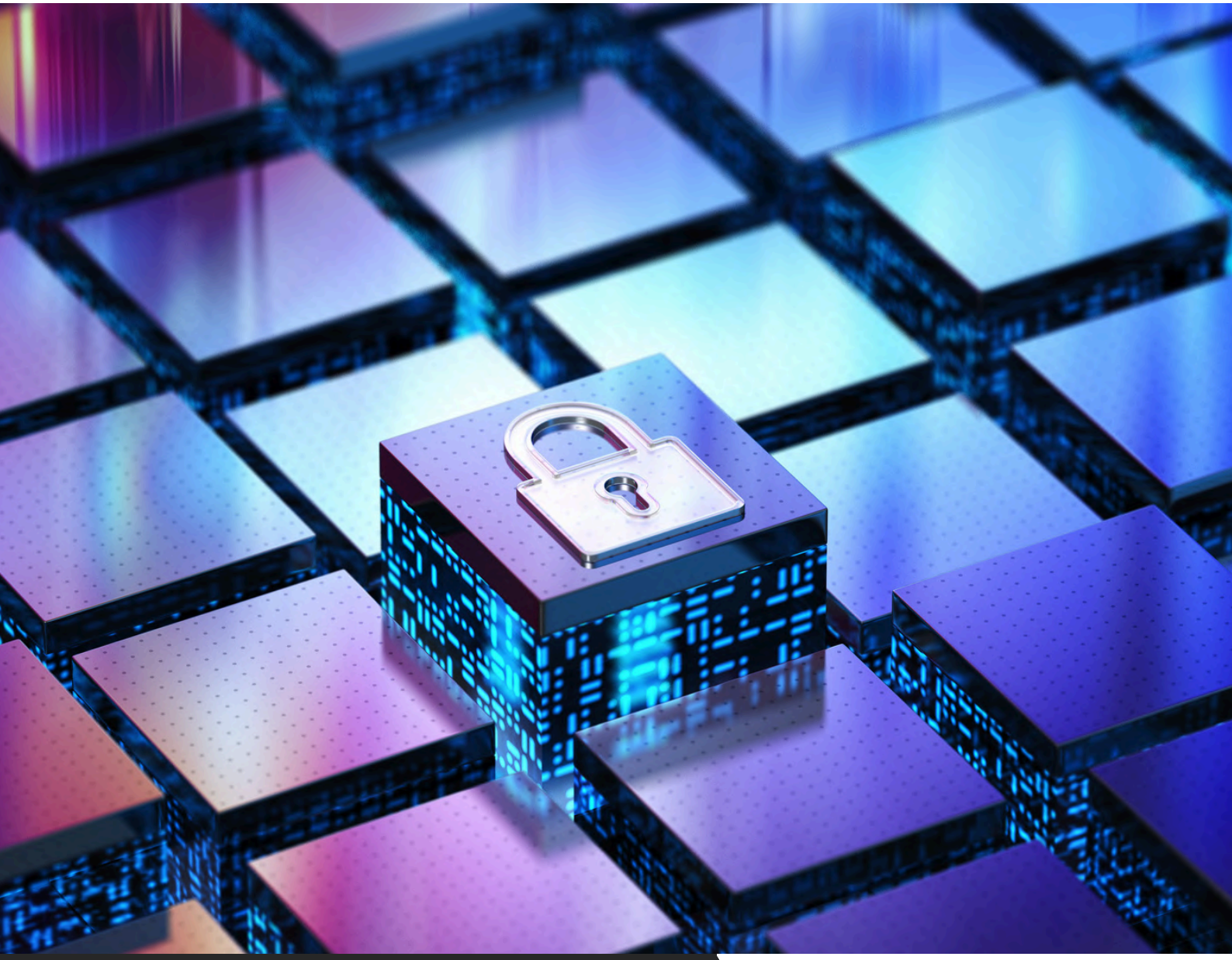
POLSKIE STOWARZYSZENIE ESG



CYBERBEZPIECZEŃSTWO A ZRÓWNOWAŻONY ROZWÓJ

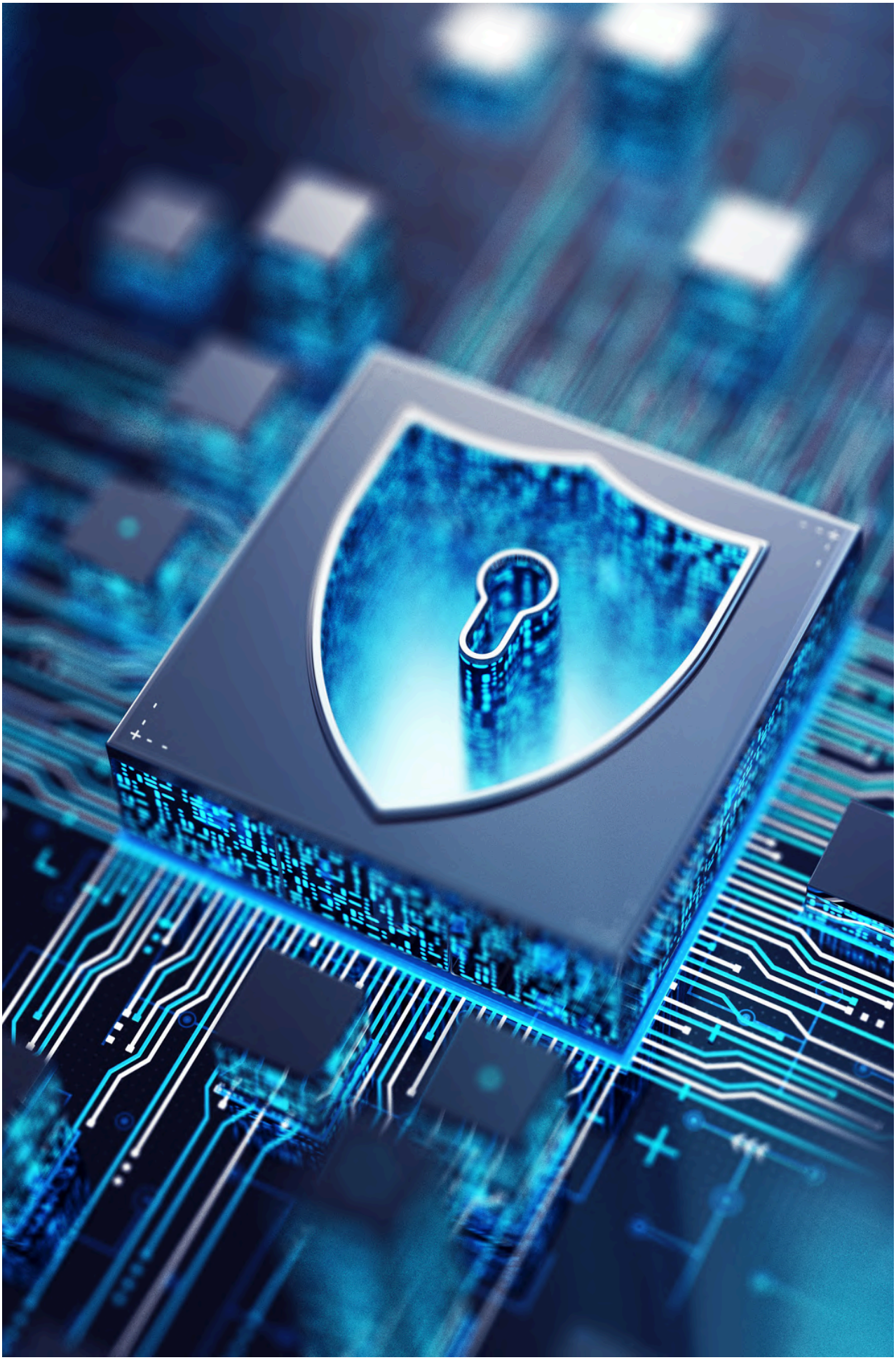
POLSKIE STOWARZYSZENIE ESG

www.polskiestowarzyszenieesg.pl

PARTNERZY MERYTORYCZNI RAPORTU:

SOLET

GS1 Polska



Szanowni Państwo,

Gdyby cyberzagrożenia były krajem, byłyby jedną z najbogatszych gospodarek świata. Konkretnie znalazłyby się na trzecim miejscu – zaraz za USA i Chinami.

Cyberzagrożenia powodują więcej szkód niż PKB Niemiec, Indii i Japonii – łącznie!

Cyberzagrożenia w 2024 r. spowodowały 9,5 biliona dol. strat na całym świecie.

Ogromna skala i rentowność cyberzagrożeń sprawiają, że cyberbezpieczeństwo jest jedną z najważniejszych inwestycji dla przedsiębiorstw i rządów na całym świecie.

W raporcie, który trzymacie Państwo w rękach przedstawiamy główne zagrożenia związane z cyberbezpieczeństwem które mogą być szczególnie szkodliwe dla branży ESG, najbardziej wartościowe sposoby przeciwdziałania zagrożeniom i regulacje związane z sektorem, które będą wyznaczać trendy w zakresie bezpieczeństwa danych, zarządzania ryzykiem i przejrzystości operacyjnej.

Życzymy przyjemnej lektury!

Joanna Dargiewicz - Rożek
Członkini Zarządu PSE

Marta Biernacka - Miernik
Członkini Zarządu PSE

CZĘŚĆ 1

Cyberzagrożenia

Najczęstsze zagrożenia w obszarze cyberbezpieczeństwa – phishing, ransomware, ataki DDoS, manipulacja danymi środowiskowymi.

Obecnie firmy i organizacje stają się coraz bardziej narażone na cyberzagrożenia, ponieważ gromadzą i przetwarzają coraz większą ilość danych. Dotyczy to także informacji z obszaru ESG (Environmental, Social, Governance), które mają kluczowe znaczenie dla ich wizerunku i działalności.

Im bardziej rola danych ESG rośnie na znaczeniu, tym większa liczba cyberprzestępców ma nadzieję na przeniknięcie do wnętrza systemów firmy. W tym celu wykorzystują powszechnie znane, ale też najbardziej skuteczne techniki.

Phishing – czyli wyłudzanie danych. Najczęściej odbywa się to za pomocą spreparowanego e-maila, który może podszywać się pod jednego z podwykonawców, regulatorów ESG, organizacje pozarządowe lub inwestorów, w celu uzyskania dostępu do cennych danych albo by wyłudzić pieniądze za rzekome naruszenia prawa.

W lipcu 2024 r. Amerykańska Agencja Ochrony Środowiska (EPA) ostrzegała, że oszuści, podszywając się pod nią wysyłają fałszywe e-maile, zawiadamiające o naruszeniu przepisów (Notice of Violation) do firm,

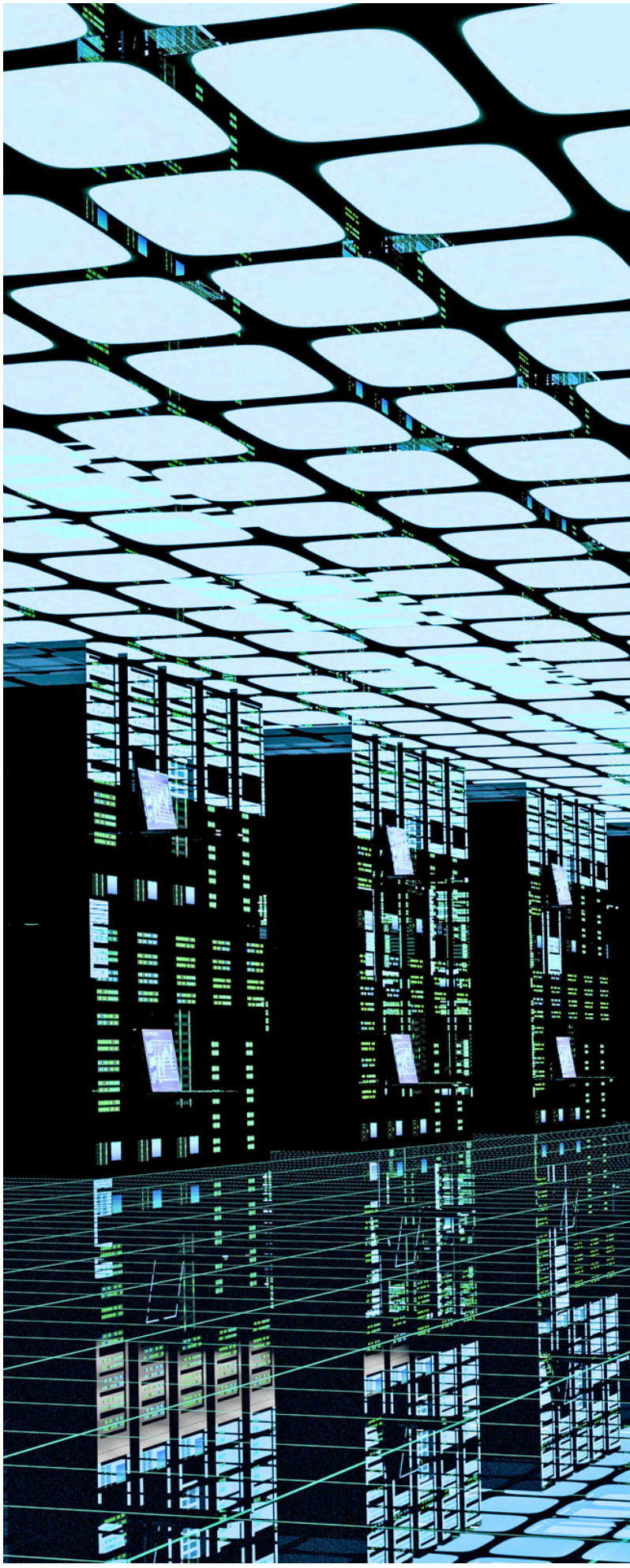
żądając od nich zapłaty za rzekome naruszenia przepisów środowiskowych, takich jak Ustawa o czystym powietrzu (Clean Air Act).

