrożenia i sytuacje, z jakimi mogą się spotkać.

Aplikacje VRowe oferują interaktywne ćwiczenia, w których pracownicy są angażowani w symulacje ataków, rozpoznawanie zagrożeń i podejmowanie odpowiednich działań w celu ochrony danych oraz systemów. Dzięki realistycznym wizualizacjom oraz immersyjnemu doświadczeniu, uczestnicy szkolenia mogą lepiej zrozumieć, jak wyglądają ty-

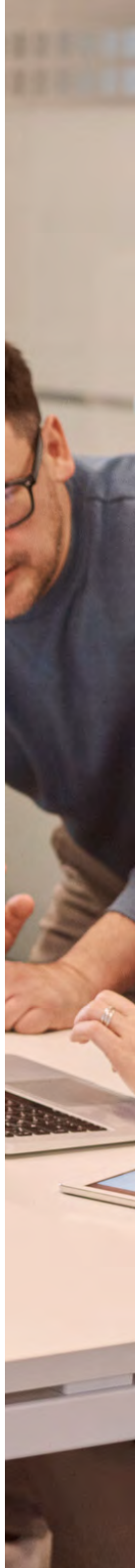


powe ataki i jakie konsekwencje mogą wynikać z błędnych decyzji.

ZALETY SZKOLEŃ Z WYKORZYSTANIEM APLIKACJI VROWE

Wykorzystanie aplikacji VRowe w szkoleniach przynosi szereg korzyści zarówno dla pracowników i dla organizacji.

- **Realistyczne doświadczenie**: Dzięki technologii wirtualnej rzeczywistości, pracownicy mogą doświadczyć sytuacji związanych z atakami cybernetycznymi w kontrolowanym środowisku. To umożliwia im zdobycie praktycznych umiejętności i lepsze przygotowanie do realnych sytuacji.
- **Zwiększona skuteczność nauki**: Aplikacje VRowe angażują zmysły i emocje uczestników, co sprzyja lepszemu zapamiętywaniu informacji oraz zdobywaniu umiejętności praktycznych. Interaktywne ćwiczenia w wirtualnym środowisku są bardziej przystępne i angażujące niż tradycyjne prezentacje lub teoretyczne kursy.
- **Dostosowane scenariusze**: Aplikacje VRowe pozwalają na personalizację i dostosowanie scenariuszy szkoleniowych do specyfiki danej organizacji. Można uwzględnić unikalne zagrożenia, z którymi firma może się spotkać, co zwiększa wartość praktyczną szkolenia.
- **Monitorowanie postępów**: Dzięki aplikacjom VRowe możliwe jest śledzenie postępów uczestników i ocena ich umiejętności w zakresie reagowania na zagrożenia. To umożliwia identyfikację słabych punktów oraz ukierunkowanie dalszego rozwoju szkoleniowego.



PODSUMOWANIE

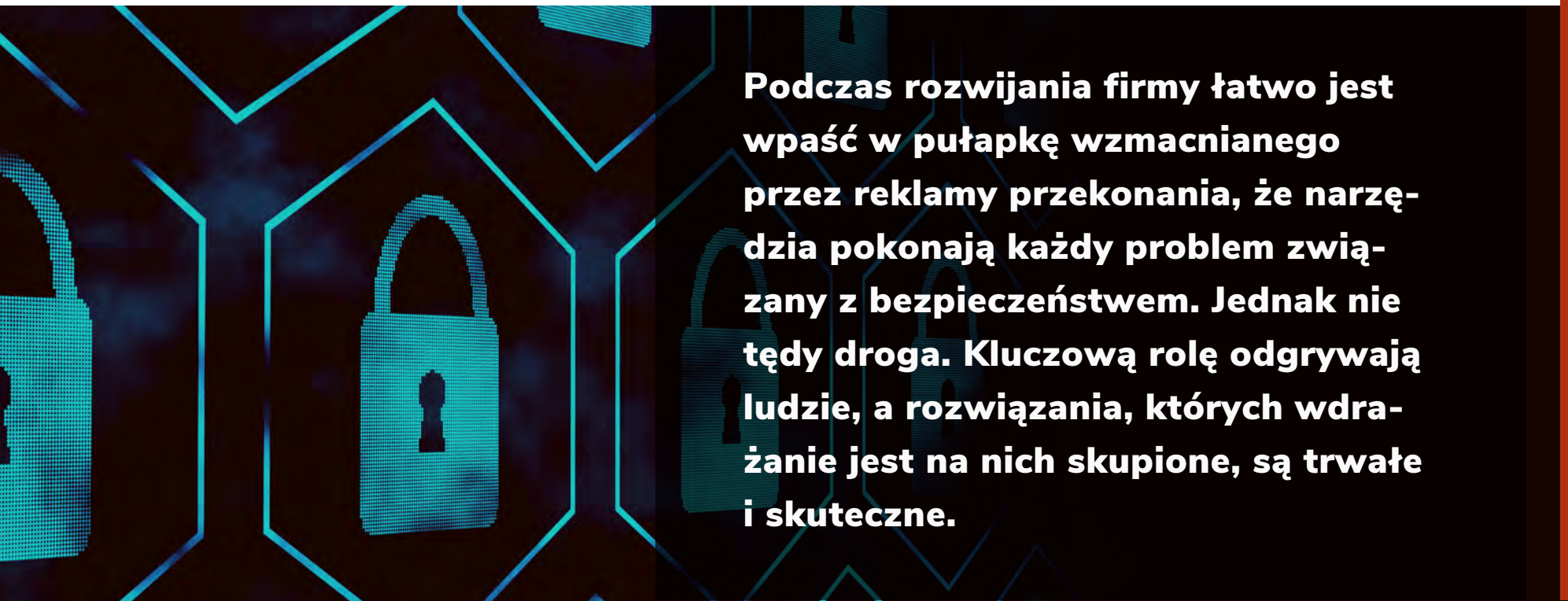
Aby skutecznie chronić przedsiębiorstwo przed cyberatakami, niezbędne jest zwiększenie świadomości pracowników i odpowiednie szkolenia.

Wykorzystanie aplikacji VRowe w procesie szkoleniowym może przynieść liczne korzyści, wzmocnić efektywność nauki oraz przygotować pracowników do realistycznych scenariuszy ataków.

Inwestowanie w szkolenia i nowoczesne technologie to kluczowe elementy w budowaniu kultury cyberbezpieczeństwa i skutecznej ochrony przed zagrożeniami w dzisiejszym dynamicznym środowisku informatycznym.

NARZĘDZIA NIE ROZWIĄŻĄ PROBLEMÓW BEZPIECZEŃSTWA

Adrian Sroka
Security Architect



Podczas rozwijania firmy łatwo jest wpaść w pułapkę wzmacnianego przez reklamy przekonania, że narzędzia pokonają każdy problem związany z bezpieczeństwem. Jednak nie tędy droga. Kluczową rolę odgrywają ludzie, a rozwiązania, których wdrażanie jest na nich skupione, są trwałe i skuteczne.

POKUSA UŻYCIA NARZĘDZI

W pracy często zmagamy się z problemem braku czasu. Chcielibyśmy zaadresować różne obszary działania firmy, jednak nie zawsze są one priorytetowe i wobec tego część z nich odsuwamy na dalszy plan. Między innymi bezpieczeństwo.
Z troską o nie jest jak z polisą ubezpieczeniową. Warto ją mieć, ale na co dzień nie widzimy z niej żadnej korzyści, tylko koszty.

By pracować szybciej i efektywniej, korzystamy z wielu narzędzi. Począwszy od systemów CRM, przez narzędzia do zarządzania publikacjami, aż po te bardziej wyspecjalizowane. Ponadto, poszukując rozwiązań naszych problemów, odnajdujemy opisy narzędzi, dzięki którym inni osiągnęli istotne rezultaty. Możemy więc pomyśleć, że zadbanie o bezpieczeństwo to po prostu dobranie odpowiedniego zestawu narzędzi i skonfigurowanie ich na potrzeby naszej firmy. Wygląda to na wygodną, szybką i niezbyt kosztowną metodę zadbania o bezpieczeństwo.

KONSEKWENCJE ROZPOCZYNANIA OD WDROŻENIA NARZĘDZI

Załóżmy, że byłaby to właściwa droga. Jak wygląda najpopularniejszy scenariusz takiego wdrożenia? Zespół (na przykład, wytwarzający oprogramowanie) pracuje zgodnie z pewnym procesem. Któregoś dnia jedna z osób znajduje informację na przykład o nowym skanerze podatności zależności. Zespół jak dotąd nie skanował tego obszaru, więc wszyscy popierają pomysł, żeby w ten sposób zacząć.

Najpierw instalują i konfigurują całe narzędzie. Następnie wyznaczają wymagany poziom bezpieczeństwa (w tym przypadku np. brak problemów powyżej określonej istotności) i zaczynają pracę nad zwiększaniem bezpieczeństwa z pomocą tego narzędzia.

Pierwsze kilka tygodni to często okres ekscytacji. Wszyscy są zainteresowani tematem i chętnie monitorują wyniki. Przychodzi jednak okres stagnacji oraz coraz rzadszego zaglądania do narzędzia. Zaś ono samo tego bezpieczeństwa zagwarantować nie może.
Dodatkowo część problemów przez nie wykrytych to “false positive”, co często zniechęca. Oczywiście, można by to poprawić i ustawić nowe reguły, ale początkowy entuzjazm już opadł i zespół jest tym mniej zainteresowany.

Często w takiej chwili entuzjazm przechodzi na nowe narzędzie — nową zabawkę. Tak więc może i czujemy, że zadbaliśmy o określony obszar, może nawet raportujemy, że zrobiliśmy coś dla bezpieczeństwa, ale takie podejście nie daje realnych korzyści firmie. Nie porównałbym go ani do słabej polisy, ani nawet do tak bazowego poziomu zabezpieczeń jak apteczka w samochodzie.

NOWA PRACA U PODSTAW

Czy to oznacza, że wybrane narzędzie było złe? Nie.
Czy było źle skonfigurowane? Nie.

To często oznacza, że po prostu było źle wdrożone. Kluczowy jest tu brak zrozumienia potrzeb.

Problem można rozwiązać, poprzez poświęcenie czasu na analizę danego narzędzia i jego konfigurację. Jednak sedno tkwi w tym, że wszyscy użytkownicy, nie tylko osoba konfigurująca narzędzie, muszą być świadomi potrzeb, związanych z określonym obszarem. Muszą rozumieć, czym on jest, dlaczego jest istotny i wiedzieć, jak o niego dbać. Aby zadbać o nowy zakres, musimy więc zacząć od “nowej pracy u podstaw”. Czyli z wiedzą o bezpieczeństwie, jej kluczowym znaczeniu i możliwości włączenia w codzienną pracę należy dotrzeć do każdego pracownika - nie tylko dewelopera, ale także PR-owca czy analityka.

Zaczynanie od narzędzi lub narzucanych odgórnie procedur jest jak wchodzenie na nowy rynek, bez uprzedniego poznania i przygotowania adekwatnych działań. Rozwiązaniem tych problemów jest adresowanie tematów z zakresu bezpieczeństwa według schematu: Ludzie, Procesy, Narzędzia — dokładnie w tej kolejności.

LUDZIE

Mówiąc o pracy u podstaw, mam na myśli docieranie z wiedzą do każdego pracownika, który posiada dostęp do zasobów firmy. Jak pokazują ataki, to od siły "najsłabszego ogniwa" zależy siła całej organizacji. Dla przykładu wymienię tutaj dwa:

- **Atak na pracownika zespołu DevOps w LastPass, polegający na zainfekowaniu komputera w celu zdobycia haseł.**
- **Nakierowany phishing na bazie danych z LinkedIn na pracowników Sony Pictures, którego celem było uzyskanie dostępu do komputerów**.

Czy narzędzia mogą zabezpieczyć przed takimi atakami? Nie. Dobrze ułożone procesy mogą pomóc je szybko wykrywać, ale podstawowym i pierwszym krokiem w trosce o bezpieczeństwo powinna być edukacja. Jeżeli dokładamy zespołowi nową odpowiedzialność, musimy się upewnić, że jego członkowie wiedzą, jak działa określony obszar. Rozumieją, dlaczego jest ważny oraz wiedzą, w jaki sposób rozwiązywać pojawiające się problemy.

Jeżeli dajemy dostępy do ważnych dla naszej firmy zasobów, po-winniśmy być pewni, że nie tylko zachowa on/a należytą ostrożność, ale także będzie umiał/a odpowiednio postępować w sytuacjach budzących wątpliwości. Warto stworzyć w organizacji przestrzeń do wymiany takiej wiedzy.