Ale phishing może mieć też znacznie łagodniejszą postać – to może być załącznik w wiadomości od rzekomego kontrahenta, zawierający dane środowiskowe. W 2016 r. przestępcom udało się przeniknąć do ściśle chronionej infrastruktury Banku Centralnego Bangladeszu, bo jeden z pracowników otworzył CV potencjalnego kandydata do pracy.

Managerowie ESG powinni być szczególnie wyczuleni na tzw. **spear phishing,** czyli na wyjątkowo wysublimowaną formę phishingu. Polega ona na tym, że przestępcy zanim wyślą oszukańczego maila robią dokładny wywiad na temat ofiary, by podszywać się np. pod współpracownika lub znajomą osobę z innej spółki. Dokładnie analizują jej wpisy w serwisach społecznościowych i obserwują dynamikę znajomości z osobą, pod którą chcą się podszyć, żeby poznać np. jej charakterystyczne powiedzonka lub poczucie humoru.

Innym typem zagrożenia jest **ransomware** (ang. ransome – okup). To złośliwe oprogramowanie, które szyfruje zawartość komputera ofiary (a w skrajnych przypadkach nawet całej organizacji) i obiecuje ją odblokować dopiero po wpłaceniu słonego okupu, najczęściej w postaci kryptowalut.

Również firmy dostarczające usługi w obszarze ESG (np. kalkulatory śladu



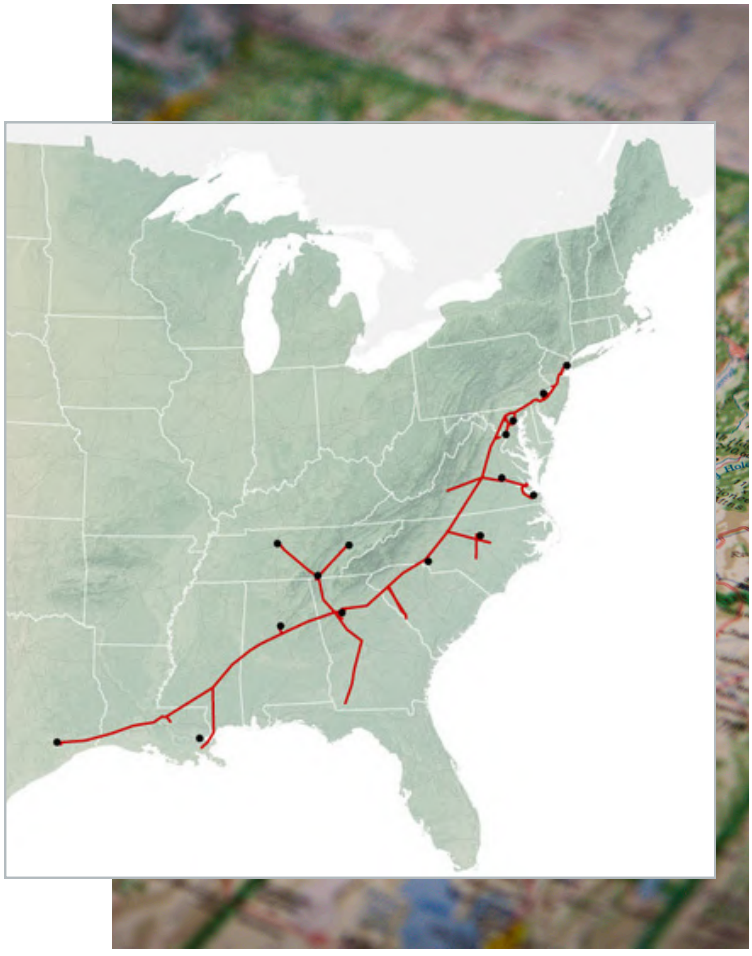
węglowego, systemy zbierania danych) są atrakcyjnym celem, ponieważ przechowują wrażliwe informacje dotyczące emisji dwutlenku węgla, polityki równościowej czy strategii zrównoważonego rozwoju. Utrata tych danych może prowadzić do problemów regulacyjnych i reputacyjnych.

Atak **DDoS** jest z punktu widzenia atakowanego najmniej uciążliwym spośród cyberataków. Przede wszystkim dlatego, że przeważnie z jego powodu nie dochodzi do szkód wizerunkowych lub finansowych. Firmy ESG mogą paść ofiarą takich ataków ze względu na ich znaczenie dla rynków finansowych i polityki korporacyjnej. Atak DDoS może zakłócić działanie platform monitorujących środowisko, systemów raportowania czy stron internetowych organizacji ESG.

CASE STUDY #1

Colonial Pipeline – bezprecedensowy okup

W maju 2021 r. doszło do największego w historii ataku na infrastrukturę naftową USA. Colonial Pipeline to amerykańska firma, która przesyła ropę i paliwa ropopochodne z Teksasu do Nowego Jorku i wielu stanów po drodze. Zarządza ona największym systemem ropociągów w USA o długości ponad 8,8 tys. km. Około 55 proc. paliw konsumowanych na wschodnim wybrzeżu Stanów Zjednoczonych jest dostarczanych właśnie przez nią.



7 maja 2021 r. przesył ropy został wstrzymany. Ani kropla paliwa nie popłynęła tym ropociągiem aż do 12 maja – a powrót do pełnej sprawności wszystkich systemów zajął jeszcze więcej czasu.

...wszystko przez ransomware, który sparaliżował działanie firmy.

Przestępcy początkowo celowali w dział finansów, ale ostatecznie dostali się do sieci spółki w banalny sposób – pozyskali hasło związane z narzędziem VPN (virtual private network, czyli oprogramowanie, które m.in. zdalnie pozwala połączyć się z systemem firmy). VPN nie miał dodatkowych zabezpieczeń w postaci weryfikacji dwuetapowej.

W efekcie wstrzymania działalności Colonial Pipeline w wielu stanach USA zaczęło brakować paliwa. Niektóre lotniska, np. w Charlotte czy Atlancie zmuszone były do odwołania lub zmiany części lotów. Amerykanie rzucili się do stacji benzynowych robić zapasy paliwa, co doprowadziło do braków zaopatrzenia, a średnia cena paliwa poszybowała do rekordowych poziomów. 9 maja, dwa dni po ataku, ówczesny prezydent Joe Biden wprowadził stan wyjątkowy, który zniósł ograniczenia na transport produktów naftowych w USA. Wszystko w celu jak najszybszego uporania się z niedoborem paliwa.

W ciągu kilku godzin od zaszyfrowania danych Colonial Pipeline zgodził się zapłacić okup. Włamywacze żądali 75 bitcoinów, co w tamtym czasie wynosiło 4,4 mln dol. Płatność została dokonana pod nadzorem FBI.

Poważne zakłócenia w dostawach paliwa na wschodnim wybrzeżu USA miały swoje konsekwencje środowiskowe. Wzrosły ceny paliw, co miało bezpośredni wpływ na koszty transportu i emisję CO2. Braki paliwa zmusiły wiele firm do korzystania z alternatywnych źródeł energii, co wpłynęło na strategie ESG w zakresie zrównoważonego transportu. Atak zwiększył również presję regulacyjną na sektor energetyczny, co doprowadziło do zaostrzenia przepisów dotyczących cyberbezpieczeństwa w infrastrukturze krytycznej oraz wdrożenia surowszych wymogów w raportowaniu ryzyka ESG, takich jak obowiązek stosowania zaawansowanych systemów cyberbezpieczeństwa, regularne audyty zgodności oraz bardziej rygorystyczne wymogi dotyczące szyfrowania i przechowywania danych poufnych.

Wpływ cyberataków na zaufanie i reputację firmy

Cyberataki, w tym te związane z obszarem ESG, mogą poważnie zaszkodzić reputacji firmy oraz wpłynąć na poziom zaufania interesariuszy. Konsekwencje obejmują:

- **Utratę wiarygodności wśród inwestorów i klientów.**
  Firmy, które padły ofiarą cyberataków, mogą zostać uznane za niewiarygodne w zakresie zarządzania danymi – w tym także danymi ESG, co prowadzi do spadku wartości akcji oraz trudności w pozyskiwaniu kapitału.

- **Obniżenie ratingów ESG.**
  Organizacje oceniające zrównoważony rozwój firm mogą obniżyć ich oceny w rankingach ESG, co wpływa na ich pozycję na rynku i możliwości współpracy z partnerami biznesowymi.

- **Straty finansowe wynikające z kar i pozwów.**
  Naruszenia danych mogą skutkować nałożeniem wysokich kar finansowych przez regulatorów, a także pozwami zbiorowymi ze strony klientów lub organizacji ekologicznych. Przykładem może być atak ransomware na firmę Norsk Hydro w 2019 r., który doprowadził do strat rzędu 70 mln dol. oraz opóźnień w raportowaniu emisji CO2. Opóźnienia te skutkowały potencjalnymi sankcjami ze strony regulatorów oraz utratą zaufania inwestorów, co miało negatywny wpływ na rating ESG firmy.

- **Długofalowa utrata zaufania społecznego.**
  Firmy, które uwzględniają zrównoważony rozwój w swojej strategii biznesowej, kształtują swój wizerunek poprzez transparentność i odpowiedzialność. Incydenty związane z cyberatakami mogą osłabić ten wizerunek i zmniejszyć lojalność konsumentów oraz partnerów biznesowych.

- **Wzrost kosztów operacyjnych.**
  Firmy zmuszone są inwestować znaczne środki w poprawę zabezpieczeń, audyty oraz działania naprawcze, co może osłabić ich zdolność do realizacji celów zrównoważonego rozwoju.

CZĘŚĆ 2

Ryzyka związane z danymi i regulacjami

Ochrona danych

Bezpieczne przechowywanie danych ESG to kluczowe wyzwanie dla wszystkich firm raportujących w tych obszarach. Muszą dopilnować nie tylko, aby dane ze wszystkich obszarów i spółek córek spływały na czas, lecz także wybrać odpowiedni i bezpieczny sposób ich przechowywania.

Do wyboru jest kilka sposobów.

Narzędzie na miarę
To rozwiązanie tylko dla największych i najbardziej zasobnych podmiotów. Tylko takie stać na to, żeby ich dział IT samodzielnie od podstaw stworzył narzędzie, które będzie doskonale skrojone pod potrzeby danej organizacji.

Takie rozwiązanie ma wiele plusów: daje organizacji pełną kontrolę – i to już od etapu projektowania. Można zadecydować o funkcjach narzędzia i dopasować je do swoich potrzeb i procedur.

W przypadku takich narzędzi firma nie jest zależna od żadnego innego podmiotu – nie jest skazana na regulamin dostawcy ani potencjalne zmiany w abonamencie. Takie rozwiązanie jest też najbezpieczniejsze – można od podstaw wdrożyć niestandardowe zabezpieczenia, doskonale zespolone z całą infrastrukturą firmy i ze wszystkimi politykami.

Ale oczywiście wszytko to sprawia, że jest to opcja najdroższa – i to zarówno jeśli chodzi o koszty jego wdrożenia, jak i utrzymania. Czas potrzebny na oddanie gotowego produktu też będzie długi.

Chmura komercyjna

Czyli taka od dużego dostawcy, typu Microsoft, Google, Amazon. Takie narzędzie bardzo ułatwia zbieranie danych ESG – można zrobić współdzielony folder i cały zespół może jednocześnie pracować na przechowywanych tam plikach. Takie rozwiązanie jest w miarę tanie (nie wymaga budowania infrastruktury), elastyczne, ma dość wysoki poziom zabezpieczeń, zespół ma do niego dostęp z dowolnego urządzenia i miejsca na świecie.

Jednak firmy, które go wybiorą, będą zależne od dostawcy – będą musiały się liczyć z tym, że w każdej chwili mogą zmienić się warunki użytkowania, cena lub polityka prywatności. Choć rozwiązania chmurowe są dość dobrze zabezpieczone, to jednak mogą one być celem ataków. Może się też zdarzyć, że współpracownik udostępni przechowywane w chmurze dane osobie, która nie powinna mieć do nich dostępu. Powstaje też pytanie, czy w przyszłości dane przechowywane w komercyjnych chmurach nie będą wykorzystywane do trenowania sztucznej inteligencji wielkich firm technologicznych. Google już teraz trenuje swoją AI na publicznie dostępnych Dokumentach Google i publicznie dostępnych komentarzach z Map.

Gotowe narzędzie dla managerów ESG

Gotowe oprogramowanie do zarządzania danymi ESG, takie jak IBM Envizi, Diaphane, Synesgy, CoZero czy Envirly, może być atrakcyjnym rozwiązaniem, ponieważ oferuje zgodność z regulacjami, automatyzację raportowania oraz minimalne wymagania konfiguracyjne. Z punktu widzenia cyberbezpieczeństwa, korzystanie z takiego narzędzia może mieć jednak zarówno zalety, jak i ryzyka.

Zaletą jest to, że renomowani dostawcy zazwyczaj zapewniają wysokie standardy zabezpieczeń, regularne aktualizacje i zgodność z wymogami prawnymi. Dane są chronione w profesjonalnie zarządzanych centrach danych, co zmniejsza ryzyko związane z lokalnymi awariami lub atakami. Dodatkowo, zewnętrzne oprogramowanie często oferuje funkcje monitorowania, audytu oraz szyfrowania, które mogą przewyższać wewnętrzne rozwiązania firmowe.

Z drugiej strony, korzystanie z gotowego narzędzia oznacza częściowe uzależnienie od dostawcy. Firmy muszą dokładnie przeanalizować politykę prywatności i warunki przechowywania danych, zwracając uwagę na lokalizację serwerów oraz zgodność z regulacjami dotyczącymi transferu danych (np. RODO). Istotnym ryzykiem jest także możliwość podwyżek cen, zmiany warunków użytkowania lub nawet zakończenia wsparcia dla platformy, co może skomplikować długoterminowe zarządzanie danymi ESG.

Decydując się na gotowe oprogramowanie, warto sprawdzić, czy dostawca oferuje możliwość eksportu danych w otwartych formatach, co ułatwi ich ewentualne przeniesienie do innego systemu. Kluczowe jest także zapewnienie wielopoziomowej kontroli dostępu, regularnych testów penetracyjnych oraz zabezpieczeń przed nieautoryzowanym dostępem, aby zminimalizować ryzyko cyberataków.

Przyszłość cyberbezpieczeństwa w ESG: Nowe wyzwania i technologie zabezpieczające (AI, blockchain, analiza zagrożeń w czasie rzeczywistym).

Wraz z rosnącą cyfryzacją i naciskiem na zrównoważony rozwój, cyberbezpieczeństwo stało się kluczowym elementem strategii ESG (Environmental, Social, Governance). Nie jest to już jedynie kwestia ochrony aktywów cyfrowych, ale fundamentalny aspekt wpływający na reputację, stabilność finansową i zaufanie interesariuszy.

W niniejszej publikacji przedstawiamy krótką analizę trendów i przykłady nowoczesnych technologii, które rewolucjonizują podejście do ochrony oraz integralności danych, zmniejszają ryzyka związane z cyberbezpieczństwem i minimalizują czas reakcji na incydenty.

Zacznijmy jednak od wyzwań:

(Environment):
Cyberataki mogą prowadzić do poważnych konsekwencji, takich jak szkody środowiskowe poprzez destabilizację systemów kontroli infrastruktury.

(Social):
AI jest wykorzystywane do ciągłego ulepszania ataków, co chwilę pojawiają się nowe kampanie phishingowe, vishingowe i inne, gdzie modele AI umożliwiają podszycie się pod członków naszej organizacji nie tylko tekstem, ale również głosem i video imitującym naszych pracowników. Ponadto, deficyt specjalistów łączących wiedzę z zakresu AI i cyberbezpieczeństwa utrudnia wdrażanie skutecznych rozwiązań.

(Governance):
Wymóg raportowania ESG zwiększa presję na wiarygodność danych, które też mogą być celem ataków.

PARTNER MERYTORYCZNY: SOLET

Technologie zabezpieczające:

Analiza zagrożeń w czasie rzeczywistym z wykorzystaniem sztucznej inteligencji (AI) jest kluczowym elementem nowoczesnych strategii cyberbezpieczeństwa, umożliwiającym szybkie wykrywanie i reagowanie na potencjalne ataki. Dzięki zaawansowanym technologiom, takim jak systemy SIEM (Security Information and Event Management) oraz SOAR (Security Orchestration, Automation and Response), a także narzędzia do analizy behawioralnej, organizacje mogą monitorować aktywność w swojej infrastrukturze i identyfikować anomalie mogące wskazywać na zagrożenia. Wykorzystanie AI w tych systemach pozwala na automatyzację analizy ogromnych ilości danych, wykrywanie wzorców i anomalii, które byłyby trudne dla człowieka do zauważenia oraz przewidywanie potencjalnych ataków na podstawie analizy historycznych danych.

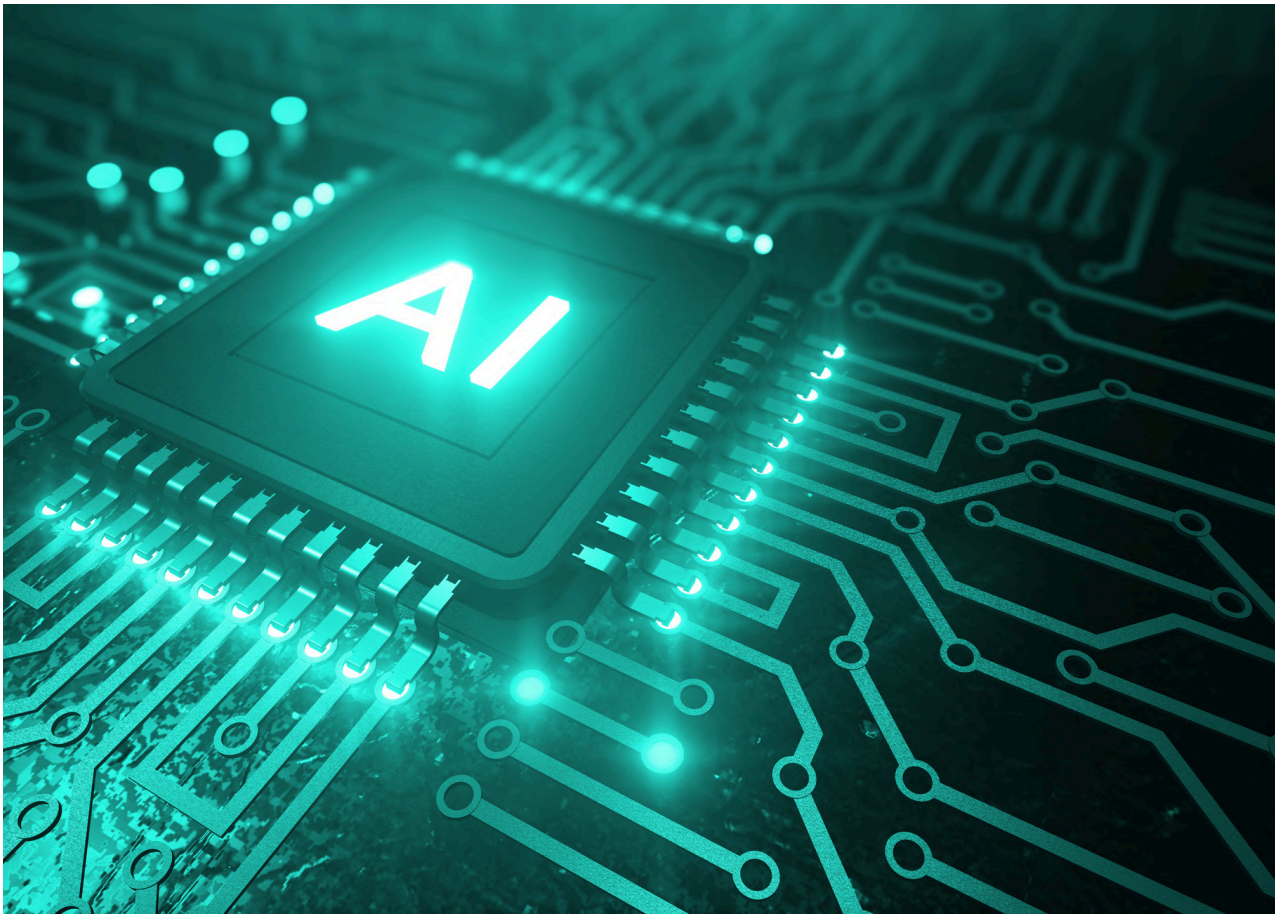
Platforma IBM QRadar wykorzystuje AI do analizy i korelacji danych z różnych źródeł, takich jak logi systemowe, zdarzenia sieciowe czy informacje o zagrożeniach. Algorytmy uczenia maszynowego w QRadar są wykorzystywane do budowania modeli behawioralnych, które pozwalają na identyfikację nietypowych zachowań użytkowników i systemów. AI w QRadar umożliwia również automatyczne wykrywanie zaawansowanych zagrożeń, takich jak ataki zero-day, które nie są oparte na znanych sygnaturach. Dodatkowo, QRadar wykorzystuje AI do redukcji fałszywych alarmów, co pozwala analitykom skupić się na rzeczywistych zagrożeniach.

Wsparcie do obsługi incydentów zapewnia rozwiązanie IBM SOAR, które m.in. dzięki chatbotowi i analizie incydentów, wspartej modelami AI oraz automatyzacji, może znacząco przyspieszyć, a także uprościć pracę operatorów zajmujących się na co dzień taką analizą. Modele AI w IBM SOAR są wykorzystywane do automatycznego klasyfikowania incydentów, priorytetyzacji działań oraz sugerowania optymalnych scenariuszy reakcji na ataki.

Kolejnym rozwiązaniem, które uzupełnia takie środowisko, jest IBM Verify Identity Protection, który pomaga organizacjom ograniczać ryzyko związane z zarządzaniem tożsamością i dostępem, zapewniając solidną ochronę przed ewoluującymi zagrożeniami. AI w IBM Verify Identity Protection jest wykorzystywane do analizy behawioralnej użytkowników, wykrywania nietypowych wzorców logowania oraz identyfikacji potencjalnych prób przejęcia kont. Dzięki takim rozwiązaniom, firmy mogą nie tylko chronić swoje zasoby, ale również minimalizować ryzyko przestojów operacyjnych i utraty danych. Co więcej, AI pozwala na ciągłe uczenie się systemów bezpieczeństwa, adaptując się do nowych zagrożeń i technik ataków, co jest kluczowe w dynamicznie zmieniającym się krajobrazie cyberbezpieczeństwa.