Niech to nie będą tylko nudne szkolenia do zaliczenia czy skomplikowana procedura do przeczytania.

Następnie powinniśmy dać zespołowi czas na ułożenie nowego rytmu pracy i eksperymentowanie. Dzięki temu osoby zaangażowane wyrobią sobie opinię na temat adresowanego obszaru i same zauważą trudności, z którymi jest on związany.

PROCESY

Czy jest idealny moment na wprowadzenie procesów? Tak. To czas, gdy pracownicy są już świadomi istotności danego obszaru bezpieczeństwa oraz wyrobili własne nawyki zajmowania się nim.

Ustrukturyzowanie procesu to ułożenie planu działania w określonych sytuacjach. Po fazie eksperymentowania znamy już przebieg pracy, więc układamy procedury tak, by umożliwić pracownikom szybkie i automatyczne działanie. Co więcej, ułatwiamy również zapoznanie się z zasadami nowym osobom lub innym zespołom, gdy będziemy chcieli rozszerzyć opracowane praktyki na całą organizację.

Praktyka pokazuje, że taki proces nie jest od razu idealny. Wymaga dostosowywania i dopracowywania. Tak wprowadzany jednak wychodzi na przeciw potrzebom i trudnościom, nie stając się kolejnym uciążliwym wymaganiem oderwanym od realiów codziennej pracy, o którym nikt nie pamięta. Zależy nam właśnie na bezpieczeństwie realnym, dającym ochronę przed zagrożeniami, nie zaś tylko formalnym potwierdzeniu wysiłków podejmowanych w tej dziedzinie w postaci zestawu raportów wymaganych przez regulacje.

W miarę sukcesywnego stosowania dochodzimy do ostatniego pytania: co zajmuje najwięcej czasu?

NARZĘDZIA

To właśnie idealny moment na ostatni krok: wprowadzenie narzędzi. Znamy już dobrze wyznaczony obszar. Wiemy, jak o niego dbać i określiliśmy oczekiwany poziom bezpieczeństwa (np. liczba błędów danego typu). Teraz właśnie warto wdrażać narzędzia, których celem jest wsparcie naszej pracy albo nawet jej zautomatyzowanie. Ponadto jest to idealny moment na ustalenie i egzekwowanie (za pomocą odpowiednich narzędzi) oczekiwanego progu bezpieczeństwa.

W ten sposób narzędzie pomaga w pracy i, co najważniejsze, odpowiada na rzeczywiste problemy/potrzeby interesariuszy tego tematu.

DLACZEGO TO WAŻNE?

Model Ludzie - Procesy - Narzędzia stawia osoby odpowiedzialne za dany obszar w centrum zainteresowania. Dzięki temu docelowy proces jest adekwatny, a ludzie wykonują swoją pracę efektywnie. Czując istotność bezpieczeństwa danego obszaru i mając możliwość jego poznania, biorą za niego pełną odpowiedzialność.

Działa to również motywująco na samych pracowników. Nikt nie lubi, gdy dokłada mu się obowiązki bez zapytania go o zdanie, bez pokazania możliwości rozwoju. Ponadto z mniejszym zaangażowaniem wykonujemy zadania, gdy nie widzimy w nich sensu. Za to każdy lubi otrzymywać pomoc. Czy to od człowieka, czy to od narzędzi.

Czy przedstawiony model ma wady?

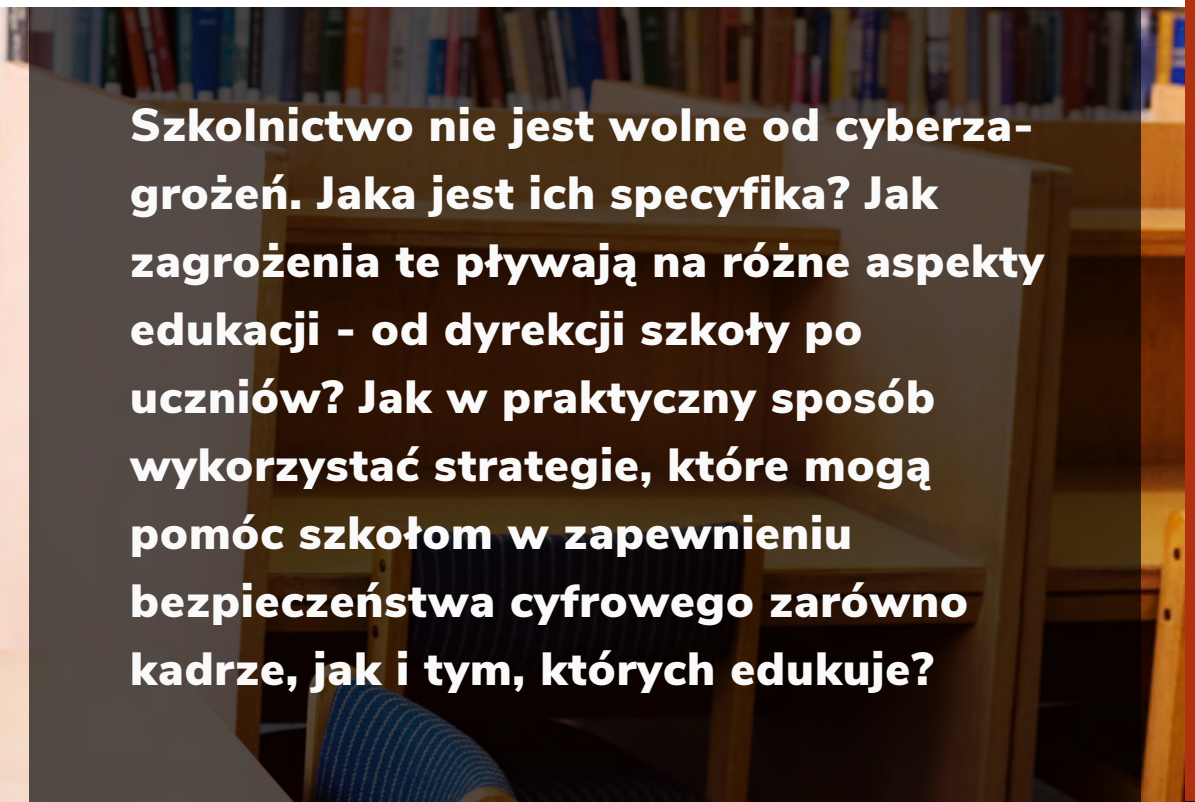
Tak. Wdrożenie praktyki i osiągnięcie zadowalającego stanu zadbania o określony obszar bezpieczeństwa w ten sposób trwa dłużej niż w przypadku wyjścia od narzędzi bądź procedur przygotowanych dla całej firmy przez działy prawny i bezpieczeństwa.

Czy coś rekompensuje tę wadę?

Tak. Jest to podejście długodystansowe. Tak wdrożona praktyka przynosi firmie realne korzyści (nie tylko w obszarze bezpieczeństwa, gdyż z powodzeniem możemy ją stosować w innych dziedzinach), zostaje w ludziach i łatwiej utrzymać ją w organizacji.

CYBERZAGROŻENIA W SZKOLNICTWIE

Artur Markiewicz
netszczon.pl



Szkolnictwo nie jest wolne od cyberzagrożeń. Jaka jest ich specyfika? Jak zagrożenia te pływają na różne aspekty edukacji - od dyrekcji szkoły po uczniów? Jak w praktyczny sposób wykorzystać strategie, które mogą pomóc szkołom w zapewnieniu bezpieczeństwa cyfrowego zarówno kadrze, jak i tym, których edukuje?

CZYM RÓŻNI SIĘ SPECYFIKA CYBERZAGROŻEŃ W SZKOLNICTWIE?

Prawnicy mówią - to zależy, a ludzie od bezpieczeństwa cyfrowego, że każdy ma swoją specyfikę. Ta specyfika wynika z wielu czynników. Kilka z nich to: branża, ilość i rodzaj użytkowników, obowiązujące regulacje, mnogość systemów, urządzeń.

W przypadku szkolnictwa dochodzi mocny nacisk na własność sprzętu, którym posługuje się najliczniejsze grono użytkowników. Często nauczyciel jest właścicielem sprzętu, a w kontekście bezpieczeństwa to wiele zmienia. O ile szkoła może wymusić techniczne zabezpieczenia na swoich komputerach, o tyle na prywatnym komputerze już tego zrobić nie może.

Bardzo często to wynika z niedofinansowania i przyzwyczajeń. Nauczyciel musi, albo chce korzystać ze swoich urządzeń.

CYBERBEZPIECZEŃSTWO: POŁĄCZENIE TECHNOLOGII, PROCESÓW I LUDZI?

Dochodzimy do meritum założeń cyberbezpieczeństwa. To połączenie technologii, procesów, procedur, regulacji, ludzi i ich wiedzy, nawyków, zaangażowania.

Dołóżmy do tego potrzebę edukacji najmłodszych, dostarczenia im narzędzi pracy, dynamikę rozwoju technologii, wymogi programowe, ambicje dzieci, trendy, mody, niezrozumienie przez dorosłych ich potrzeby zaimponowania wśród rówieśników. Mamy tu oblicze finalnego odbiorcy produktów szkolnictwa.

Zbierając to w całość, szkoła jako organizacja musi spełniać wiele wymogów, ma deficyt środków, brakuje zaopiekowania się infrastrukturą, mnogość systemów, braków nie pomaga w tym wszystkim.

- Czy to wszystko decyduje o pozycji startowej skazanej na porażkę?
- Czy skazuje nas to na klęskę przy każdym zagrożeniu?
- Czy wychowankowie szkoły wyjdą z niej z deficytem wiedzy o współczesnej technologii?

NIE!

Ta sytuacja jest rozpoznana i pozwala znajdować rozwiązania. Jesteśmy w bardzo komfortowej sytuacji, gdyż łatwo możemy ułożyć drogę w kierunku bezpieczeństwa.

Pozwól poprowadzić się po tej drodze, a zobaczysz jak łatwo można zaadresować przeciwności i jednocześnie wzbogadzić bagaż doświadczeń naszych podopiecznych.

CO NAS CZEKA NA SZLAKU...

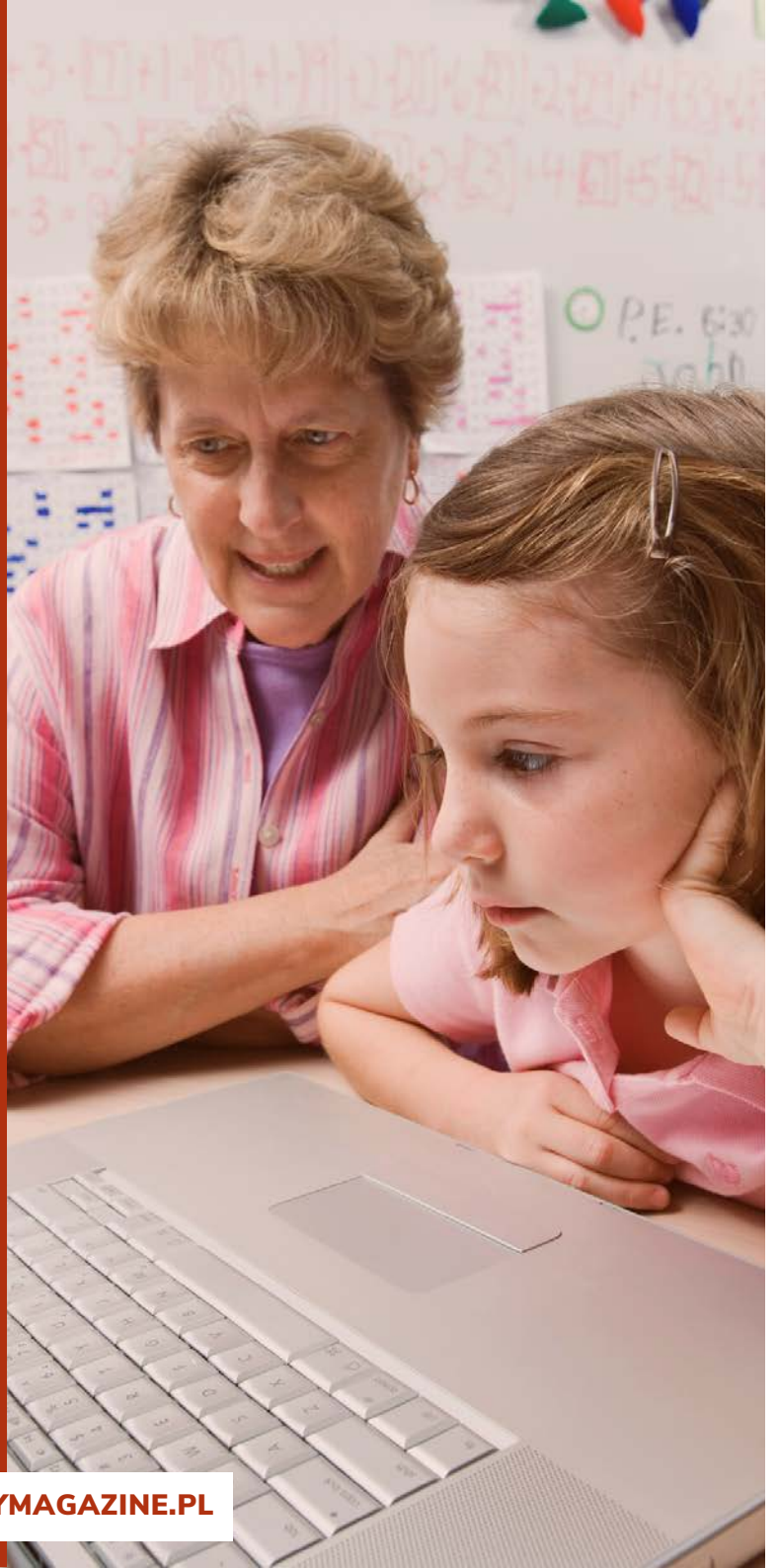
Dyrekcja odpowiada za wszystko. Na jej głowie jest infrastruktura, finansowanie, regulacje, odpowiedzialność. Nie wszystko, czego potrzebują, musi kosztować krocie.

Podstawowe rozwiązania najczęściej już są. Nowe mogą wymagać nakładów finansowych. Tu pojawia się szansa wynikająca z otoczenia. Dobrze dobrane rozwiązania mogą kosztować grosze, o ile zatroszczył się o to ktoś, kto swoją wiedzą i doświadczeniem pozwoli dobrać je, skonfigurować i zaopiekować się nimi.

Innymi słowy, postawmy na wynagrodzenie ludzi, zapytajmy środowisko, bo może w okolicy jest ktoś, kto wesprze placówkę we właściwych wyborach. Regulacje takie jak RODO są na tyle dojrzałe, że wiemy, jak optymalnie się nimi posługiwać.

NAUCZYCIELE JAKO WZORCE W CYBERBEZPIECZEŃSTWIE

Kadra nauczycielska odpowiada za swoich podopiecznych. Jeden z obszarów to bycie wzorem, autorytetem, partnerem dla dzieci i młodzieży. Dzieciaki nie oczekują, że nauczyciel będzie wiedział wszystko, wystarczy im czasami pokazanie drogi. Coś, co nauczyciele mogą zrobić, to być spój-



nym z fundamentami zabezpieczeń dóbr w sieci.

Jednym z nich jest posiadanie różnych haseł do różnych miejsc, wspieranie logowania drugim składnikiem logowania. Zadbanie o pracę na zaktualizowanym sprzęcie, posiadanie (sprawdzonych) kopii zapasowych. Nawyki ograniczonego zaufania, weryfikacji informacji to podstawa skutecznego bycia autorytetem. Można nauczyć tego dzieciaki.

Co mamy na przeciwnym froncie? Trywialny sposób na wyciek danych, zaszyfrowanie i żądanie okupu. Braki w ciągłości pracy, wstyd, straty wizerunkowe. Uczniowie na naszym szlaku, stosując się do wymienionych fundamentów, wiedząc jak i dlaczego, stają się odporni na wiele oszustw skierowanych na dobra materialne.

Ograniczone zaufanie i poczucie własnej wartości uchronią przed zagrożeniami związanymi z sexpredatorami (szukają zdjęć, filmów, najbardziej zależy im na zrobionych materiałach na życzenie od znanej ofiary). Zatroskanie się o psychikę dzieci, zbudowanie relacji przyjacielskiej i poczucia zaufania minimalizuje konsekwencje hejtu, a nawet zmniejszy liczbę agresorów.

W tym punkcie naszej wycieczki, widzisz pewnie, że technologia nie jest głównym punktem ograniczania zagrożeń w sieci.

Jest niezbędna, ale gdyby była wystarczająca, to kwestią pieniędzy by było zmniejszenie liczby skutecznych ataków przestępców. Tak się nie dzieje.

Wielkie organizacje dysponujące ogromnym zapleczem finansowym mają wycieki danych. To nawyki pracowników, sposoby reagowania na zagrożenia są kluczem do podnoszenia kosztów przestępcom.

PRZESTĘPCY MAJĄ DWIE DROGI OSIĄGANIA SWOICH CELÓW

Ataki "hakerskie" to wykorzystanie dziur w oprogramowaniu, konfiguracjach, luk w systemach, zgadywanie haseł. Ofiara dokładnie w momencie ataku nie jest potrzebna przestępcy. Jego ofiara wcześniej zostawiła środowisko z jakimiś zabezpieczeniami, które przestępca będzie próbował przełamać. Czy mu się to uda? To zależy od jego motywacji i zależności potencjalnych korzyści a środków na zdobycie celu.

Najczęściej skonfigurowane środowisko według dobrych praktyk, posiadające aktualizacje jest wystarczające. Przestępca pójdzie tam, gdzie mu łatwiej. Aby tak było, dyrekcja może mieć dobrego duszka znającego się na informatyce, który pozwoli tak przygotować środowisko.

DRUGA DROGA PRZESTĘPCY TO OSZUSTWA

Tutaj ofiara jest niezbędna, żeby wykonać działanie niezbędne przestępcy. Wirusy same się nie instalują, robi to człowiek ciekawy, co to za dokument w mailu. Pieniądze same nie uciekają z konta, ich właściciel sam je wysyła do przestępcy. Najczęściej nie czyta pytania banku, czy na pewno chce wysłać 1500 zł na konto 0009.

SECURITYMAGAZINE.PL

OCHRONA IOT, POCZTY I ALERTY O CYBER-ZAGROŻENIACH

Redakcja
SECURITY MAGAZINE

Na całym świecie przybywa startupów specjalizujących się w cyberbezpieczeństwie. W tym tekście wskażemy te, które zapewniają ochronę poczty w chmurze, powiadamiają nas o cyberzagrożeniach, a także wykrywają naruszenia związane z IoT czy infrastrukturą krytyczną.

BEZPIECZNA OCHRONA POCZTY E-MAIL W CHMURZE

Abnormal Security to startup z Kalifornii, który koncentruje się głównie na zapewnieniu bezpieczeństwa poczty e-mail, m.in. za sprawą automatyzacji. To rozwiązanie chmurowe.

Głównym celem organizacji jest zapobieganie atakom za pośrednictwem wiadomości e-mail i podobnym zagrożeniom. Startup chwali się, że dzięki zastosowaniu zaawansowanych mechanizmów automatyzacji, jego operacje związane z bezpieczeństwem są wydajne.

Specjalizacją Abnormal Cybersecurity jest również ochrona poczty przychodzącej. Rozwiązanie startupu skutecznie blokuje ukierunkowane ataki, takie jak próby wyłudzenia danych uwierzytelniających, włamania do firmowych kont e-mail czy oszustwa w łańcuchu dostaw. Platforma firmy koncentruje się również na zapobieganiu przejmowaniu kont e-mail oraz atakom przy użyciu aplikacji innych firm. Ponadto cały proces cyberbezpieczeństwa jest zautomatyzowany, a użytkownicy otrzymują alerty dotyczące zagrożeń.

Startup ponadto wykorzystuje architekturę natywną w chmurze opartą na interfejsie API. Dzięki temu instalacja systemu jest szybka i nie wymaga skomplikowanej konfiguracji czy dostosowywania. Abnormal Cybersecurity zbiera unikalne zestawy danych z wiadomości e-mail, usług Active Directory, aplikacji do współpracy i wielu innych, co przyczynia się do skutecznego zabezpieczenia.

Firma korzysta też ze sztucznej inteligencji w celu wykrywania anomalii behawioralnych. Tworzy ona modele behawioralne dla użytkowników i organizacji, co pozwala na skuteczną identyfikację znanych i nowo pojawiających się ataków.

Abnormal Cybersecurity oferuje również zintegrowaną architekturę do ochrony wielokanałowej. Oprócz wewnętrznej poczty e-mail, platforma ta chroni także konta e-mail oraz infrastrukturę poczty e-mail. Co więcej, można ją rozszerzyć na inne kanały komunikacji, takie jak Slack, Microsoft Teams czy Zoom, co zapewnia jednolite zabezpieczenie w różnych środowiskach.

INFORMOWANIE O CYBERZAGROŻENIACH

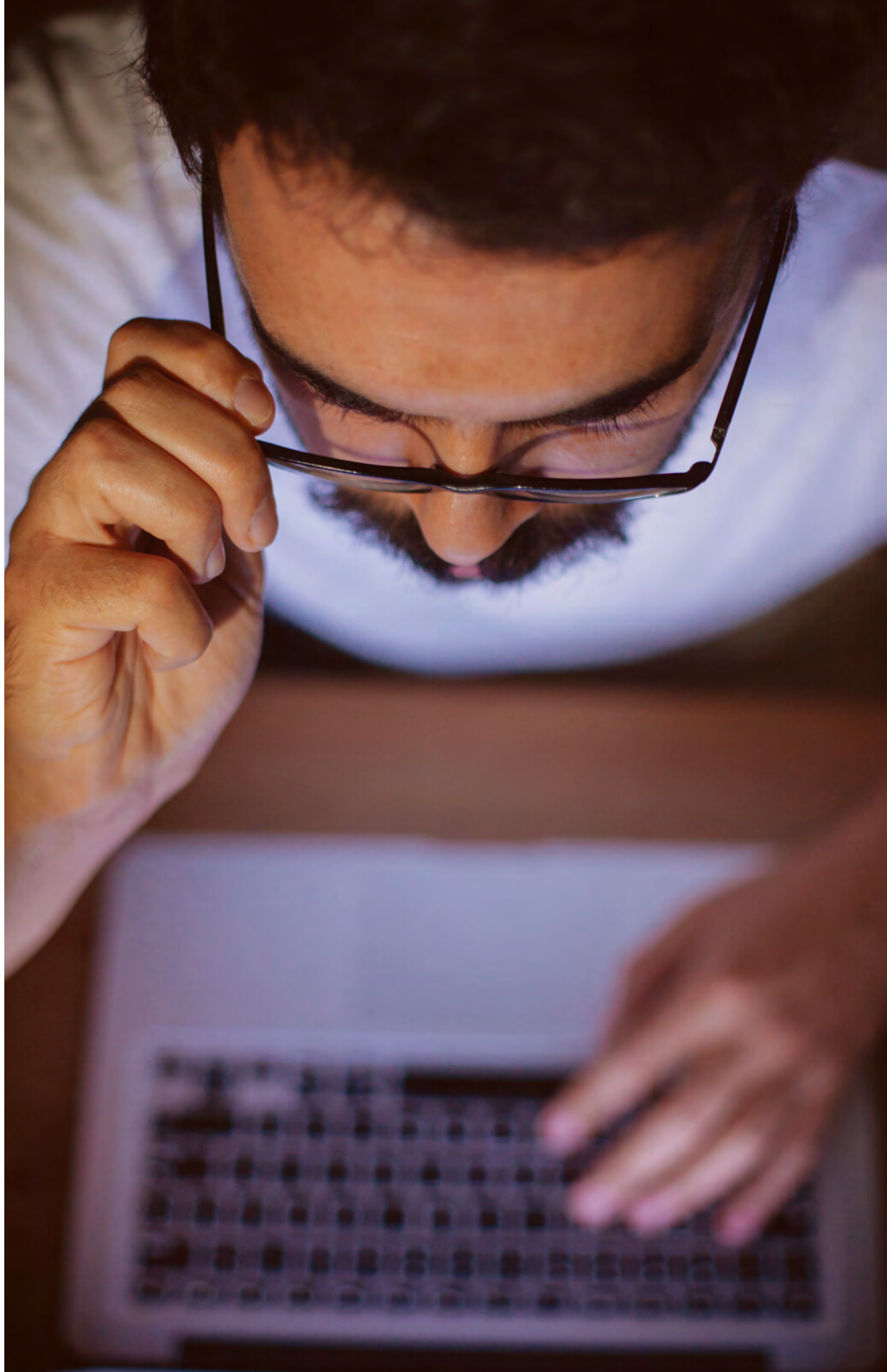
EclecticIQ to niderlandzki (holenderski) startup zajmujący się dostarczaniem informacji o cyberza-