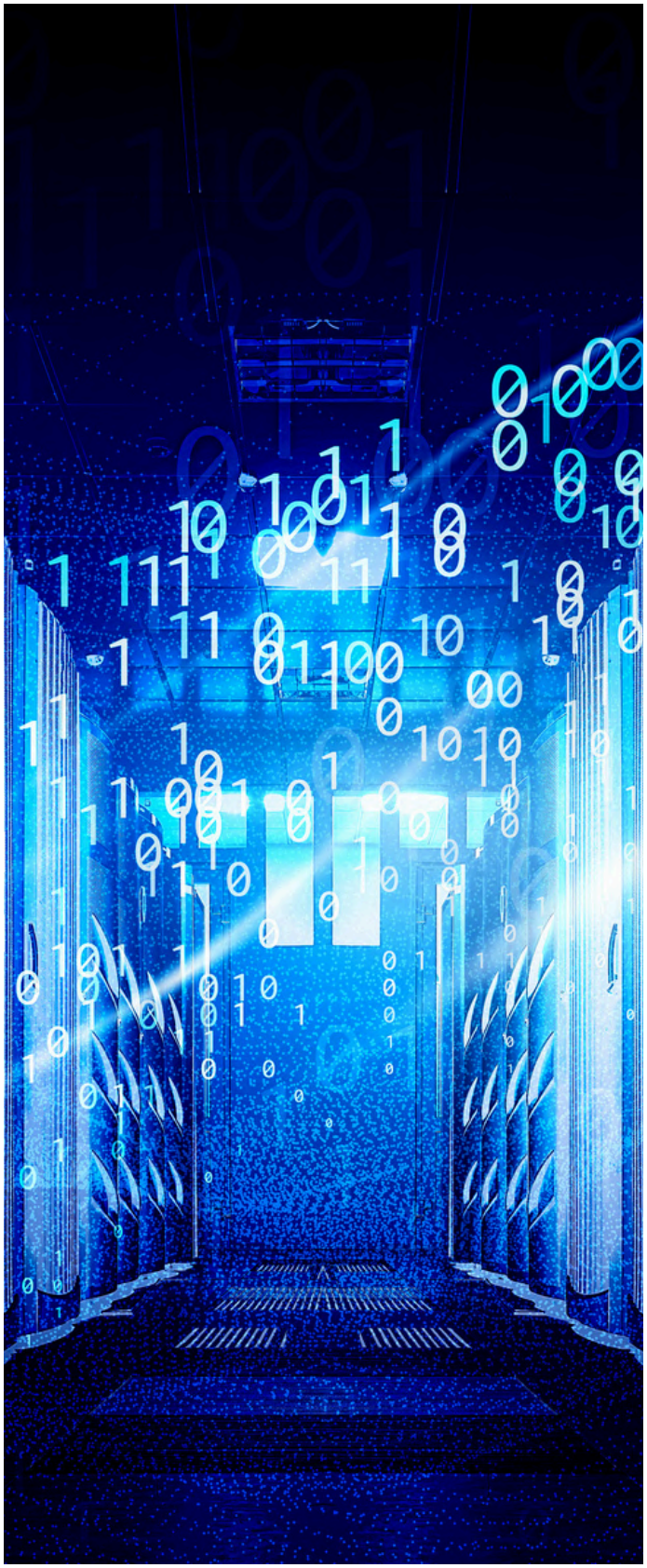
Oprócz szybkiego reagowania na bieżące zagrożenia, kluczowym elementem efektywnej analizy w czasie rzeczywistym jest budowanie i utrzymywanie dogłębnej wiedzy o infrastrukturze IT organizacji. Wykorzystanie narzędzi takich jak Microsoft Intune czy IBM MaaS360 umożliwia centralne zarządzanie urządzeniami i aplikacjami, co przekłada się na lepszą widoczność oraz kontrolę nad środowiskiem IT. Platformy te dostarczają szczegółowe informacje o konfiguracji urządzeń, zainstalowanym oprogramowaniu, a także o potencjalnych lukach w zabezpieczeniach, dzięki temu zespoły cyberbezpieczeństwa mogą proaktywnie identyfikować i eliminować słabe punkty, zanim zostaną wykorzystane przez cyberprzestępców.

Integracja danych z Intune czy MaaS360 z systemami SIEM/SOAR pozwala na korelację zdarzeń z różnych źródeł, co umożliwia wykrywanie złożonych ataków, które mogłyby pozostać niezauważone przy analizie pojedynczych logów. Na przykład, nietypowe logowanie z urządzenia zarządzanego przez Intune, w połączeniu z podejrzaną aktywnością sieciową, może wskazywać na kompromitację konta użytkownika. Regularne aktualizacje wiedzy o infrastrukturze, automatyzacja procesów inwentaryzacji i konfiguracji, a także wykorzystanie analizy behawioralnej (np. IBM Verify Trust), pozwalają na szybkie wykrywanie anomalii oraz minimalizację czasu reakcji na incydenty.



Wykorzystanie sztucznej inteligencji (AI) w obszarze ESG

Wykorzystanie sztucznej inteligencji (AI) w obszarze ESG otwiera nowe możliwości dla organizacji umożliwiając bardziej efektywne zarządzanie ryzykiem i optymalizację działań z zakresu zrównoważonego rozwoju. Prognozowanie ryzyk z wykorzystaniem AI staje się kluczowym narzędziem, pozwalającym na identyfikację potencjalnych zagrożeń w łańcuchach dostaw, które mogą mieć negatywny wpływ na środowisko. Algorytmy AI, analizując dane z różnych źródeł, takie jak informacje o dostawcach, dane logistyczne i czynniki zewnętrzne, są w stanie przewidzieć luki oraz słabe punkty w łańcuchu dostaw, co pozwala na wdrożenie działań zapobiegawczych. Na przykład, AI może pomóc w identyfikacji dostawców, którzy stosują niezgodne ze zrównoważonym rozwojem praktyki, lub przewidzieć ryzyko opóźnień w dostawach, mogące prowadzić do zwiększenia emisji CO2, dzięki temu organizacje mają szansę redukować ryzyko środowiskowe, minimalizować negatywny wpływ na społeczności lokalne i poprawiać efektywność operacyjną.



W kontekście analizy danych ESG, kluczową rolę odgrywają platformy takie jak IBM Envizi, które wykorzystują AI do automatyzacji zbierania, analizy i raportowania danych związanych ze zrównoważonym rozwojem. IBM Envizi pozwala organizacjom na centralizację danych ESG z różnych źródeł, takich jak zużycie energii, emisje gazów cieplarnianych, dane dotyczące gospodarki odpadami czy informacje o społecznej odpowiedzialności biznesu. Dzięki zastosowaniu algorytmów AI, platforma umożliwia automatyczne wykrywanie anomalii i trendów w danych, co pozwala na identyfikację obszarów wymagających poprawy i monitorowanie postępów w realizacji celów ESG. IBM Envizi wspiera również generowanie raportów zgodnych z międzynarodowymi standardami, takimi jak GRI (Global Reporting Initiative) czy SASB (Sustainability Accounting Standards Board), co ułatwia organizacjom budowanie transparentności i wiarygodności w relacjach z interesariuszami. Dzięki takim narzędziom, firmy mogą nie tylko efektywniej zarządzać swoimi działaniami ESG, ale także wykorzystywać dane do podejmowania strategicznych decyzji, które wspierają zrównoważony rozwój i budują długoterminową wartość dla organizacji.

Technologia blockchain, choć kojarzona głównie z kryptowalutami, znajduje coraz szersze zastosowanie w cyberbezpieczeństwie oferując unikalne możliwości zabezpieczania danych i transakcji. Dzięki swojej zdecentralizowanej naturze oraz niezmienności zapisów, blockchain umożliwia tworzenie odpornych systemów, minimalizujących ryzyko manipulacji i ataków.

W kontekście ESG, blockchain może znacząco poprawić bezpieczeństwo cyfrowe, zapewniając integralność danych, zarządzanie tożsamością oraz zabezpieczanie transakcji finansowych. Przykłady zastosowania obejmują finanse i bankowość, gdzie platformy takie jak Onyx od JPMorgan Chase umożliwiają szybsze, a także bezpieczniejsze transfery pieniężne. W zarządzaniu tożsamością blockchain zapewnia bezpieczne przechowywanie i weryfikację tożsamości cyfrowych, zapobiegając kradzieży tożsamości oraz oszustwom. W opiece zdrowotnej technologia ta umożliwia bezpieczne przechowywanie i udostępnianie danych pacjentów oraz śledzenie autentyczności leków. W łańcuchu dostaw, blockchain zapewnia śledzenie produktów i ich zgodność z normami etycznymi. W sektorze nieruchomości smart kontrakty automatyzują transakcje, a w sztuce i rozrywce NFT reprezentują własność cyfrowych dzieł sztuki. Mimo wyzwań związanych ze skalowalnością i integracją, blockchain ma potencjał, aby znacząco wzmocnić bezpieczeństwo cyfrowe w kontekście ESG.

Przyszłość cyberbezpieczeństwa wymaga od nas proaktywnego podejścia i przygotowania na nadchodzące wyzwania. Jednym z kluczowych kierunków rozwoju jest Quantum-Safe Cryptography, czyli kryptografia odporna na ataki kwantowe. Wraz z postępem technologii kwantowych, obecne algorytmy szyfrujące, które stanowią fundament naszego bezpieczeństwa cyfrowego, stają się podatne na złamanie. Prognozy wskazują, że do 2030 roku komputery kwantowe osiągną moc obliczeniową wystarczającą do dekompozycji tych algorytmów w czasie rzeczywistym. Dlatego też, intensywne prace badawczo-rozwojowe koncentrują się na opracowaniu nowych algorytmów kryptograficznych, które będą odporne na ataki kwantowe. Organizacje muszą już teraz rozpocząć proces migracji do tych nowych standardów, aby zapewnić długoterminowe bezpieczeństwo swoich danych i systemów. Inwestycje w technologie kwantowo-odporne stają się nie tylko kwestią bezpieczeństwa, ale także elementem budowania zaufania oraz zapewnienia ciągłości działania w erze post-kwantowej.

Podsumowując, integracja cyberbezpieczeństwa z polityką ESG organizacji to kluczowy krok w budowaniu zaufania i zapewnieniu zrównoważonego rozwoju. Organizacje powinny uwzględniać cyberbezpieczeństwo w swoich strategiach ESG traktując je jako integralną część odpowiedzialności społecznej i ładu korporacyjnego. Budowanie kultury cyberbezpieczeństwa wśród pracowników oraz partnerów biznesowych jest niezbędne do minimalizacji ryzyka ludzkiego błędu, który często jest przyczyną incydentów. Inwestycje w nowoczesne technologie zabezpieczające, takie jak AI, blockchain i systemy analizy zagrożeń w czasie rzeczywistym, pozwalają na skuteczną ochronę przed coraz bardziej zaawansowanymi cyberatakami. Regularne szkolenia i programy uświadamiające podnoszą świadomość zagrożeń i uczą, jak ich unikać. Monitorowanie oraz raportowanie wskaźników cyberbezpieczeństwa w ramach raportów ESG zwiększa transparentność i pozwala na ocenę skuteczności działań podejmowanych przez organizację.

PARTNER MERYTORYCZNY: SOLET

Na zakończenie, warto zauważyć, że wdrożenie i certyfikacja normy ISO 27001 może znacząco ułatwić proces budowania solidnych fundamentów cyberbezpieczeństwa, stanowiąc podstawę dla systemowego zarządzania bezpieczeństwem informacji. Uzyskanie certyfikatu ISO 27001 sygnalizuje, że organizacja poważnie traktuje ochronę danych i systemów, co jest kluczowe w kontekście rosnących wymagań ESG. Co więcej, wdrożenie ISO 27001 efektywnie adresuje również zalecenia dyrektywy NIS2, która nakłada na organizacje z sektorów kluczowych oraz ważnych obowiązek wdrożenia odpowiednich środków cyberbezpieczeństwa. Standard ten, poprzez swoje kompleksowe podejście do zarządzania ryzykiem i ciągłego doskonalenia, zapewnia ramy, które ułatwiają spełnienie wymogów NIS2 dotyczących m.in. zarządzania incydentami, bezpieczeństwa łańcucha dostaw, jak również stosowania środków technicznych i organizacyjnych, dzięki czemu cyberbezpieczeństwo staje się integralnym elementem strategii biznesowej, a nie tylko reakcją na incydenty.

W obliczu tych wyzwań, organizacje coraz częściej poszukują zaufanych partnerów, którzy pomogą im w budowaniu i utrzymaniu skutecznych strategii cyberbezpieczeństwa. Warto w tym kontekście zwrócić uwagę na firmę Solet, która dzięki swojemu doświadczeniu i wiedzy specjalistycznej, może stać się kluczowym sojusznikiem w drodze do zabezpieczenia organizacji. Solet oferuje kompleksowe usługi w zakresie cyberbezpieczeństwa, w tym audyty, wdrożenia, szkolenia oraz wsparcie w uzyskaniu certyfikacji ISO 27001 i zgodności z NIS2. Dzięki indywidualnemu podejściu i zrozumieniu specyficznych potrzeb każdej organizacji, Solet jest w stanie dostarczyć rozwiązania, które nie tylko minimalizują ryzyko cyberataków, ale także wspierają realizację celów ESG. Współpraca z partnerem takim jak Solet pozwala organizacjom skoncentrować się na swojej podstawowej działalności, mając pewność, że ich bezpieczeństwo cyfrowe jest w rękach ekspertów.

CASE STUDY #2

Norsk Hydro – trzy tygodnie bez komputerów

Podobno, gdy telefon dzwoni późno w nocy lub wczesnym rankiem, to dzwoniący nie może mieć dobrej informacji... Tak właśnie było, gdy w marcu 2019 r. o 4 rano rozdzwonił się telefon przy łóżku Hilde Merete Aasheim, prezeski Norsk Hydro. Jej firma jest jednym z największych na świecie producentów aluminium, działa też w branży energii odnawialnej.

Tego dnia wiadomości były naprawdę fatalne: spółka, której dopiero zaczęła szefować, była atakowana.