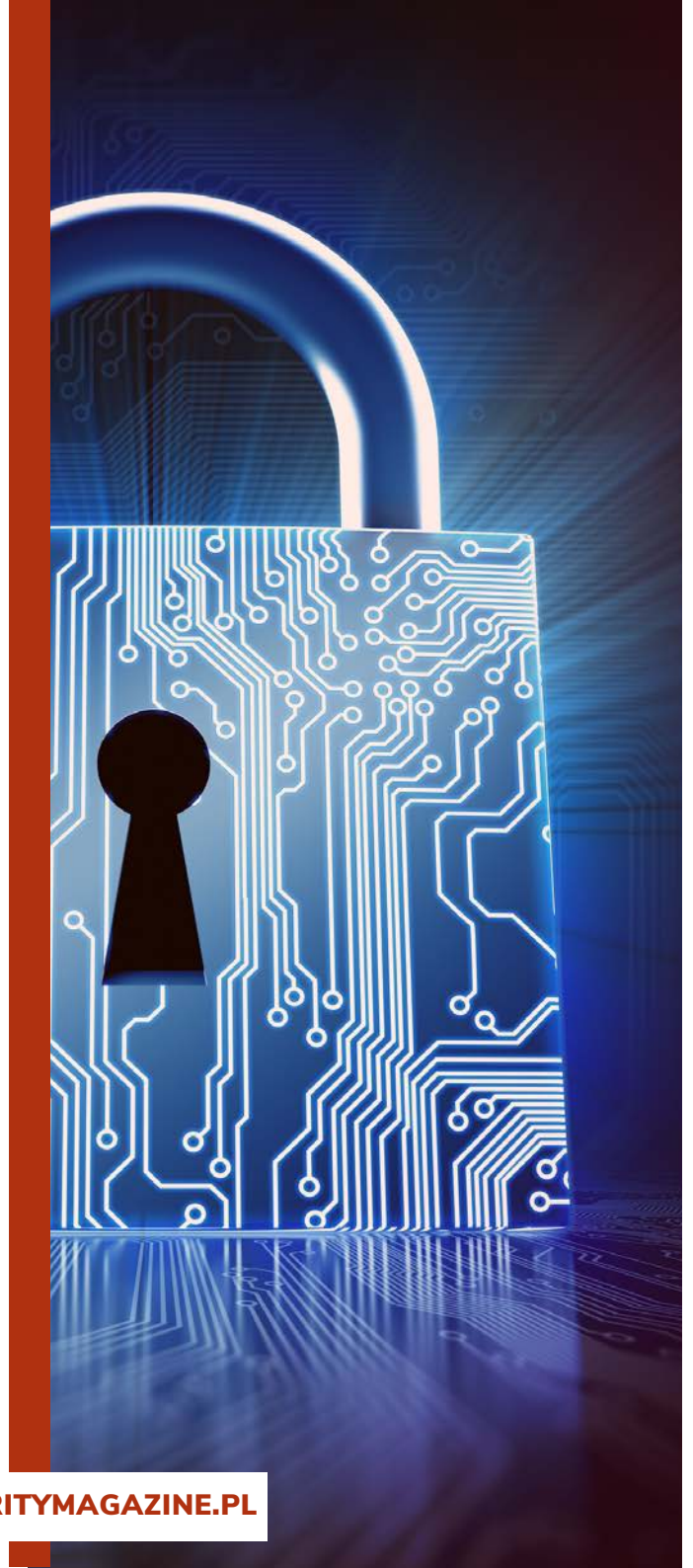
grożeniach. Oferuje oprogramowanie, które zbiera odpowiednie dane, integruje je wewnątrz przedsiębiorstwa i dostarcza je, zapewniając także funkcje raportowania. Dzięki temu istnieje możliwość bycia na bieżąco ze wszelkimi cyberzagrożeniami.

Startup chwali się, że dzięki jego rozwiązaniu poprawiona zostanie wydajność zespołów ds. cyberzagrożeń, łącząc przetwarzanie maszynowe i dystrybucję danych dotyczących naruszeń z analizą i współpracą opartą na ludzkim czynniku. To wszystko przy zachowaniu kontroli analityków, swobody działania i elastyczności.

EclecticIQ twierdzi też, że dzięki swojej patformie istnieje możliwość włączenia się do społeczności współpracujących stron trzecich, takich jak ISAC, agencje lub firmy partnerskie. Jednocześnie kontrolując, jakie poufne informacje udostępniamy. Istnieje także możliwość zbudowania własnej sieci współpracy, korzystając z architektury typu hub-and-spoke, mesh lub połączonej, a jednocześnie dbając o pełną prywatność i zapewniając kontrolę dostępu opartą na rolach.

Platforma startupu ma też zapewinć skalowalność, podobną do chmury i wybór spośród różnych opcji architektur wdrożeniowych, takich jak pojedyncze lub rozproszone wdrożenia, środowiska.





Ekosystem EclecticIQ TIP for CTI ma dostarczać firmom zaawansowane narzędzia zorientowane na analityków, umożliwiające przekroczenie ograniczeń narzędzi open source lub własnoręcznie opracowanych. Dostarcza on także podstawowe wskazówki, umożliwiające wdrożenie najnowocześniejszych wewnętrznych praktyk dotyczących informacji o cyberzagrożeniach.

OCHRONA IOT I KRYTYCZNEJ INFRASTRUKTURY

Nozomi Networks to kolejny kalifornijski startup. Ten jednak specjalizuje się w cyberbezpieczeństwie infrastruktury IoT, operacyjnej i krytycznej. Dzięki swojemu zestawowi narzędzi, organizacja umożliwia minimalizowanie ryzyka i maksymalizowanie odporności przez zwiększenie widoczności sieci i punktów końcowych, zaawansowane wykrywanie zagrożeń oraz analizę danych opartą na sztucznej inteligencji.

Startup oferuje również monitorowanie każdego urządzenia IoT, OT oraz ICS w sieci. Dzięki temu użytkownicy mogą obserwować role, protokoły, przepływy danych i inne istotne informacje. Nozomi Networks umożliwia także zarządzanie ryzykiem operacyjnym. Startup chwali się, że dzięki skupieniu się na cyberzagrożeniach infrastruktury OT i IoT, firma może zredukować liczbę generowanych alertów bezpieczeństwa o 70%. To pozwala na skoncentrowanie się na najważniejszych zagrożeniach i szybką reakcję.

Nozomi Networks udostępnia również informacje o zagrożeniach, do-

tyczące pojawiających się ataków typu zero-day, złośliwego oprogramowania, botnetów i luk w zabezpieczeniach. Dzięki temu użytkownicy mogą działać proaktywnie, uwzględniając wytyczne dotyczące zgodności zabezpieczeń OT i IoT.

Ważnym aspektem jest również unikanie zakłóceń w działalności biznesowej. Nozomi Networks dostarcza natychmiastowe informacje o anomaliiach procesów OT i IoT oraz ryzyku i zagrożeniach. Dzięki temu użytkownicy są w stanie szybko reagować i minimalizować negatywne skutki dla operacji.

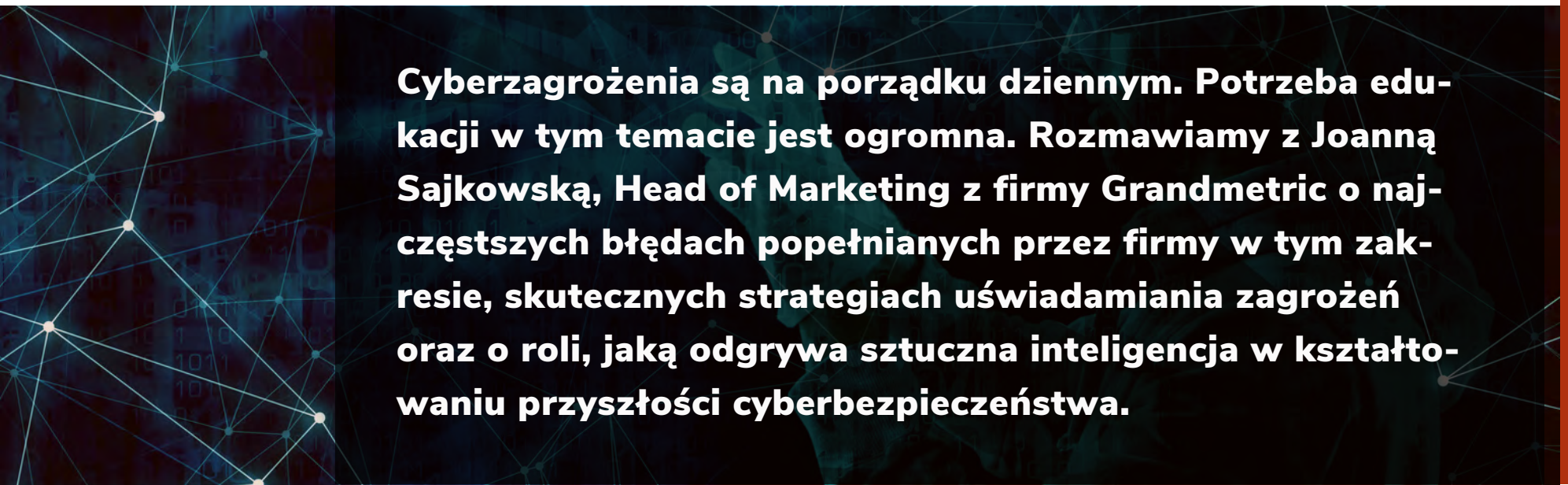
Startup wykorzystuje sztuczną inteligencję do generowania przydatnych wniosków. Eliminuje nadmiar alertów i wzmocnia zabezpieczenia infrastruktury OT i IoT, opierając się na wpływowych wnioskach, analizie przyczyn źródłowych i celowanym działaniu naprawczym.

Nozomi Networks twierdzi też, że zapewnia nieograniczoną skalowalność. Dzięki zastosowaniu usług typu SaaS (Software-as-a-Service) w dziedzinie cyberbezpieczeństwa OT i IoT, startup umożliwia skonsolidowane gromadzenie danych, analizę i zarządzanie nimi na poziomie globalnym.

To tylko niektóre ze startupów mogących pomóc firmom w poprawieniu zabezpieczeń i ogólnie cyberbezpieczeństwa.

CYBERBEZPIECZEŃSTWO TO MARATON, NIE SPRINT. ROZMOWA Z JOANNĄ SAJKOWSKĄ

Joanna Sajkowska
Grandmetric



Cyberzagrożenia są na porządku dziennym. Potrzeba edukacji w tym temacie jest ogromna. Rozmawiamy z Joanną Sajkowską, Head of Marketing z firmy Grandmetric o najczęstszych błędach popełnianych przez firmy w tym zakresie, skutecznych strategiach uświadamiania zagrożeń oraz o roli, jaką odgrywa sztuczna inteligencja w kształtowaniu przyszłości cyberbezpieczeństwa.

Czy, Pani zdaniem, środowisko biznesu jest wystarczająco świadome zagrożeń związanych z cyberbezpieczeństwem? Jakie są najczęstsze błędy, które popełniają firmy, organizacje, zakłady pracy, w zakresie własnego bezpieczeństwa?

Joanna Sajkowska: Świadomości o zagrożeniach i cyberbezpieczeństwie nigdy za wiele. Ostatnie lata pokazują, że ataków na infrastrukturę państwową oraz na biznes jest coraz więcej, a zajmują się nimi nierzadko zorganizowane grupy. W Dark Webie można łatwo zamówić atak na dowolną organizację (z gwarancją powodzenia lub zwrotem pieniędzy).

Myślę, że świadomość zagrożeń rośnie, ale jest niewystarczająca. Tegoroczny raport Cisco Cybersecurity Readiness Index podaje, że zaledwie 7% polskich firm charakteryzuje tzw. dojrzałość w dziedzinie cyberbezpieczeństwa. To bardzo mało.

Najczęściej popełniane błędy wynikają przede wszystkim z podchodzenia do bezpieczeństwa jak do sprintu, tymczasem to pełnowartościowy maraton. Wymaga powtarzalnych treningów w postaci regularnych aktualizacji, wymiany przestarzałego sprzętu i poddawaniu się przynajmniej raz w roku stress testom, takim jak audyty bezpieczeństwa.

Jak najskuteczniej można dziś ostrzegać i uświadamiać ludzi ze świata biznesu przed zagrożeniami? Którymi kanałami?

J.S.: Powiedziałabym, że wszystkie chwyty dozwolone. Cyber-

bezpieczeństwo od lat zajmuje ważne miejsce na konferencjach technologicznych, czas, żeby wyszło z cienia i trafiło pod strzechy. A to się stanie, kiedy odpowiednio dużo ekspertów zacznie korzystać choćby z kanałów social media czy wykorzystywać video.

Najskuteczniej przekonują przykłady, liczby i... humor. Z tym ostatnim doskonale radzą sobie z tym HRejterzy. Co do pierwszego - sami często powołujemy się na pentesty, podczas których dostaliśmy się do pasków płacowych zarządu przez niezabezpieczony port w drukarce. Pokazanie pasków podczas omawiania raportu z testów zrobiło na zarządzie naszego klienta piorunujące wrażenie.

Tak, przyznać trzeba, że działania CodeTwo, to świetnie przygotowana strategia marketingowa. Więc w jaki sposób trendy w marketingu mogą pomóc w promocji wiedzy na temat cyberbezpieczeństwa?

J.S.: Marketing daje doskonałe narzędzia do krzewienia wiedzy i świadomości dotyczącej cyberbezpieczeństwa. Strategie zależą od tego, do kogo chcemy dotrzeć: czy to inżynierowie lub managerowie, którzy na co dzień pełnią role związane z bezpieczeństwem, czy zaledwie go dotykają.

Myślę, że częstym błędem jest założenie, że nasi odbiorcy już wszystko wiedzą o ochronie organizacji - sposobach, politykach, narzędziach. To wiedza, którą należy aktualizować. Do tego dochodzi nierzadko do sytuacji, w których inżynierowie dostrzegają potrzebę zmian, ale są blokowani przez managerów, którzy nie planują wydatków w zakresie cybersecurity. Wtedy powinniśmy skupić się na tym, żeby użyć argumentów ekonomicznych i strategicznych. Słowem - pomóc osobom technicznym przekonać zarządy, że dbanie o cyberbezpieczeństwo to nie luksus, ale konieczność.

A jak Pani wykorzystuje marketing do działań na rzecz cyberbezpieczeństwa? Również tych promujących rozwiązania Grandmetric?

J.S.: W Grandmetric od początku skupiamy się na edukowaniu rynku o projektowaniu, zabezpieczaniu, także zarządzaniu nowoczesnymi sieciami LAN oraz WAN i całą infrastrukturą IT. Na naszej stronie internetowej można znaleźć kursy czy przewodniki stworzone dla inżynierów i managerów. Ostatnio wydaliśmy np. **"Jak chronić biznes przed cyfrowymi zagrożeniami?"** czy **"Next-Generation Firewall. Porównanie produktów dla sektora MŚP".**

Aktywnie wykorzystujemy LinkedIn i Facebook, rozwijamy również kanał Watch Grandmetric na YouTube oraz regularnie wydajemy newsletter. Dużo eksperymentujemy. Naszym ostatnim eksperymentem jest Flash Technologiczny, w którym w krótki, (mam nadzieję) zabawny sposób pokazujemy, co się dzieje w świecie IT i że ataki na sprzęt nawet największych producentów to codzienność.

W tych działaniach, na jakie wyzwania Pani napotkała?

J.S.: Myślę, że największym wyzwaniem jest przekonanie, że nasi odbiorcy już wszystko wiedzą. Że nie warto przypominać o podstawach, bo wtedy nie będziemy wiarygodni jako poważni inżynierowie. Druga strona tego medalu jest taka, że nieraz świetnym specjalistom, z którymi pracuję, wydaje się, że nie mają nic wartościowego do powiedzenia. Bo już przecież ktoś inny to zrobił. W świecie social mediów, w którym pojedyncza wiadomość ma czas życia kilku minut, powtarzanie jest szczególnie potrzebne. Po pierwsze dlatego, że nasze treści docierają zawsze do bardzo ograniczonego grona odbiorców. Po drugie dlatego, że uważność ludzi spada. Jeśli chcemy przykuć ich uwagę, musimy konsekwentnie i regularnie mówić na ważny dla nich temat.

Zmieńmy nieco temat. Jaki wpływ, Pani zdaniem, ma stale rosnące zastosowanie AI na cyberbezpieczeństwo? Czy pomaga w zwalczaniu cyberprzestępczości?

J.S.: Wpływ jest znaczny na obie strony. Po pierwsze, początkowe wersje aplikacji AI, takich jak Chat GPT umożliwiały tworzenie malware bez wysiłku. W kolejnych wersjach komendy służące generowaniu złośliwego kodu zostały ograniczone, jednak co sprawniejsi użytkownicy nadal potrafili je obejść.

Także próg wejścia w tworzenie malware zmalał niesamowicie. To daje ogromne pole manewru do poszukiwania nowych wektorów ataku na systemy, użytkowników i dane. Drastycznie zmniejsza też koszt ich pozyskania.

Jednocześnie zaawansowane algorytmy uczenia maszynowego czy sztucznej inteligencji są wykorzystywane przez mechanizmy Threat Intelligence. Tak jest chociażby w Cisco Umbrella, które na podstawie badanych stron potrafi ocenić, czy zawartość kolejnych jest niebezpieczna. Rozwija się więc możliwość skutecznego rozpoznawania zagrożeń na podstawie pojedynczych przesłanek lub ich kombinacji, które można wykryć za pomocą zaawansowanych algorytmów.

Jak ciągły rozwój technologii wpływa z kolei na Pani pracę w zakresie marketingu w branży cybersecurity?

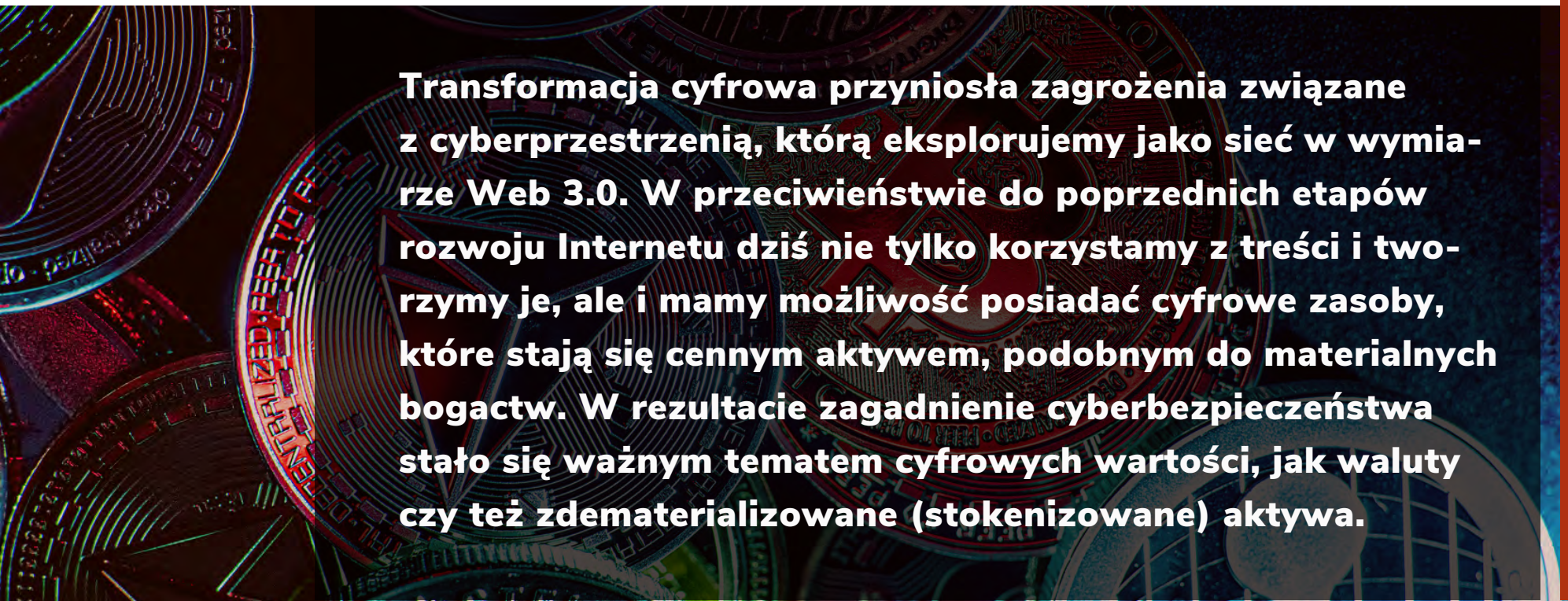
J.S.: Dla mnie to wspaniała możliwość obserwowania, jak zmienia się świat, i brania w tym udziału. Jestem z ostatniego pokolenia, które wychowało się bez telefonu komórkowego. Na studiach (elektronika i telekomunikacja) śledziłam postęp związany z wejściem Wi-Fi i budową sieci 3G. Dzisiaj jesteśmy o lata świetlne dalej w rozwoju.

Korzystam z dobrodziejstw narzędzi opartych o AI (Chat GPT, translatory, narzędzia do generowania transkrypcji, grafik czy napisów), jednak staram się przy tym bardzo dbać o swoje dane. Korzystam z managera haseł, raz na kwartał przeglądam aplikacje, do których byłam zalogowana i usuwam dostęp do tych, z których nie korzystam. Dbam też o regularne aktualizacje systemów, na których pracuję. Wierzę, że dzięki technologii możemy pracować mądrzej i bezpieczniej, nawet jeśli bezpieczeństwu w cyberprzestrzeni musimy poświęcać więcej czasu niż 5 czy 10 lat temu.

Dziękuję za inspirującą rozmowę.

WEB 3.0 ZMIENIA POSTRZEGANIE BEZPIECZEŃSTWA CYFROWYCH WARTOŚCI

Kamil Gancarz
BITFOLD AG



Transformacja cyfrowa przyniosła zagrożenia związane z cyberprzestrzenią, którą eksplorujemy jako sieć w wymiarze Web 3.0. W przeciwieństwie do poprzednich etapów rozwoju Internetu dziś nie tylko korzystamy z treści i tworzymy je, ale i mamy możliwość posiadać cyfrowe zasoby, które stają się cennym aktywem, podobnym do materialnych bogactw. W rezultacie zagadnienie cyberbezpieczeństwa stało się ważnym tematem cyfrowych wartości, jak waluty czy też zdematerializowane (stokenizowane) aktywa.

Metody zabezpieczeń, jak regularna zmiana haseł czy uwierzytelnianie dwuskładnikowe (w postaci SMS-a, aplikacji mobilnej, a ostatnio nawet przy użyciu tokena fizycznego) nie są nowością dla użytkowników internetowych. Warto jednak zastanowić się, jak chronić osoby decydujące się na działania na rynku kryptowalut lub szerzej technologii Blockchain.

W miarę wzrostu zainteresowania i świadomości dotyczącej funkcjonowania walut cyfrowych istotne jest przyjrzenie się temu, jak dba się o bezpieczeństwo cyfrowych portfeli, przechowujących klucze prywatne. Problem bezpieczeństwa dotyczy wszystkich, którzy korzystają z nowoczesnych technologii opartych o Blockchain. Niezależnie od tego, czy jesteśmy zaawansowanymi użytkownikami tej technologii, czy też dopiero zaczynamy zgłębiać jej tajniki, bezpieczeństwo w sieci jest dla nas bardziej kluczowe niż kiedykolwiek wcześniej.

CZĘSTE I SKUTECZNE ATAKI

Historia jednoznacznie pokazuje, że ataki na cyfrowe wartości poruszających się w świecie kryptowalut są nie tylko częste, ale też potężne w skutkach.

Firma analityczna, badająca Blockchain - Chainalysis ogłosiła miniony rok „największym rokiem w historii" pod względem liczby projektów kryptograficznych dotkniętych atakami i kradzieżą. Oficjalnie mówi się, że w 2022 roku osiągnięto rekordową kwotę skradzionych środków wynoszącą 3,8 miliarda dolarów w wyniku włamań na elementy ekosystemu kryptowalut. Obecny rok zapowiada się równie niebezpiecznie dla właścicieli cyfrowych wartości, bowiem jedynie w pierwszych trzech miesiącach 2023 roku miało miejsce aż 40 ataków, które skutkowały kradzieżą łącznie 400 milionów dolarów.

Rozważając historię kradzieży zasobów cyfrowych, warto przytoczyć te największe, które obrazują, na jak dużą skalę działają hakerzy.

Jedno z największych i najbardziej spektakularnych włamań w historii miało miejsce w marcu 2022 roku, kiedy hakerzy dokonali kradzieży Ethereum oraz stablecoina USDC o wartości około 625 milionów dolarów z sieci Ronin, obsługującej popularną platformę gier typu blockchain, Axie Infinity. Mimo że część skradzionych funduszy została odzyskana przez Binance, to nadal pozostaje to największym przekrętem w historii kryptowalut.

Warto też wspomnieć o ataku, który miał miejsce w sierpniu 2021, kiedy samotny haker wykorzystał lukę w zdecentralizowanej platformie finansowej Poly Network, kradnąc ponad 600 milionów dolarów.