Atak zaczął się niepostrzeżenie trzy miesiące wcześniej. Zaufany klient przesłał w e-mailu zainfekowany załącznik, który na komputerze pracownika Norsk Hydro uruchomił trojana**.** Kilka dni później to złośliwe oprogramowanie zostało wykryte przez antywirusa, ale było już za późno. **Włamywacze mieli dostęp do wewnętrznych systemów firmy. Gdy w końcu uruchomili ransomware i zaszyfrowali pliki spółki, sparaliżowali pracę 35 tys. osób w 40 państwach.** Żadna z nich nie była w stanie zalogować się do swojego sprzętu.

Tym razem wysokość okupu była uzależniona od tego, jak szybko Norsk Hydro go zapłaci. Im szybciej firma by się na to zdecydowała, tym kwota miała być niższa....

…ale Norwegowie stwierdzili, że nie mają zamiaru płacić ani centa. I była to bardzo dalekosiężna decyzja.

Skoro nie było okupu, to nie było też klucza deszyfrującego. A firmę jednak trzeba prowadzić. Dlatego Norsk Hydro niemal trzy tygodnie działał w trybie offline. Informacje przekazywał na papierze. Notatki dla pracowników zostawiane były na samoprzylepnych karteczkach. Finanse i nadzór nad produkcją prowadzone były w papierowej dokumentacji, jak za dawnych czasów.

Dostęp do komputerów – i to tylko częściowy! – został przywrócony dopiero po trzech tygodniach prac. **Pełne koszty tego ataku szacowane są na 71 mln dol.**

Konsekwencje tego włamania były jednak nie tylko finansowe. Obejmowały też opóźnienia w raportowaniu emisji CO2, co z kolei wpłynęło na relacje firmy z regulatorami i inwestorami. Utrudnienia w dostępie do danych środowiskowych spowodowały czasowe problemy z przestrzeganiem norm ESG, co mogło obniżyć ocenę firmy w rankingach zrównoważonego rozwoju. Ponadto brak terminowych raportów zwiększył ryzyko nałożenia kar regulacyjnych oraz wpłynął na reputację firmy jako lidera odpowiedzialnej produkcji aluminium. Wzrost kosztów operacyjnych dodatkowo osłabił możliwości finansowe firmy na inwestycje w dalsze inicjatywy związane ze zrównoważonym rozwojem.

PARTNER MERYTORYCZNY: GS1 Polska

Waga i jakość danych produktowych – klucz do zaufania i bezpieczeństwa w cyfrowym handlu

W erze zrównoważonego rozwoju dane to nie tylko narzędzie operacyjne, ale fundament odpowiedzialnego i przejrzystego biznesu. Wymogi regulacyjne, takie jak dyrektywa CSRD i standardy ESRS, jasno wskazują na konieczność zarządzania danymi w sposób jakościowy i spójny – szczególnie w kontekście łańcucha dostaw. Jednym z kluczowych obszarów są dane produktowe, które łączą świat konsumenta, producenta i regulatora.

W świecie cyfrowego handlu dane produktowe stały się nieodłącznym elementem doświadczenia zakupowego. Dla konsumenta dokonującego zakupów online, karta produktowa to jedyne „okno" na produkt – nie ma możliwości dotknięcia, powąchania czy fizycznego obejrzenia towaru. Dlatego jakość, kompletność i wiarygodność danych produktowych mają dziś kluczowe znaczenie nie tylko dla decyzji zakupowej, ale również dla bezpieczeństwa konsumenta i zaufania do marki.

Dlaczego dane produktowe są tak ważne?

Dane produktowe to nie tylko opis i zdjęcie – to zestaw informacji, który pozwala konsumentowi:

- **ocenić, czy produkt spełnia jego potrzeby,**
- **upewnić się, że jest bezpieczny w użyciu (np. dla dzieci, alergików, osób z ograniczeniami zdrowotnymi),**
- **zweryfikować jego oryginalność,**
- **porównać go z innymi alternatywami.**

PARTNER MERYTORYCZNY: GS1 Polska

Braki lub nieprawidłowości w tych danych mogą prowadzić do błędnych decyzji, niezadowolenia, a nawet zagrożenia zdrowia.

Podstawowa identyfikacja produktowa – rola numeru GTIN i standardów GS1

Podstawą dobrej jakości danych jest prawidłowa identyfikacja produktu. Kluczową rolę pełni tutaj numer GTIN (Global Trade Item Number) – globalny standard GS1, który jednoznacznie identyfikuje każdy produkt na całym świecie. GTIN działa jak „numer PESEL" dla produktu – pozwala powiązać go z wiarygodnym zestawem danych, niezależnie od tego, w jakim kraju i przez jaki kanał sprzedaży jest oferowany.

GS1 jako organizacja standaryzująca zarządza również Globalnym Rejestrem Produktowym (GS1 Registry Platform) – globalną bazą produktów oznaczonych numerami GTIN, prowadzoną przez właścicieli marek. Umożliwia ona platformom handlowym i konsumentom dostęp do zaufanych, aktualnych danych produktowych bezpośrednio od źródła.

Bezpieczeństwo konsumenta w centrum uwagi

Wysokiej jakości dane mają bezpośredni wpływ na bezpieczeństwo konsumentów:

- W przypadku produktów spożywczych, kosmetyków czy farmaceutyków, kluczowe są informacje o składzie, alergenach, dacie przydatności czy sposobie użycia.
- Konsument powinien mieć dostęp do rzetelnych ostrzeżeń (np. dotyczących wieku dziecka, zawartości substancji drażniących, konieczności konsultacji lekarskiej).
- Dane muszą być zgodne z wymogami prawnymi – brak wymaganych informacji może prowadzić do odpowiedzialności prawnej sprzedawcy lub producenta.

Podróbki i nieautoryzowana sprzedaż – realne zagrożenie

W środowisku online łatwo natrafić na podróbki produktów, które mogą wyglądać autentycznie, ale być w rzeczywistości niebezpieczne lub niespełniające norm. Brak numeru GTIN lub jego niewłaściwe użycie często sygnalizuje nieautoryzowaną dystrybucję. Możliwość weryfikacji produktu w rejestrze GS1 pozwala szybko odróżnić oryginał od podróbki i ograniczyć ich obecność w obiegu.

Spójność danych we wszystkich kanałach sprzedaży

W modelu omnichannel, gdzie produkt jest oferowany równolegle w sklepie online, aplikacji mobilnej, katalogu i punkcie stacjonarnym, spójność danych jest absolutnie kluczowa. Rozbieżności w nazwie, zdjęciach czy składzie wprowadzają konsumenta w błąd i mogą skutkować reklamacjami lub zagrożeniem zdrowotnym. Centralne źródło danych oparte na GTIN i standardach GS1 eliminuje ten problem.

Zgodność z przepisami i ochrona przed sankcjami

W wielu sektorach przepisy nakładają obowiązek przekazywania konkretnych informacji – zarówno w opakowaniu, jak i online. Nieprzestrzeganie tych zasad może skutkować karami finansowymi, wycofaniem produktów z rynku czy kontrolami instytucji nadzorczych. Wysokiej jakości, zgodne z normami dane to nie tylko komfort, ale też zabezpieczenie prawne.

PARTNER MERYTORYCZNY: GS1 Polska

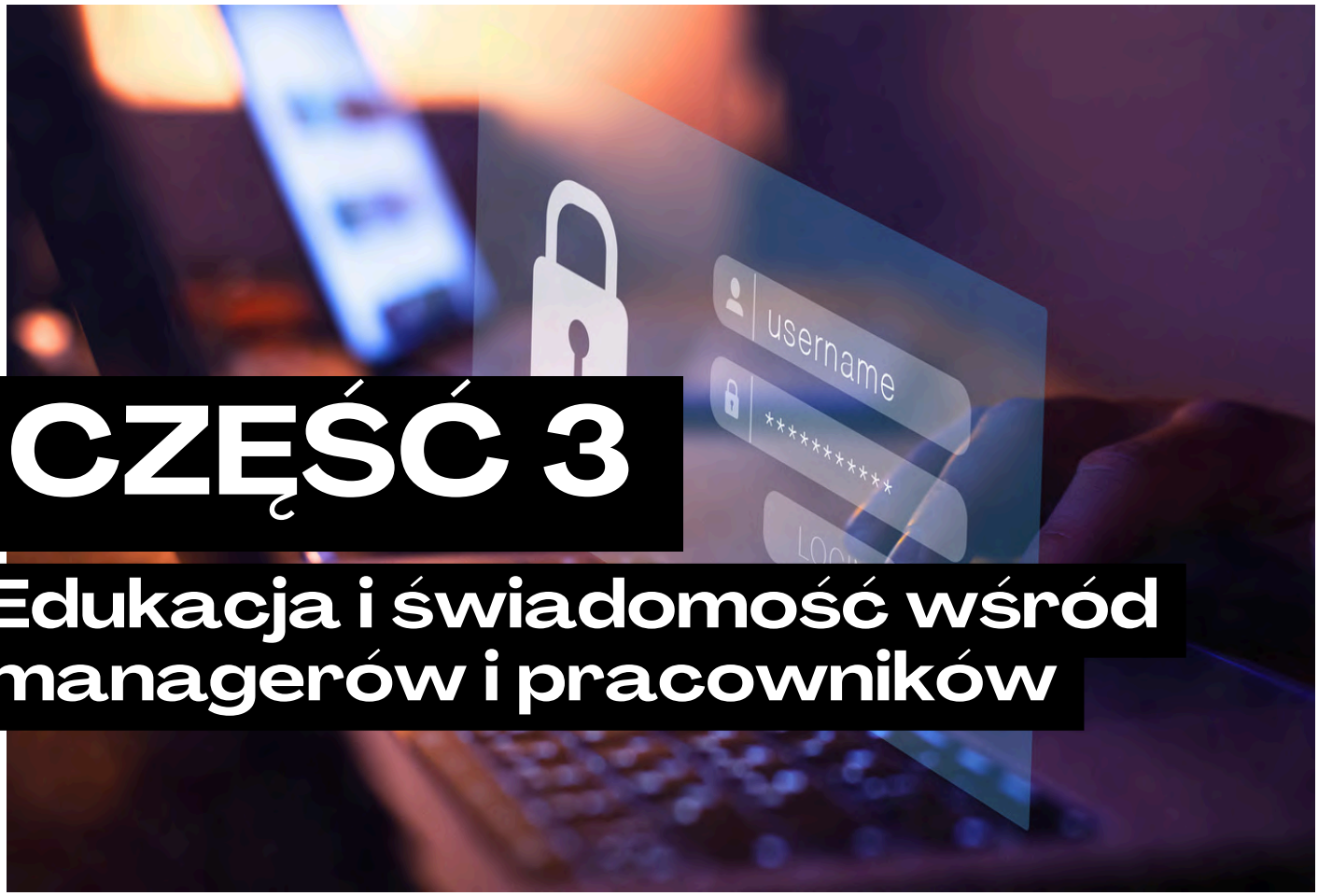
Ochrona reputacji marki i ograniczenie ryzyka

W erze mediów społecznościowych jedna wpadka produktowa może przełożyć się na dużą utratę zaufania. Jeśli konsument kupi produkt, którego opis nie odpowiada rzeczywistości, niezależnie od winy – najczęściej obarcza markę. Dlatego tak ważne jest, by to marka przejmowała kontrolę nad danymi produktowymi, zapewniając ich jakość, spójność i wiarygodność na wszystkich etapach łańcucha sprzedaży.

Dane produktowe to dziś punkt styku konsumenta z produktem, który może przesądzić o zaufaniu, bezpieczeństwie i decyzji zakupowej. Poprawna identyfikacja za pomocą numeru GTIN, zgodność z globalnymi standardami GS1 oraz dostęp do wiarygodnych danych z oficjalnych rejestrów tworzą fundament bezpiecznego i transparentnego rynku.

Inwestycja w jakość danych produktowych to inwestycja w zaufanie konsumentów, reputację marki i długofalowy rozwój biznesu.

Wysokiej jakości dane produktowe to dziś nie tylko element konkurencyjności, ale także warunek spełnienia wymogów raportowania niefinansowego. Ich znaczenie rośnie wraz z rozwojem ram ESG i ESRS, które wymagają mierzalnych, wiarygodnych i audytowalnych danych. Dlatego wdrożenie spójnych standardów danych – takich jak GS1 – staje się strategiczną decyzją każdej firmy, która chce budować zrównoważoną przyszłość.



CZĘŚĆ 3

Edukacja i świadomość wśród managerów i pracowników

Szkolenia z cyberbezpieczeństwa. Jak zwiększyć odporność organizacji poprzez edukację?

Najsłabszym ogniwem zawsze jest człowiek – to chyba najczęściej powtarzana fraza w cyberbezpieczeństwie. Niestety, wciąż prawdziwa. Nie bez powodu najczęstsze ataki rozpracowują odbiorcę maila, a nie zabezpieczenia systemu informatycznego. W końcu łatwiej zagrać na emocjach (poczuciu zagrożenia, konieczności podjęcia natychmiastowej decyzji, chęci uniknięcia dużej dopłaty itd.), niż znaleźć konkretną podatność w systemie.