Niestety, ataki na kryptowaluty nie ograniczają się tylko do dużych platform. Również portfele kryptowalutowe, takie jak Trust Wallet, wraz z ich użytkownikami, stają się ofiarami przestępstw. Jedną z największych, ostatnich kradzieży na tym portfelu dokonała organizacja przestępcza z siedzibą we Włoszech. Wykorzystała ona socjotechnikę do kradzieży USDC o wartości 4 milionów USD z portfela należącego do Webaverse, firmy z obszaru Web 3.

Jak pokazują powyższe przykłady cyfrowe waluty stanową atrakcyjny cel dla przeprowadzających ataki hackerskie. Nie dziwi więc fakt, że możliwość kradzieży zasobów cyfrowych w postaci kryptowalut, posiadających realną wartość monetarną stanowi poważne zagrożenie dla wszystkich użytkowników działających na rynku kryptowalut, zarówno klienta indywidualnego jak i instytucji czy projektu kryptowalutowego.

Dlatego też jakość i procedury zabezpieczeń metodologii przechowania kluczy prywatnych są najbardziej isotnym aspektem cyberbezpieczeństwa całego sektora.

W POSZUKIWANIU BEZPIECZEŃSTWA

Czy istnieją skuteczne sposoby na zabezpieczenie naszych cyfrowych zasobów przed nieuprawnionym dostępem? Stosowanie dedykowanych portfeli software'owych do przechowywania kluczy prywatnych jest często niewystarczające, co potwierdzają liczne hacki. Co więcej, na ataki są nawet narażenie użytkownicy dedykowanych portfeli sprzętowych typu „cold wallet", chociaż już tutaj ataki muszą być zdecydowanie bardziej wysublimowane.

Bezpieczeństwo kryptowalut czy tokenów opiera się na skutecznym zarządzaniu ryzykiem poprzez odpowiedni system, który chroni nasze aktywa kryptograficzne przed nieautoryzowanym dostępem. To absolutnie kluczowe dla każdego, kto działa w tej branży. Niedostateczne zabezpieczenie kryptowalut może prowadzić do całkowitej utraty środków w wyniku różnych wektorów ataku.

Co do zasady, właściwa implementacja technologii Blockchain gwarantuje ekstremalnie wysoki poziom bezpieczeństwa, jednakże to, co pozostaje najsłabszym ogniwem, jest końcowy użytkownik, a w szczególności jego klucze prywatne i w tym obszarze wciąż istnieje zdecydowanie niedostateczna świadomość skutecznej ochrony i unikania ataków.

Wyniki raportu Bitfold, zatytułowanego "Badanie opinii użytkowników portfeli do przechowywania i transakcji kryptowalutami", rzucają światło na kluczowe czynniki brane pod uwagę przy wyborze portfela kryptowalutowego – bezpieczeństwo i niezawodność. Badanie to, które przeprowadzone m.in. w trakcie Invest Cuffs – prestiżowej konferencji w Krakowie dedykowanej branży inwestycyjnej, ukazuje, że preferencje użytkowników skupiają się przede wszystkim na wyborze portfeli, które gwarantują najwyższy poziom

ochrony przed atakami oraz zapewniają niezawodność i pewność działania. Jak wynika z raportu, około 50% ankietowanych preferuje rozwiązania dedykowane tylko do kryptowalut, podczas gdy druga połowa chciałaby posiadać kompleksowe urządzenia zapewniające bezpieczeństwo w szeroko pojętej cyberprzestrzeni.

CYFROWY PORTFEL SKROJONY NA MIARĘ POTRZEB

Jak przedstawia, wyżej przytoczony, przeprowadzony przez firmę Bitofd raport, wśród użytkowników portfeli do przechowywania i transakcji kryptowalutami, wraz ze wzrostem wielkości cyfrowego majątku, rośnie znaczenie jakości i bezpieczeństwa portfela, w którym go przechowują. Chociaż główne trendy i technologie w cyberbezpieczeństwie często pochodzą zza oceanu, warto przyjrzeć się narzędziom tworzonym w Polsce.

Jak się okazuje, polscy eksperci w dziedzinie technologii Blockchain, cyberbezpieczeństwa oraz elektroniki budują rozwiązanie na rosnące zapotrzebowanie na ochronę zarówno cyfrowego pieniądza, jak innych cennych cyfrowych aktywów. Polacy budują innowacyjny sprzętowy portfel dla kluczy prywatnych oparty na technologii blockchain i innych zastosowaniach asymetrycznej kryptografii.

To urządzenie, nazwane Bitfold, wykorzystuje opatentowaną technologię bezpieczeństwa, znanej jako sprzętowa śluza danych (hardware air-gap), która jest chroniona patentami w UE, USA, Turcji, Szwajcarii, Lichtensteinie oraz prowadzone są postępowania patentowe w 18 innych krajach świata.

Bitfold może służyć do zabezpieczania różnych cyfrowych aktywów, w tym kryptowalut, a także cyfrowej tożsamości, stokenizowanych dóbr takich jak np. nieruchomości oraz szeregu usług finansowych, a także usług bazujących na znanych rozwiązaniach z Web 2.0. Bitfold budowany jest jako pierwszy osobisty, mobilnym cyfrowy sejf, będący kluczem do nowej cyfrowej (rozszerzonej) rzeczywistości.

Bitfold ma stanowić pierwszą na świecie formę interfejsu, która daje możliwość każdemu użytkownikowi prywatnemu lub korporacyjnemu łatwego wysyłania, odbierania, a przede wszystkim bezpiecznego przechowywania cyfrowych aktywów. Najistotniejsze, że nie jest do tego potrzebny ża-

den „pośrednik”, taki jak komputer czy smartfon.

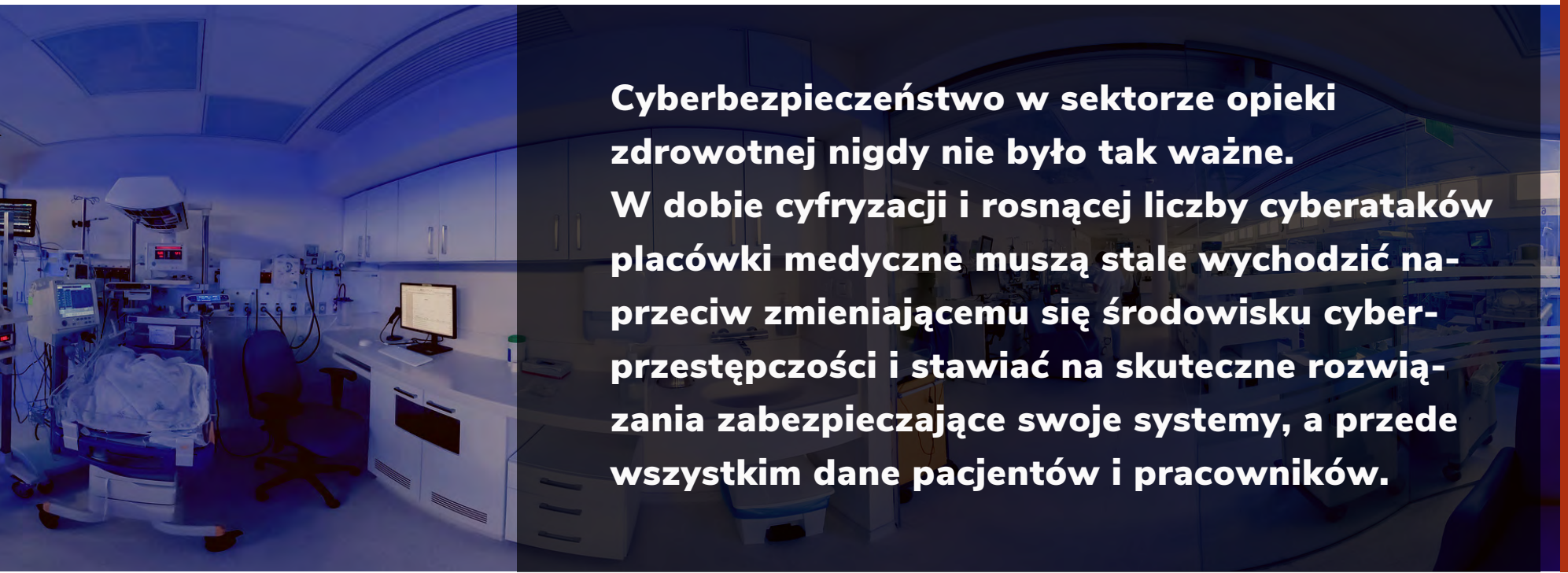
Bitfold będzie mógł doskonale pełnić rolę portfela przeznaczonego do transakcji w całym ekosystemie Web3. Technologia w oparciu, o którą tworzony jest Bitfold może być również wykorzystana w przyszłości do różnych działań mających na celu zapewnienie bezpieczeństwa, takich jak podwójna weryfikacja, podpis elektroniczny (nawet kwalifikowany) czy obsługa bankowości internetowej.

Misją Bitfold jest zapewnienie ludziom większej wolności i prawdy poprzez ułatwienie korzystania z technologii Blockchain i kryptografii, przy zachowaniu najwyższego bezpieczeństwa. Firma tworzy solidne podstawy dla nowej rzeczywistości, tworząc portfel sprzętowy nowej generacji, który uwolni prawdziwy potencjał przestrzeni cyfrowej.

W świetle ostatnich upadków banków i ogromnego systemowego problemu w sektorze finansowym rozwiązania do self-custody (samodzielnego przechowywania) cyfrowych wartości będą odgrywać kluczową rolę w zmieniającym się i ewoluującym systemie finansowym.

INWESTYCJA W CYBERBEZPIECZEŃSTWO PLACÓWKI MEDYCZNEJ

Tomasz Bill
thebill oraz Alfa Lingua



Cyberbezpieczeństwo w sektorze opieki zdrowotnej nigdy nie było tak ważne. W dobie cyfryzacji i rosnącej liczby cyberataków placówki medyczne muszą stale wychodzić naprzeciw zmieniającemu się środowisku cyberprzestępczości i stawiać na skuteczne rozwiązania zabezpieczające swoje systemy, a przede wszystkim dane pacjentów i pracowników.

Cyberbezpieczeństwo w sektorze opieki zdrowotnej jest kluczowe dla ochrony danych pacjentów oraz pracowników, ale również stanowi istotny element w utrzymaniu ciągłości świadczenia usług medycznych. Oprócz środków własnych na działania związane z podnoszeniem poziomu cyberbezpieczeństwa można wykorzystać środki dostępne w ramach dofinansowania z NFZ. Dane pacjentów są cennym celem dla cyberprzestępców, a ich utrata lub naruszenie może prowadzić do poważnych konsekwencji prawnych i finansowych.

Jako niezależny ekspert w dziedzinie języka komunikacji marek oraz budowania wizerunku firm czy organizacji we współpracy z jednym z moich klientów, firmą Nomios, która jest partnerem Programu Współpracy w Cyberbezpieczeństwie (PWCyber), pokażemy na co placówki medyczne powinny zwrócić szczególną uwagę i jaką rolę może odegrać firma doradzająca w zakresie wyboru najlepszych cyberzabezpieczeń.