Z badania Uniwersytetu Stanforda i firmy Tessian zajmującej się oprogramowaniem wynika, że aż 88% włamań spowodowanych jest przez ludzkie błędy. Z kolei wg badania IBM Security ten wskaźnik bliższy jest 95%.

Dlatego nieocenionym sposobem zwiększania cyberbezpieczeństwa w każdej spółce są szkolenia pracowników. Bo atak phishingowy na Spółkę Skarbu Państwa będzie zaprojektowany inaczej niż na sieć sklepów i inaczej niż na organizację finansową.

Każde takie szkolenie powinno uwzględniać specyfikę zespołu i jego pracy i opierać się na przykładach z życia, nie na teorii.

CASE STUDY #3

Pracownik jako najsłabsze ogniwo

Był 2015 r. Pracownicy Banku Centralnego Bangladeszu nie wiedzieli, że od miesięcy byli na celowniku jednej z najbardziej zuchwałych grup cyberprzestępców na świecie.

W końcu się udało – kluczem do sukcesu okazał się mail wysłany do działu HR, w którym znajdowało się CV kandydata do pracy i jego entuzjastyczny list motywacyjny. Nieświadomy zagrożenia pracownik banku otworzył CV i... tym samym wpuścił hakerów do systemu.

A ci mieli jeden cel: wykraść 1 mld dol.

Za skokiem tym stała Grupa Lazarus, powiązana z rządem Korei Północnej, do której należą jedni z najzdolniejszych matematyków i informatyków kraju. Ta grupa do dziś jest postrachem największych organizacji świata – dziś przede wszystkim tych kryptowalutowych.

Ale w 2015 r. zależało im na dolarach. Dlatego, gdy już zyskali dostęp do sieci, metodycznie, komputer po komputerze torowali sobie drogę tak, żeby dotrzeć do terminala, z którego można dokonywać przelewów.

Znaleźli go niemal dokładnie rok po tym, jak pracownik HR otworzył feralnego maila z fałszywym CV. A później sprawy potoczyły się już bardzo szybko.

Hakerzy przemyśleli wszystko (niemal) co do najdrobniejszych szczegółów. Gdy już wiedzieli, jak opróżnić konto, musieli jeszcze wybrać datę i unieszkodliwić drukarkę, która drukowała informację o każdym poleceniu przelewu.

Rezerwa finansowa Banku Centralnego Bangladeszu znajdowała się w Nowym Jorku. Dlatego skok rozpoczął się w czwartek 4 lutego ok. 20 czasu Dhaki (stolicy Bangladeszu). Wtedy wszyscy pracownicy banku wychodzili i rozpoczynali weekend (Bangladesz to państwo muzułmańskie). Tymczasem w USA był czwartek rano, FED działał i przyjmował polecenia przelewów.

Gdy pracownicy banku w Dhace przyszli znów do pracy w niedzielę okazało się, że ktoś kazał wyzerować rezerwy instytucji. Ale w USA nikt nie odbierał telefonu, bo tam weekend wciąż trwał. Pieniądze zostały przelane na Filipiny, gdzie z kolei poniedziałek 8 lutego był świętem, zatem dniem wolnym od pracy. Przestępcy mieli zatem aż cztery dni, żeby przelać pieniądze z konta na konto i się z nimi ulotnić.

Prawie im się udało. Choć z amerykańskiego konta faktycznie wypłynął miliard dolarów, to ostatecznie niektóre późniejsze transakcje udało się zatrzymać.

Ostatecznie Koreańczycy z Północy uciekli z kwotą 81 mln dolarów!

CZĘŚĆ 4

Zabezpieczenia i dobre praktyki

Silne hasła i uwierzytelnianie wieloskładnikowe – Jakie rozwiązania powinny wdrożyć MŚP, by zwiększyć swoje bezpieczeństwo?

- **123456**
- **qwerty123**
- **qwerty1**
- **zaq12wsx**
- **qwerty**
- **123456789.**

Lista najpopularniejszych haseł w Polsce wciąż i niezmiennie nie zaskakuje. Od lat na pierwszym miejscu jest 12345 – hasło, które można złamać w mniej niż sekundę. Qwerty123 też jest oczywistym wyborem. Cała najpopularniejsza pierwsza 20. przygotowana w 2024 r. przez firmę NordPass, tworzącą managera haseł, jest przygnębiająco prosta do złamania.

Dlatego firmy coraz częściej wdrażają środki bezpieczeństwa, które mają poprawić higienę korzystania z internetu przez pracowników:

- blokują słabe hasła
- stosują uwierzytelnianie wieloskładnikowe – czyli do zalogowania się np. do służbowego maila oprócz hasła konieczne jest też wpisanie kodu z SMS lub z aplikacji uwierzytelniającej
- uwierzytelnianie wieloskładnikowe stosowane jest często w usługach finansowych, sieciach VPN, dostępie do chmury firmowej

- stosują zasadę najmniejszych uprawnień – każdy pracownik ma tylko takie dostępy, jakie są mu niezbędne do wykonywania obowiązków.

Amerykański rządowy instytut standaryzacji i technologii w ubiegłym roku zmienił własne wytyczne. Teraz już nie sugeruje, by systemy wymuszały zmianę hasła co miesiąc lub co kwartał. Okazało się bowiem, że częsta zmiana hasła wcale nie poprawiała bezpieczeństwa – wręcz przeciwnie. Użytkownicy zmuszeni do częstej zmiany hasła zmieniali po prostu poprzednie dodając do niego kolejny numer (np. zamiast “hasło2024” pisali “hasło2025”). To pozwalało potencjalnemu przestępcy równie łatwo odgadnąć hasło, sprawdzając po prostu stare hasło z kolejnymi numerami.

Dlatego eksperci odradzają częste zmienianie haseł. Zamiast tego sugerują stosowanie haseł-fraz, które nie mają sensu, ale które łatwo zapamiętać, jak np. "PociągZK0$zalinaDO3łku". Takie hasło przez swoją długość i niestandardowy miks znaków jest trudne do złamania klasycznymi metodami (np. słownikową, która sprawdza najpopularniejsze słowa i hasła, czy brute-force, która sprawdza po kolei setki tysięcy możliwych kombinacji znaków, bo im dłuższe hasło, tym trudniej je złamać tą metodą).

Czy wiesz, że...

W 2024 r. każdej sekundy przeprowadzano 7 tys. prób złamania haseł.

Źródło: Microsoft

Jak stworzyć silne hasło:

- ma co najmniej 12–16 znaków
- powinno zawierać małe i duże litery, cyfrę i znak specjalny
- jedno hasło do jednej usługi
- powinno być łatwe do zapamiętania, np. "M@rowerZebra!92Planeta"
- w przypadku wielu skomplikowanych haseł warto korzystać z managera haseł. Mają go też popularne przeglądarki internetowe.

warto sprawdzić, czy nasze hasło lub e-mail już nie wyciekło. Można to zrobić tu: https://haveibeenpwned.com/

Rybek karmić nie trzeba

Rozświetlone neonami, kiczowate i upojone nadzieją (lub szampanem) – takie właśnie jest Las Vegas, amerykańska stolica hazardu. Jest w nim 150 wielkopowierzchniowych kasyn i aż 300 mniejszych.

W jednym z nich w 2017 r. było akwarium z rybkami. Właściciele postawili na nowoczesność – chcieli czegoś, co będzie ładnie wyglądać i cieszyć oko graczy, a jednocześnie nie będzie wymagać dużo zachodu. Wybrali więc model z dostępem do internetu, który zdalnie sam dostosowywał temperaturę wody, podawał jej zasolenie i sam o odpowiednich porach karmił rybki.

Właśnie takie inteligentne akwarium stało się dla hakerów bramą do najpilniej strzeżonych sekretów kasyna. Po prostu żaden z pracowników kasyna nie pomyślał o tym, że także akwarium trzeba zabezpieczyć przed niepowołanym dostępem.

Liczba ataków na tzw. internet rzeczy, czyli przedmioty codziennego użytku z dostępem do sieci, rośnie z roku na rok.

Wg ostrożnych szacunków urządzeń z internetu rzeczy w 2023 r. było 16,6 mld sztuk. Z danych IBM wynika, że ponad połowa z nich ma krytyczne podatności, które tylko proszą się o włamanie.

To może być termostat, drukarka, kamerka, ekspres do kawy, toster, router, urządzenie medyczne albo zabawka dla dziecka – każde urządzenie z dostępem do sieci daje włamywaczom nową ścieżkę. Taką, o której przeważnie nikt nie pamięta.

Włamywacze, którzy przez niezabezpieczone akwarium dostali się do sieci kasyna nie wyprowadzili z niego pieniędzy. Ukradli za to 10 GB danych i dokładnie spenetrowali całą sieć. Dostali się do danych pracowników, informacji o najczęstszych bywalcach kasyna, poznali też dane finansowe.

Zarządzanie dostępami i uprawnieniami w organizacji

Współczesne organizacje przechowują ogromne ilości danych oraz korzystają z różnych systemów IT, co sprawia, że zarządzanie dostępami i uprawnieniami pracowników staje się kluczowym elementem bezpieczeństwa. Niewłaściwie skonfigurowane dostępy mogą prowadzić do wycieków danych, ataków cybernetycznych i nadużyć. Aby temu zapobiec, można stosować zasady ograniczonego zaufania.

- **Zasada najmniejszych uprawnień** – polega na tym, że każdy pracownik powinien mieć minimalne uprawnienia pozwalające na wykonywanie swoich obowiązków. Jeśli pracuje w dziale ESG, to nie musi mieć dostępu do danych księgowych

- **Zero zaufania** – taką nazwą określa się podejście do pracowników w cyberbezpieczeństwie. Zamiast zakładać, że każdy użytkownik w sieci jest zaufany, organizacja zakłada, że trzeba stale weryfikować tożsamość i uprawnienia osób w systemie.

- **Ciągły audyt** – pracownicy migrują wewnątrz firmy – to zupełnie normalne. Awansują, zmieniają dział albo funkcję w dziale. Jednak należy regularnie przeglądać i rewidować dostępy, żeby pracownicy nie mieli nieużywanych lub nadmiernych uprawnień. Chroni to nie tylko przed cyberwłamaniami, lecz także przed wyciekami danych.

Nadmierne dostępy otwierają pole do wewnętrznych nadużyć. Ale jeszcze bardziej niebezpieczne jest nieodwołanie uprawnień odchodzących pracowników. Jeśli konto takiego pracownika było słabo zabezpieczone, to przestępcy mogą je wykorzystywać do prób wejścia do systemu firmy.

Jeśli spółka nie stosuje podwójnej weryfikacji, to wykradzione hasło może otworzyć podwoje do wszystkich systemów. A jeśli hasło takiej osoby należało też do osoby z dużymi uprawnieniami, to dane firmy są praktycznie niechronione.

CZĘŚĆ 5

Przyszłość cyberbezpieczeństwa w ESG

Kto naprawdę prosi o przelew?

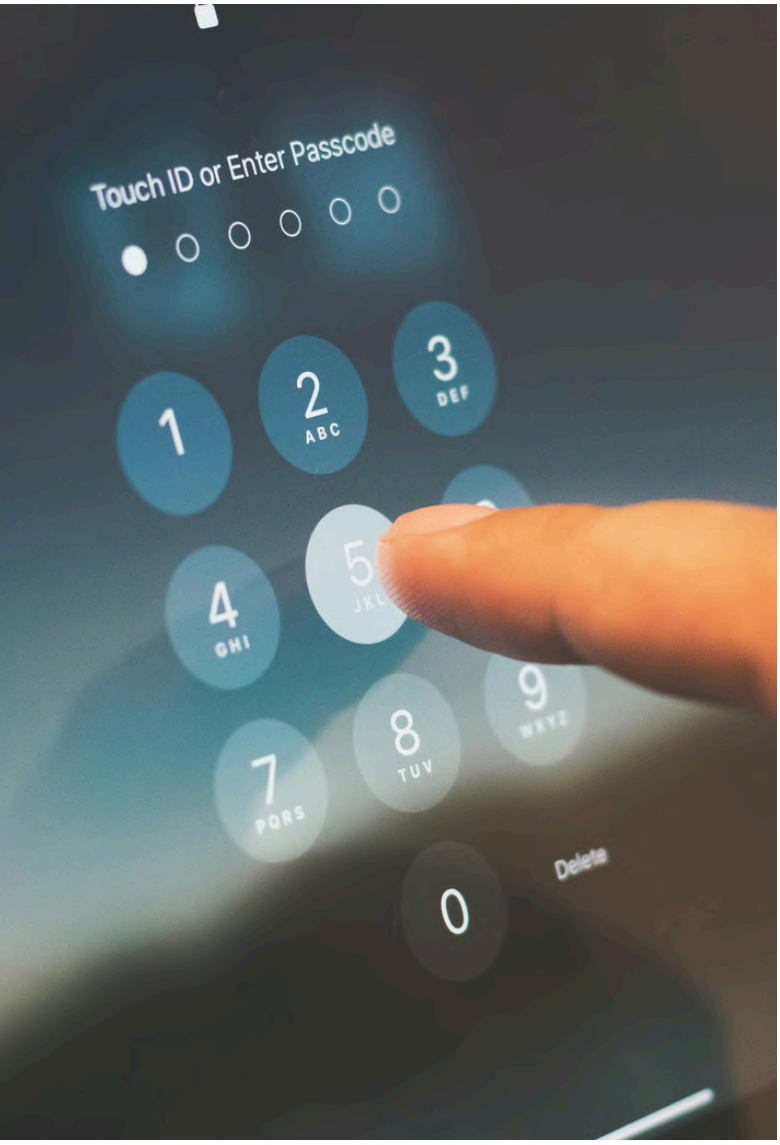
Sztuczna inteligencja ma coraz szersze zastosowania. Poprawia nie tylko produktywność, lecz także służy przestępcom do coraz bardziej wyrafinowanych skoków.