NAJCZĘSTSZE RODZAJE CYBERATAKÓW SKIEROWANYCH W PLACÓWKI MEDYCZNE

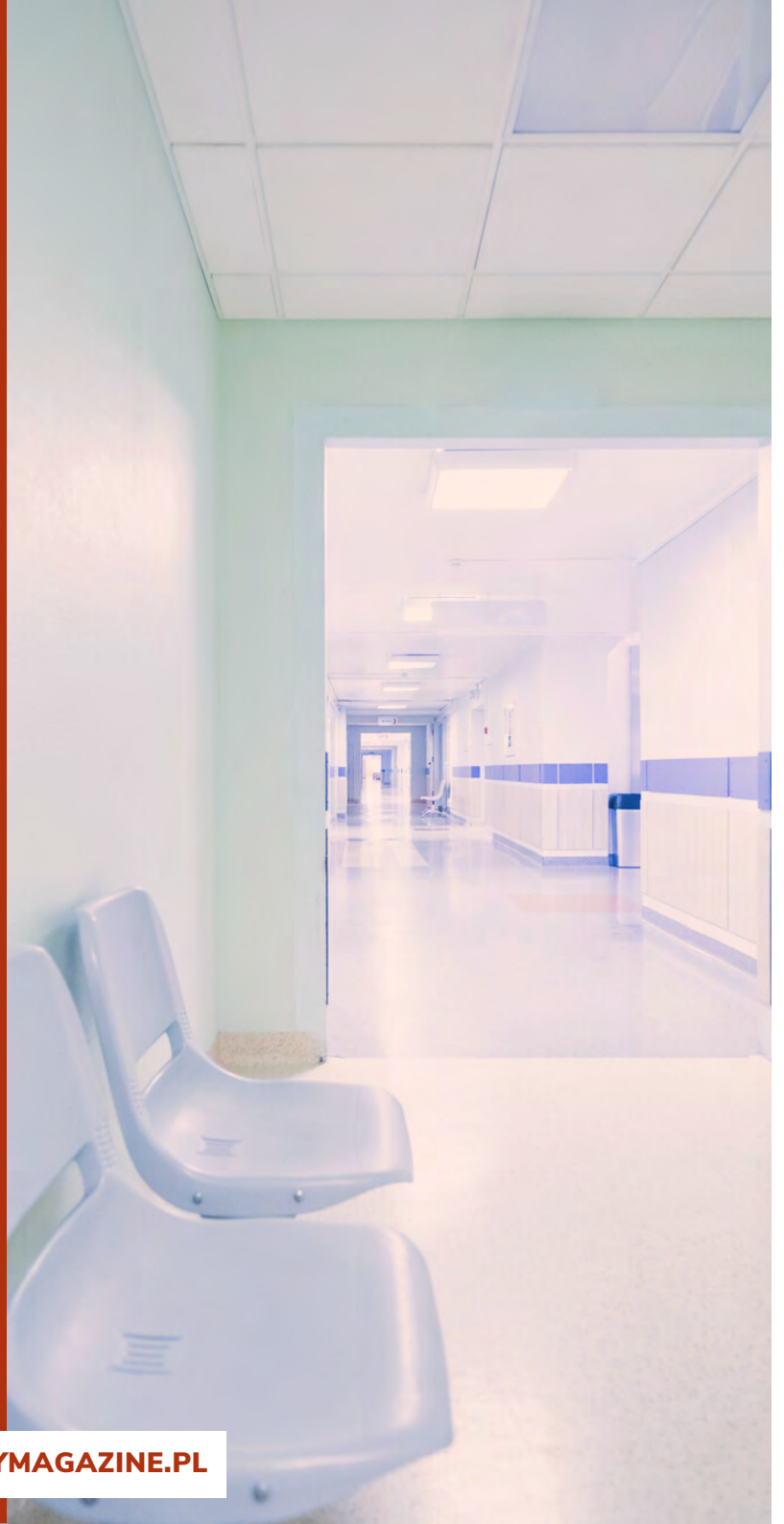
Poniżej przedstawiamy cztery zagrożenia dla infrastruktury informatycznej placówek medycznych, które naszym zdaniem są kluczowe:

Ataki typu ransomware polegają na zaszyfrowaniu danych przez cyberprzestępców, którzy następnie żądają okupu za ich odszyfrowanie.

Tzw. „phishing” polegający na tym, że przestępcy próbują nakłonić użytkowników do podania swoich danych logowania lub innych wrażliwych informacji. Phishing jest krokiem wstępnym ataków ransomware czy wyprowadzenia danych z organizacji – faktycznie chodzi o podanie danych lub pobranie i uruchomienie oprogramowania typu malware).

Ataki na urządzenia IoT, z których korzysta wiele placówek medycznych. Do takich urządzeń należą przede wszystkim monitory pacjentów czy urządzenia do pomiaru parametrów życiowych. Te oraz inne urządzenia mogą być podatne na ataki, jeśli nie są odpowiednio zabezpieczone.

Naruszenie danych, cyberprzestępcy mogą próbować włamać się do systemów, aby uzyskać dostęp do wrażliwych danych pacjentów. Dane te są wykradane m.in. aby uzyskać od ofiary okup.



DLACZEGO TWOJA PLACÓWKA POWINNA SKORZYSTAĆ Z DOFINANSOWANIA NFZ?

Zarządzenie nr 108/2023/DI z dnia 14 lipca 2023 roku wprowadza szereg zmian, które mają na celu podniesienie poziomu bezpieczeństwa teleinformatycznego u świadczeniobiorców. Zmiany obejmują m.in. możliwość finansowania działań dotyczących miejsc, o których mowa w ustawie o działalności leczniczej. Warto skorzystać z tej możliwości, by zwiększyć bezpieczeństwo pacjentów oraz pracowników.

Kluczowe obszary, które należy zabezpieczyć

Ochrona danych pacjentów

Placówki medyczne gromadzą ogromne ilości wrażliwych danych, które są atrakcyjnym celem dla cyberprzestępców. Właściwe ich zabezpieczenie jest nie tylko kwestią zgodności z prawem, ale przede wszystkim etyczną odpowiedzialnością wobec pacjentów.

Wyróżniamy dwa rodzaje zagrożeń dla wrażliwych danych pacjentów. Jednym z nich jest atak, który zmierza do utraty danych pacjentów np. ransomware. Drugim natomiast jest nieautoryzowany wyciek, będący skutkiem włamania lub nieodpowiedniego zarządzania danymi i ich przechowywania przez pracownika placówki. Dofinansowanie pozwoli na zainwestowanie w najnowsze technologie i praktyki, które zapewnią ochronę tych danych.

Zapewnienie ciągłości działania

Ataki cybernetyczne mogą prowadzić do paraliżu działalności placówek medycznych, co zagraża bezpośrednio życiu i zdrowiu pacjentów. Dzięki dodatkowym środkom pieniężnym placówki mogą zainwestować w systemy, które pomogą im szybko reagować na incydenty i minimalizować ich wpływ na działalność.

Uniknięcie kar finansowych

W przypadku jakiegokolwiek, nawet najmniejszego wycieku danych, placówki mogą zostać obciążone dotkliwymi karami finansowymi. Dodatkowo, pacjenci, których dane zostały naruszone, mogą składać pozwy sądowe. Dofinansowanie pozwoli placówkom na zainwestowanie w systemy i praktyki, które zminimalizują ryzyko takich incydentów.

3 GŁÓWNE ELEMENTY SKUTECZNEJ I BEZPIECZNEJ INFRASTRUKTURY PLACÓWEK MEDYCZNYCH

Bezpieczeństwo teleinformatyczne w placówkach medycznych opiera się na trzech głównych elementach: zabezpieczeniach technicznych, procedurach bezpieczeństwa i szkoleniach dla personelu. Wybór odpowiednich narzędzi i rozwiązań jest kluczowy dla zapewnienia bezpieczeństwa teleinformatycznego. Warto skonsultować się z ekspertami, takimi jak firma Nomios, aby dowiedzieć się, które rozwiązania będą najlepsze dla Twojej placówki.

Tworzenie i utrzymanie systemów kopii zapasowych

To najczęściej proponowane rozwiązanie, które skutecznie zabezpieczy infrastrukturę placówki medycznej. W przypadku ataku ransomware, systemy

kopii zapasowych umożliwiają szybkie przywrócenie danych bez konieczności płacenia okupu.

Polityka DLP

Głównym zadaniem rozwiązania DLP (Data Loss Prevention) jest zapewnienie poufności danych wrażliwych poprzez unikanie przypadkowej lub złośliwej utraty tych danych. Zapobiega to sytuacjom takim jak nieautoryzowany wyciek wrażliwych danych pacjentów.

Utworzenie lub outsourcing SOC

Security Operations Center odpowiada za nadzorowanie działań związanych z bezpieczeństwem. Firma Nomios oferuje organizacjom wsparcie zewnętrznych ekspertów ds. cyberbezpieczeństwa, którzy monitorują środowisko chmury, urządzenia, logi oraz sieć pod kątem zagrożeń. Jest to idealne rozwiązanie, gdy w placówce brak środków na utworzenie własnego zespołu SOC.

SIEM

System SIEM (Security Information and Event Management) potrafi pobierać dane z rozmaitych systemów lub użyć oddzielnej platformy zarządzania logami do utworzenia pojedynczego ekranu monitoringu.

Takie rozwiązanie ułatwia wydajną współpracę między zespołami i ciągły monitoring w czasie rzeczywistym. Cały system zabezpieczeń i sieci przedsiębiorstwa jest ze sobą skorelowany. Umożliwia to również nieprzerwane raportowanie zgodności.

Szkolenia z cyberbezpieczeństwa dla personelu

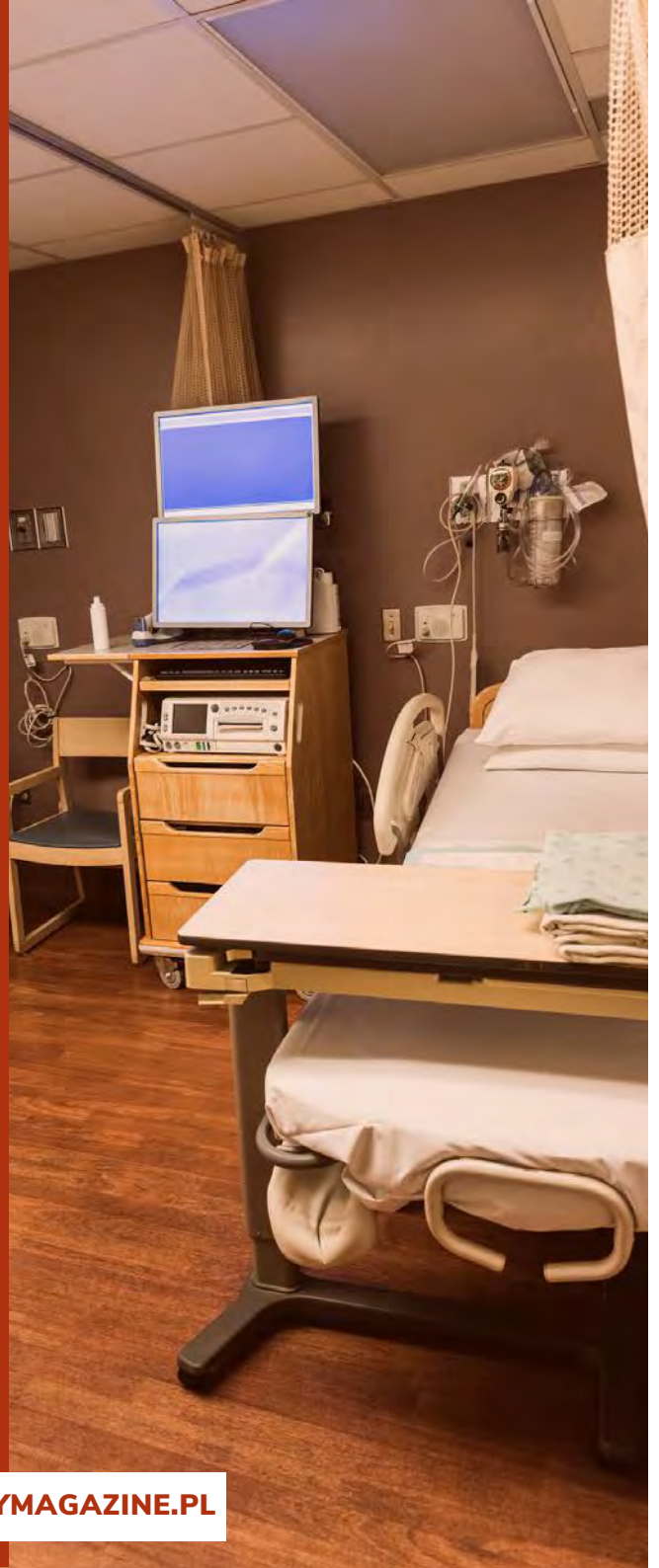
Niestety, to właśnie ludzie są najczęściej wykorzystywanym wektorem ataku, a jednocześnie to czynnik ludzki może również doprowadzić do wycieku danych. Najbardziej wartościowe regularne szkolenia z zakresu cyberbezpieczeństwa skutecznie obniżają ryzyko ataku poprzez phishing, inżynierię społeczną i inne taktyki.

Regularne audyty bezpieczeństwa cyfrowego

Pomagają w identyfikacji potencjalnych luk w zabezpieczeniach i zapewnić, że wszystkie systemy są aktualne i skonfigurowane prawidłowo.

Plan reagowania na incydenty, tzw.: „Damage Control”

Nawet z najlepszymi zabezpieczeniami, istnieje zawsze ryzyko wystąpienia zdarzenia bezpieczeństwa. Ważne jest, aby mieć plan reagowania na incydenty, który określa, jak należy reagować na



potencjalne ataki, jak komunikować się z pacjentami i jak powrócić do normalnej działalności.

Część z tych obszarów może być finansowana za pomocą dodatkowych środków z NFZ przeznaczonych na zwiększenie cyberbezpieczeństwa w placówkach medycznych.