W 2024 r. boleśnie przekonał się o tym pewien mężczyzna z Hongkongu.

Zaczęło się jak zwykle, od fałszywego maila. W wiadomości osoba podająca się za dyrektora finansowego firmy z Wielkiej Brytanii pisała, że trzeba będzie przeprowadzić pewną tajną transakcję. To obudziło jego niepokój.

Ale zwołane kilka chwil później wideokonferencja z całym zespołem ten niepokój rozwiała. Na spotkaniu pojawili się wszyscy członkowie zespołu, mieli włączone kamerki, zadawali pytania, też wyrażali wątpliwości co do “tajnej transakcji”. Ale dyrektor finansowy na wszystkie te wątpliwości miał racjonalną odpowiedź. W końcu wszyscy uznali, że ten przelew nie może być szkodliwy.

Po zakończonym spotkaniu mężczyzna przelał z firmowego konta 200 mln dolarów hongkońskich, czyli ok. 25 mln dol.



Dopiero po rozmowie na żywo ze swoim przełożonym okazało się, że ten mężczyzna był jedyną prawdziwą osobą na wcześniejszej wideokonferencji. Wszyscy pozostali ludzie z jego zespołu zostali wygenerowani przy pomocy AI. Sztuczna inteligencja wykorzystała ich twarz, mimikę i głos do stworzenia perfekcyjnej persony.

Taki skok wymagał dużych nakładów i długiego planowania oraz drobiazgowych przygotowań. Trzeba było rozpoznać potencjalną ofiarę, poznać członków jego zespołu, wejść w posiadanie próbek audio ich głosu oraz nagrań wideo, żeby móc wygenerować odpowiednio realistyczne postaci. Tego typu cierpliwość i duże zasoby pieniężne sugerują, że za tym skokiem stał ktoś, kto miał duży margines błędu (np. państwo lub powiązani z państwem hakerzy) lub grupa, która taki skok robiła już wcześniej.

Nowe wyzwania i technologie zabezpieczające

Przed eksplozją generatywnej AI ze sztucznej inteligencji w cyberbezpieczeństwie korzystały niemal wyłącznie firmy tworzące oprogramowanie antywirusowe. Ich systemy automatycznie przeczesywały bazy danych w poszukiwaniu nowych zagrożeń i były wyczulone na wszelkie odstępstwa od normy, np. zmianę zachowania użytkownika. Jednak dziś AI jest tak samo dostępna dla tych, którzy bronią, jak i tych, którzy atakują.

Sztuczna inteligencja stosowana jest przede wszystkim do automatyzacji ataków, ale tak naprawdę pomaga na każdym etapie oszustw.

- pisze lepsze maile phishingowe niż człowiek. AI może naśladować ton, styl i język rzeczywistej komunikacji zaufanych organizacji
- tworzy polimorficzne złośliwe oprogramowanie – takie, które nieustannie zmienia swój kod, aby uniknąć wykrycia

- tworzy fałszywe strony internetowe i fałszywe recenzje w internecie, żeby przekonać osoby, które próbują zweryfikować, czy dana usługa lub produkt są warte zainteresowania
- za jej pomocą można generować audio i wideo i podszywać się pod prawdziwe osoby

Ale AI gra też po jasnej stronie mocy. Może być wykorzystywana przede wszystkim do wykrywania i analizy anomalii. Na takiej zasadzie działają spółki DataWalk, która współpracuje m.in. z polskim Ministerstwem Finansów czy Ministerstwem Sprawiedliwości USA, Palantir, który udziela wsparcia wywiadowczego Ukrainie czy Nethone, przejęty przez firmę MangoPay. Wszystkie one stawiają na wykrywanie nieprawidłowości w systemach. Mogą one być tak proste i banalne, jak inny sposób wypełniania pola z imieniem i nazwiskiem w formularzu lub chaotyczne ruchy myszką.

To, co dla oka człowieka jest niemal niezauważalne, AI może połączyć w większą całość i wskazać, że dany użytkownik zachowuje się tak dziwnie, że zaraz może próbować oszustwa np. bankowego. Systemy oparte na AI biorą poc uwagę tysiące zmiennych, często np. analizują, czy użytkownik wpisuje swoje dane “z palca”, czy wkleja je w formularz. Pierwsza opcja jest szeroko rozpowszechniona w Europie, podczas gdy Amerykanie typowo wklejają wszystko z notatnika. Jeśli użytkownik łączy się z systemem z Europy, ale zachowuje jak mieszkaniec innej części świata, do tego porusza kursorem myszki, jakby po raz pierwszy lub drugi korzystał z danej usługi, to zmechanizowany system może to wykryć i oflagować, przez co próba transakcji będzie pod zwiększonym nadzorem.

Regulacje i standardy bezpieczeństwa

Wraz ze wzrostem znaczenia zrównoważonego rozwoju i odpowiedzialnego zarządzania, wszystkie firmy w Europie muszą dostosowywać się do coraz bardziej restrykcyjnych regulacji w zakresie bezpieczeństwa danych, zarządzania ryzykiem i przejrzystości operacyjnej.

Dyrektywa CSRD (Corporate Sustainability Reporting Directive)
Została transponowana do polskiego porządku prawnego w grudniu 2024 r. i zobowiązuje większą liczbę firm do raportowania kwestii ESG. Na początku regulacje w zakresie dyrektywy NFRD (poprzedzającej dyr. CSRD) objęły ok. 150 największych spółek w Polsce (szczególnie tych z sektora finansowego). Obecnie (kwiecień 2025) czekamy na ostateczny kształt zmian jaki przyniesie zaproponowany przez Komisję Europejską pakiet uproszczeniowy OMNIBUS, ale docelowo dyrektywa swoim zasięgiem objąć miała ok. 50 tys. spółek w całej Unii Europejskiej.

CSRD zobowiązuje firmy do bardziej szczegółowego raportowania danych zrównoważonego rozwoju i wprowadza stosowanie jednolitych standardów raportowania – ESRS (European Sustainable Reporting Standard). Celem regulacji jest przede wszystkim zwiększenie wiarygodności danych i ograniczenie tzw. greenwashingu.

Dyrektywa NIS2 (Network and Information Security Directive 2)
Dyrektywa NIS2 weszła w życie 16 stycznia 2023 r., a państwa członkowskie Unii Europejskiej, w tym Polska, miały czas do 17 października 2024 r., żeby wdrożyć ją do lokalnego prawa. W naszym kraju to wciąż się nie wydarzyło, ale Ministerstwo Cyfryzacji zapewnia, że wydarzy się to w tym roku.

Dyrektywa NIS2 nakłada nowe obowiązki związane z cyberbezpieczeństwem na spółki działające w UE. Jej celem jest zwiększenie poziomu ochrony sieci i systemów informatycznych w Unii Europejskiej, szczególnie w sektorach kluczowych dla gospodarki i społeczeństwa, czyli w energetyce, transporcie, zdrowiu, bankowości i finansach, usługach cyfrowych, sektorze farmaceutycznym i chemicznym oraz w administracji publicznej.

Firmy z tych obszarów będą musiały wdrożyć politykę zarządzania ryzykiem, obejmującą monitorowanie cyberzagrożeń i incydentów, zarządzanie kryzysowe i reakcję na cyberincydenty, czy testowanie podatności swoich systemów i przeprowadzanie analizy ryzyka.

Firmy będą musiały obowiązkowo informować o naruszeniu bezpieczeństwa ich infrastruktury – wstępne zgłoszenie trzeba będzie zrobić do 24 godz. od wykrycia, pełen raport musi być gotowy w ciągu 72 godz., a na przygotowanie raportu końcowego będzie 30 dni. Kierownictwo firm będzie musiało być bezpośrednio zaangażowane w cyberbezpieczeństwo i może być bezpośrednio pociągnięte do odpowiedzialności, jeśli wykryte zostaną zaniedbania.

Podmiot kluczowy (czyli przede wszystkim duże firmy) za naruszenie wymagań dyrektywy NIS2 może ponieść karę pieniężną w maksymalnej wysokości 10 mln euro. Maksymalna kara, którą można nałożyć na podmiot ważny, wynosi 7 mln euro.

Rozporządzenie DORA (Digital Operational Resilience Act)
Od 17 stycznia 2025 r. stosowane jest Rozporządzenie Parlamentu Europejskiego i Rady (UE) w sprawie operacyjnej odporności cyfrowej sektora finansowego. Jego celem jest zwiększenie operacyjnej odporności cyfrowej podmiotów finansowych oraz uregulowanie świadczenia usług technologii informacyjnych i komunikacyjnych na rynku finansowym.

DORA wprowadza jednolite zasady zarządzania ryzykiem ICT (technologii informacyjno-komunikacyjnych) oraz obowiązki dotyczące cyberbezpieczeństwa, monitorowania zagrożeń i raportowania incydentów.

DORA podobna jest do NIS2, ale odnosi się do bardzo konkretnego sektora: finansowego, czyli banków, ubezpieczycieli, firm inwestycyjnych, dostawców usług płatniczych i fintechów.

Każda firma z tej branży musi już wdrażać strategię zarządzania ryzykiem IT, zgłaszać wszystkie incydenty do regulatora, monitorować bezpieczeństwo u swoich dostawców usług IT i aktywnie monitorować podatność swoich systemów.

Jak się przygotować?

Wszystkie te regulacje wymagają większych nakładów finansowych oraz ludzkich. Ich zapewnienie ma doprowadzić do tego, że kluczowe sektory gospodarki będą lepiej chronione przed cyberzagrożeniami. Jak firmy powinny się przygotować?

- Audyt cyberbezpieczeństwa – Firmy powinny przeprowadzić szczegółową ocenę swoich systemów IT i wdrożyć odpowiednie zabezpieczenia;
- Audyt cyberbezpieczeństwa dostawców – Ocena ryzyka w łańcuchu dostaw i współpraca z bezpiecznymi partnerami IT;
- Wdrożenie strategii zarządzania ryzykiem ICT – Stworzenie polityki obejmującej monitorowanie zagrożeń, testowanie systemów i zarządzanie incydentami;
- Wdrożenie strategii Zero Trust – każda transakcja lub dostęp powinny być weryfikowane
- Monitorowanie dostawców IT – Firmy powinny weryfikować swoich partnerów technologicznych pod kątem zgodności z DORA;
- Testy penetracyjne i analiza podatności – Wdrożenie regularnych testów TLPT, które symulują ataki hakerskie na systemy finansowe;
- Szkolenia dla pracowników i zarządów – Zwiększenie świadomości cyberbezpieczeństwa wśród kadry kierowniczej i zespołów IT;
- Opracowanie planu reagowania na incydenty – Jasne procedury zgłaszania i zarządzania incydentami w wymaganych terminach.

Podsumowanie

Cyberbezpieczeństwo staje się najcenniejszą i najbardziej stabilną dziedziną IT. Liczba cyberataków rośnie z roku na rok. Izraelska firma Check Point twierdzi, że w 2024 r. cyberataków na całym świecie było o 44 proc. więcej, niż w 2023 r. 2023 r. był rekordowy pod względem ataków typu ransomware (dla okupu). Zanotowano ich aż o 46 proc. niż rok wcześniej. A ktoś musi z nimi walczyć.

Każdego dnia dochodzi do setek tysięcy nowych ataków. A najskuteczniejszy wciąż jest phishing – metoda, która rozpracowuje nie zabezpieczenia systemu, lecz odbiorcę e-maila lub SMS. Aż 90 proc. udanych cyberataków zaczyna się od phishingu. A konsekwencje złamania zabezpieczeń firmy są wysokie. W 2023 r. było to średnio 4,45 mln dol. Oprócz utraty pieniędzy trzeba liczyć się też z uszczerbkiem reputacyjnym. A ten naprawić jest dużo trudniej.