ZADBAJ O SWOICH PACJENTÓW ORAZ PRACOWNIKÓW

Partner programu PWCyber, firma Nomios, dysponuje niezbędnym doświadczeniem i wiedzą, aby pomóc Twojej placówce w zapewnieniu najwyższego poziomu bezpieczeństwa. Przede wszystkim stawia na wątek edukacyjny w docieraniu do grup odbiorców lub potencjalnych klientów. Jak zaznacza sama firma, która pełni rolę podmiotu doradczo-wdrożeniowego we współpracy, najlepszą prewencją przed jakąkolwiek formą cyberataku jest świadomość istniejącego zagrożenia wśród personelu.

Jak podkreślają specjaliści z Nomios „Regularne aktualizacje systemów, szkolenia dla personelu i inwestycje w odpowiednie technologie mogą znacznie zredukować ryzyko ataku.”

DOŁĄCZ DO GRONA EKSPERTÓW "SECURITY MAGAZINE"

EKSPERCI WYDANIA

KAMIL GRZESIK
Account Executive
Dell Technologies

Z firmą Dell Technologies związany jest od 2017 roku. W codziennej pracy pomaga w dobieraniu rozwiązań do tworzenia skutecznych kopii bezpieczeństwa i doradza, w jaki sposób zabezpieczać się przed skutkami udanych ataków ransomware, poprzez odpowiedni dobór technologii przechowywania danych.

RAFAŁ BRUDNICKI
Właściciel
Servers24.pl

Od 12 lat prowadzi firmę Servers24.pl. We współpracy z zespołem specjalistów pomaga dopasować rozwiązania technologiczne do bieżących i przyszłych potrzeb klientów, wspierając ich także w rozwoju bezpiecznej i nowoczesnej infrastruktury IT. Prywatnie pasjonat sportu i motoryzacji.

TOMASZ KOWALSKI
CEO i współzałożyciel
Secfense

CEO i współzałożyciel firmy z branży cybersecurity Secfense. Posiada ponad 20-letnie doświadczenie w sprzedaży technologii IT, brał udział w setkach wdrożeń sprzętu i oprogramowania w dużych i średnich firmach z sektora finansowego, telekomunikacyjnego, przemysłowego i wojskowego.

KRZYSZTOF GÓŹDŹ
Sales Manager
Secfense

Dyrektor Sprzedaży dzielący się pasją do nowych technologii oraz rozwiązań informatycznych. Z wieloletnim doświadczeniem w m.in. IBM i Hewlett Packard Enterprise, gdzie współtworzył największe w kraju centra danych, portale internetowe i klastry obliczeniowe. Pomaga organizacjom rozwiązać problem adopcji silnego uwierzytelniania i toruje drogę do przyszłości bez haseł.

EKSPERCI WYDANIA

RAFAŁ HRYNIEWICZ
Prezes zarządu
E-nform Sp. z o.o.

Ekspert i trener w obszarze whistleblowingu i przeciwdziałania korupcji. Od ponad 25 lat zajmuje się problematyką szeroko pojętego bezpieczeństwa organizacji, a od ponad 6 lat wdraża w organizacjach systemy whistleblowingowe. Wiceprezes zarządu Stowarzyszenia Praktyków Compliance.

ARTUR MARKIEWICZ
Fascynat cyberbezpieczeństwa
netszczon.pl

Lider, trener, konsultant. Cyber Security Consultant w Trecom, członek Zarządu ISSA Polska, członek zespołu Cyfrowy Skaut, lider projektu #ISSAPolskalocal. Realizuje i koordynuje projekty IT dla biznesu, edukacji czy administracji publicznej. Uczy trenerów, nauczycieli, branżowców, jaką i w jaki sposób przekazywać wiedzę dzieciom i dorosłym.

GRZEGORZ DOBROMIŃSKI
Właściciel
Secito – Security Hub

Właściciel firmy Secito – Security Hub, zajmującej się cyber-bezpieczeństwem, ochroną informacji i danych osobowych oraz szkoleniami. Przedsiębiorca i pasjonat związany z branżą IT od 2005 roku, m.in., jako Dyrektor IT i CISO. Pełni rolę inspektora ochrony danych oraz prowadzi szkolenia.

KAMIL RAFAŁ GANCARZ
CEO
BITFOLD AG

Polski finansista, przedsiębiorca, wynalazca, makroinwestor, Prezes Zarządu szwjacarsko-polskiego start-upu technologicz-nego BITFOLD AG oraz aktywny trener polskich inwestorów, ekspert i promotor branży Blockchain w zakresie technologii oraz inwestycji w tym obszarze. Członek Mensa Polska, prelegent wielu konferencji ekonomiczno-biznesowych.

EKSPERCI WYDANIA

JOANNA SAJKOWSKA
Head of Marketing
Grandmetric

Z wykształcenia inżynier telekomunikacji. Od ponad 10 lat pracuje po biznesowej stronie mocy, ale zawsze w organizacjach technicznych. Skupia się na rozpoznawaniu wartości tam, gdzie inni widzą specyfikację. W Grandmetric kieruje marketingiem i komunikacją marki, w tym kampaniami edukacyjnymi z zakresu cyberbezpieczeństwa.

TOMASZ BILL
CEO
thebill oraz Alfa Lingua

Zajmuje się projektowaniem języka komunikacji. Szkoli ze storytellingu jako narzędzia do budowania marek. Właściciel firmy szkoleniowej thebill, założyciel agencji językowej Alfa Lingua, która zajmuje się kursami językowymi, tłumaczeniami i transkreacjami materiałów marketingowych.

TOMASZ GRZELAK
CEO
Stay Safe Poland

Przewodniczący grupy ds. bezpieczeństwa w Polskiej Radzie Facility Managmentu. Security manager z wieloletnim doświadczeniem w międzynarodowym biznesie. Specjalizuje się w obszarze handlu i logistyki, z osiągnięciami we wdrażaniu innowacyjnych projektów technologicznych i organizacyjnych. Specjalista w zakresie negocjacji, zarządzania oraz bezpieczeństwa fizycznego i korporacyjnego. Niezależny konsultant ds. bezpieczeństwa.

ARTUR BICKI
CEO
EMCA Software Sp. z o.o.

Założyciel i prezes firmy EMCA Software Sp. z o.o. - producenta rozwiązania Energy Logserver. Odpowiada za całość strategii rozwoju produktu oraz koordynację prac deweloperskich. Posiada szerokie kompetencje w obszarze monitorowania i bezpieczeństwa sieci oraz metod zapobiegania cyberzagrożeniom i atakom.

EKSPERCI WYDANIA

ADRIAN SROKA
Security Architect
BritishCouncil

Architekt bezpieczeństwa i konsultant IT. Z pasją tworzy nowe rozwiązania oraz udoskonala istniejące, podnosząc jednocześnie ich techniczną, jak i funkcjonalną wartość. W pracy stosuje podejście oparte na współpracy i wiedzy. Zorientowany na zbliżanie do siebie bezpieczeństwa i dewelopmentu.

ŁUKASZ ZAJDEL
Dyrektor Sprzedaży
Perceptus Sp z o. o.

Dyrektor Sprzedaży w Perceptus Sp z o. o. Od roku 2016 związany jest z branżą cybersecurity. Z sukcesem realizuje komplementarne projekty i wdrożenia rozwiązań związanych z bezpieczeństwem IT, zarówno dla klientów komercyjnych jak i publicznych.

JAROSŁAW GNIADO
Head of Sales
Engave S.A.

Magister Uniwersytetu Warszawskiego. Od 2007 roku związany z branżą IT i nowych technologii, w której zarządza zespołami sprzedażowymi. Na co dzień odpowiedzialny na rozwój sprzedaży i biznesu w firmie Engave S.A.

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 oraz szkoleń. Oznacza to współpracę z szerokim gronem pracowników oraz pracę na poziomie strategicznym. Dzięki naszym kompetencjom oraz autorskim metodom pracy, połączonymi z najlepszymi praktykami obowiązującymi w branży jesteśmy w stanie zapewnić kompleksowe rozwiązania dla Twojej firmy lub domu.

Masz problem z kradzieżami w Twojej firmie? Lub może nie masz problemów a stany magazynowe dalej się nie zgadzają? Chcesz wdrożyć najnowsze systemy bezpieczeństwa ale nie wiesz które będą dla Ciebie odpowiednie? Zgłoś się do nas!

Nasz zespół przeanalizuje zgłoszenie, problem i wskaże najlepsze rozwiązanie. Zakres współpracy zostaje ustalony po analizie i określeniu potrzeb tak aby osiągnąć wspólny efekt, który sobie założyliśmy. 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

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

Doradztwo
- Loss prevention
- Business Resilience
- Doradztwo biznesowe
- Zarządzanie kryzysowe
- Interim Security Manager
- Zarządzanie ciągłością działania

Zainteresowany współpracą?
Skontaktuj się z nami i umów na bezpłatną konsultację!

KATALOG FIRM

servers24.pl

SERVERS24.PL

ul. Bohaterów Warszawy 4

05-800 Pruszków

Dane kontaktowe

+48 793 515 123

+48 793 753 123

Handlowy@Servers24.pl

Specjalizacje

cybersecurity | backup | virtualization | hardware | software | cloud | HCI | UPS

W Servers24.pl dostarczamy sprzęt i usługi IT, wspierając Klientów w wyborze nowoczesnych rozwiązań technologicznych niezbędnych do rozwoju ich biznesu. Nasz zespół specjalistów towarzyszy Klientom podczas projektów wymagających zarówno doradztwa, jak i wiedzy technicznej, dostosowując możliwości produktów do bieżących i przyszłych potrzeb firmy.

Od ponad 10 lat dostarczamy do firm w całej Polsce mobilne narzędzia pracy, systemy i sieci komputerowe, pełną infrastrukturę informatyczną oraz telefonię i komunikację. Realizujemy projekty między innymi z zakresu architektury hiperkonwergentnej, wirtualizacji i cloud computing, systemów i sieci komputerowych oraz cyberbezpieczeństwa i backupu.

Współpracujemy z liderami wśród producentów sprzętu i oprogramowania, między innymi z firmą Dell, Lenovo, Cisco, Microsoft, Amazon, ESET, APC, EATON, Poly, VMware czy Veeam.

Zapewniamy:

- krótki i prosty proces zakupowy (minimum biurokracji),
- szybkie wdrożenie,
- wsparcie ekspertów na każdym poziomie procesu zakupowego.

Let's talk about IT!

KATALOG FIRM

nomios

NOMIOS POLAND SP. Z O.O.

ul. Puławska 537
02-844 Warszawa

Dane kontaktowe
+48 22 567 17 40
info@nomios.pl

Specjalizacje

security | NGFW | backup | DLP | EDR | SIEM | networking | SOC | chmura | OT/IT | SOAR

Partner programu PWCyber realizowanego przez Ministerstwo Cyfryzacji

Nomios Poland to wiodący dostawca rozwiązań i usług z zakresu nowoczesnych systemów cyberbezpieczeństwa, sieci krytycznych dla biznesu, rozwiązań chmurowych i usług zarządzanych. Łącząc technologie, procesy oraz fachową wiedzę tworzymy rozwiązania i usługi następnej generacji. Klienci cenią nas za wysokiej jakości usługi i doskonałość operacyjną. Nasi partnerzy strategiczni należą do wiodących dostawców technologii na świecie.

Posiadamy najwyższe statusy partnerskie u producentów większości oferowanych systemów, a nasi inżynierowie mogą się pochwalić szerokim doświadczeniem w zakresie tworzenia kompleksowych architektur. Oferujemy autorskie rozwiązania SOC24 (Security Operations Center) oraz GREENmod (System do klasyfikacji dokumentów oraz poczty elektronicznej).

Dlaczego Nomios?

- Ponad 40 partnerów technologicznych
- Ponad 400 certyfikowanych inżynierów
- Ponad 20 lat doświadczenia
- Całodobowa obsługa Klienta na całym świecie.
  Wskaźnik satysfakcji Klienta na poziomie 8.9
- 2000+ zadowolonych Klientów
- Wśród naszych klientów:
  - Bankowość i finanse (m.in. NBP, Peako, BGK)
  - Administracja
    (m.in. NASK, Lubelskie Centrum Innowacji i Technologii)
  - Przemysł (m.in. ArcelorMittal, Grupa Azoty, PKP Intercity)
  - Telekomunikacja (m.in. Orange Polska)
  - Pozostałe (m.in. Budimex, LOT, EURO-net)
- Nomios w roli laureatów nagród branżowych, na przykład:
  - Diamenty Forbesa 2022
  - Worldwide Partner of the Year for 2022 (Juniper Networks)

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

Wydanie 4(13)/2023
POBIERZ

Wydanie 5(14)/2023
POBIERZ

Wydanie 6(15)/2023
POBIERZ

Wydanie 7(16)/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

Projekt, skład i korekta: Monika Świetlińska

Współpraca i kontakt: redakcja@securitymagazine.pl

SECURITYMAGAZINE.PL