Cyberbezpieczeństwo w praktyce

Dobre praktyki firm w zakresie cybersecurity

Dane to nowa energia: cyberbezpieczeństwo jako fundament nowoczesnej energetyki

– rozmowa z Michałem Kasztą, Dyrektorem IT w Ekovoltis

Sektor energetyczny ulega dynamicznej cyfryzacji. Jak Ekovoltis definiuje dziś znaczenie cyberbezpieczeństwa w swojej działalności?
Michał Kaszta: Cyberbezpieczeństwo w sektorze energii nie jest już obszarem zarezerwowanym wyłącznie dla działów IT. To obecnie strategiczny komponent zarządzania ryzykiem operacyjnym i reputacyjnym. W firmie takiej jak Ekovoltis – która działa w modelu zaawansowanego obrotu energią, w tym przede wszystkim energią ze źródeł odnawialnych – dane są kluczowym zasobem. Przetwarzamy informacje o zużyciu, prognozach produkcji, profilach odbiorców, które mają bezpośredni wpływ na decyzje operacyjne i handlowe. Bezpieczeństwo tych danych jest nieodzownym warunkiem stabilności i ciągłości działania.

Jakie rozwiązania w zakresie bezpieczeństwa informacji wdrożyliście jako dobre praktyki?
M.K.: Nasze podejście opiera się na trzech filarach: technologii, świadomości i kulturze organizacyjnej. Inwestujemy w infrastrukturę spełniającą najwyższe standardy – zarówno w obszarze systemów bezpieczeństwa, jak i monitorowania dostępu czy wykrywania anomalii. Jednocześnie prowadzimy stały program szkoleń i edukacji pracowników. Jesteśmy świadomi, że to właśnie użytkownicy systemów są pierwszą linią obrony przed incydentami – dlatego kompetencje cyfrowe traktujemy jako element kultury bezpieczeństwa w organizacji. Cyberbezpieczeństwo nie jest dodatkiem – jest zintegrowane z codziennym funkcjonowaniem wszystkich działów.

Ochrona danych klientów to również temat wrażliwy z punktu widzenia zaufania rynkowego. Jak do tego podchodzicie?
M.K.: Z najwyższą starannością. Dane naszych klientów – zarówno identyfikacyjne, jak i operacyjne – podlegają restrykcyjnej ochronie. Obejmujemy szczególną uwagą dane pomiarowe, informacje handlowe oraz predykcyjne, które mają wpływ na decyzje zakupowe czy kontraktowe. Ewentualne ich naruszenie oznaczałoby nie tylko konsekwencje regulacyjne, ale również utratę zaufania – czego żadna odpowiedzialna firma nie może sobie pozwolić. Dlatego wdrożone przez nas polityki bezpieczeństwa są zgodne z krajowymi i unijnymi standardami, w tym RODO i regulacjami sektorowymi.

Jak cyberbezpieczeństwo wpisuje się w kontekst ESG – w szczególności komponentu „G", czyli ładu korporacyjnego?
M.K.: W ramach ESG coraz wyraźniej widać, że solidne zarządzanie danymi i odporność cyfrowa stanowią element dojrzałego ładu organizacyjnego. Dla Ekovoltis cyberbezpieczeństwo to nie jest tylko techniczne zabezpieczenie infrastruktury – to również wyraz odpowiedzialności za transparentność działania, stabilność operacyjną i poszanowanie dla interesariuszy. To przekłada się bezpośrednio na naszą wiarygodność – zarówno wobec klientów, jak i partnerów rynkowych czy instytucji nadzorczych.

Człowiek najważniejszym ogniwem bezpieczeństwa

Stereotypowo w działach wsparcia IT funkcjonuje przekonanie, że źródło większości problemów tkwi między krzesłem a komputerem, a „włącz – wyłącz" jest remedium na 90% problemów ze sprzętem.

Zważywszy, że nawet najlepsze zapory, systemy detekcji i reakcji, zespół reagowania 24/7 nie pomogą na użytkownika niefrasobliwie żonglującego poufnymi danymi, należy oddać tej teorii odrobinę racji. W istocie to człowiek jest najważniejszym ogniwem w łańcuchu bezpieczeństwa. Dlatego w Respect Energy duży nacisk kładziemy na edukację pracowników związaną z cybersecurity,

W lutym, z okazji Dnia Bezpiecznego Internetu, zorganizowaliśmy zintensyfikowane akcje uświadamiające, których ważnym elementem były webinary:

- „Krajobraz cyberzagrożeń: Bezpieczeństwo wczoraj i jutro"
- "Bezpieczne hasła i hasłowość w AI, czyli dlaczego 100 haseł jest wygodniejsze niż 1 a używanie AI bywa nierozsądne"
- "Cyber-pułapki w social media: Phishing, deepfake, kradzież tożsamości a Twoje życie w sieci"
- "A czy Ty dasz się łatwo złapać na phishing? Czyli o tym jak cyberprzestępcy łowią swoje ofiary"

Każde z tych autorskich szkoleń było prowadzone przez naszych ekspertów, a ich nagrania zostały później udostępnione kolegom i koleżankom z pracy, którzy nie mogli wziąć udziału w spotkaniach na żywo.

Start kampanii informacyjnej był też elementem promocji naszego wewnętrznego bloga poświęconego cyberbezpieczeństwu, który stanowi stałe źródło wiedzy na temat zagrożeń i metod ich wykrywania.

Kampanie tego typu spotykają się z ciepłym przyjęciem i są kluczowym elementem wdrażania strategii cyberbezpieczeństwa. Aby je uatrakcyjnić i zwiększyć ich skuteczność warto zastosować parę hacków:

- forma ma znaczenie – krótkie nagrania, które można puścić sobie w tle poświęcone punktowo jednemu zagadnieniu sprawdzają się znacznie lepiej niż długie i komplementarne bloki szkoleniowe,
- podobna reguła tyczy się artykułów, krótkie i zwięzłe, jeśli masz możliwość zrobić infografikę – nie wahaj się, ta forma wiedzy jest najłatwiejsza w przyswajaniu,
- wskazuj na zagrożenia codziennego życia, jeśli włamania to na social media, jeśli utrata pieniędzy – to z własnego konta, takie analogie i przykłady trafiają do ludzi znacznie bardziej niż utrata nawet milionów przez firmę zza oceanu,
- proś o feedback, pytaj ludzi jakie materiały czy kwestie ich najbardziej interesują.

Jeśli do tego uda Ci się utrzymać regularność publikacji - brawo! Efekty będą niesamowite.

Błażej Szymczak, Security Director, Respect Energy Holding S.A.

Rozwój talentów i budowanie odporności cyfrowej DEKRA

Zarząd DEKRA Certification wierzy, że wspieranie młodych talentów to nie koszt – to inwestycja. Dlatego w środowisku DEKRA umożliwiono przeprowadzenie badania, które posłużyło rozwojowi naukowemu pracowników i realnie wsparło strategiczny cel DEKRA: wzmacnianie odporności cyfrowej organizacji.

Symulowany atak phishingowy, zrealizowany w kontrolowanych warunkach, miał na celu podniesienie świadomości pracowników oraz przygotowanie ich na realne zagrożenie ze strony cyberprzestępców. Projekt odegrał znaczącą rolę w rozwijaniu kultury bezpieczeństwa DEKRA, opartej na świadomości.

Ataki phishingowe często pełnią rolę wstępnego wektora ataku, inicjując bardziej zaawansowane i niebezpieczne działania cyberprzestępców. Napastnicy wykorzystują techniki socjotechniczne, aby manipulować ofiarami i wykorzystać istniejące podatności. W badaniu wykorzystano m.in. agresywny termin wykonania zadania czy groźby utraty dostępu do systemów.

Badanie przyniosło wiele konstruktywnych wniosków, m.in. że warto inwestować w cykliczne działania edukacyjne z cyberbezpieczeństwa, wzmacniać kulturę zgłaszania incydentów czy doskonalić działania prewencyjne. Pracownicy dzięki nauce poprzez praktykę w środowisku bezpiecznym do popełniania błędów, rozwijają kompetencje cyfrowe i zwiększają świadomość zagrożeń cyfrowych, technik socjotechnicznych czy poczucie odpowiedzialności za bezpieczeństwo informacji.

DEKRA uważa, że regularne przeprowadzanie symulacji phishingowych powinno stanowić element strategii bezpieczeństwa organizacji i być włączone do programu ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji. Pracownicy powinni być traktowani nie tylko jako podatność ale przede wszystkim jako aktywną linię obrony. Angażowanie pracowników w tego typu przedsięwzięcia daje możliwość rozwoju młodych talentów i doskonalenia całej organizacji.

Korzyści płynące z symulowanych ataków phishingowych:

1. Wczesne wykrywanie podatności ludzkich.
2. Wzrost świadomości pracowników w zakresie cyberbezpieczeństwa.
3. Wsparcie systemu zarządzania bezpieczeństwem informacji.
4. Szybsza reakcja pracowników, mniejsze skutki ataku i większa odporność całej organizacji.
5. Spełnienie wymogów regulacji i standardów, takich jak ISO/IEC 27001:2022 oraz NIS 2, które zalecają aktywne zarządzanie ryzykiem ludzkim.
6. Tworzenie kultury bezpieczeństwa.
7. Bezpieczne środowisko do nauki i popełniania błędów w kontrolowanych warunkach.

Cyberbezpieczeństwo – dobre praktyki firmy AdiFeed

Firma AdiFeed, działająca w ramach sektora MŚP stawia na najskuteczniejsze rozwiązania dotyczące cyberbezpieczeństwa. Nasze przedsiębiorstwo przechowuje wiele cennych danych, zarówno własnych, jak i swoich klientów, gdzie utrata tych danych może poważnie zaszkodzić reputacji firmy oraz narazić ją na straty prawne oraz finansowe. Stosowane przez nas dobre praktyki cyberbezpieczeństwa zapewniają, że firma działa w sposób ciągły i nieprzerwany.

W związku z powyższym chcielibyśmy zaprezentować nasze rozwiązania wspierane przez specjalistów IT:

Testy phishingowe – Regularnie przeprowadzamy testy phishingowe dla pracowników, co pozwala na podnoszenie ich świadomości w zakresie zagrożeń oraz wzmacnia bezpieczeństwo w organizacji.

Bezpieczne połączenia VPN – Pracownicy łączący się zdalnie z naszą firmową siecią korzystają z szyfrowanych połączeń VPN, co zabezpiecza dane przesyłane w Internecie i minimalizuje ryzyko ich przechwycenia przez osoby trzecie.

Logowanie wieloetapowe (MFA) – Wdrożyliśmy wieloetapowe logowanie, dodatkowe weryfikacje, takie jak kod SMS lub z aplikacji uwierzytelniającej, znacząco utrudniają nieautoryzowany dostęp do systemów firmy.

Oprogramowanie antywirusowe – Na firmowych urządzeniach zainstalowaliśmy oprogramowanie antywirusowe, które zapewnia ochronę przed wirusami, ransomware, malware oraz innymi zagrożeniami. Dodatkowo system blokuje dostęp do niebezpiecznych stron internetowych, zapobiegając atakom typu phishing i innym formom cyberzagrożeń.

Regularne aktualizacje i łatki bezpieczeństwa – Systemy oraz oprogramowanie są regularnie aktualizowane, co pozwala na eliminację luk w zabezpieczeniach i zapobieganie atakom, które mogą wykorzystać nie aktualizowane oprogramowanie.

Backup i odzyskiwanie danych – Tworzymy regularne kopie zapasowe kluczowych systemów i danych. Procedury odzyskiwania danych są testowane, aby zapewnić ich dostępność i integralność w przypadku awarii lub ataku.

Firewall – Korzystamy z zaawansowanych firewalli, które filtrują ruch sieciowy, blokują nieautoryzowane połączenia i chronią przed cyberatakami.

Oprócz szeregu rozwiązań czysto technicznych stosujemy także cykliczne szkolenia dla naszych pracowników. Szkolenia te mają na celu zwiększyć świadomość i odpowiedzialność pracowników, aby uniknąć prostych błędów, które mogą prowadzić do poważnych incydentów.

Odpowiedzialni w digitalizacji

„ESG nie jest dla nas tylko raportowaniem. ESG nadaje kierunek naszym działaniom zarówno w digitalizacji procesów jak i ochronie przetwarzanych danych.”
Łukasz Mieszkalski, dyrektor IT w ROBYG i Vantage Davelopment.

ROBYG, jako jeden z największych deweloperów w Polsce, realizuje kompleksowe projekty mieszkaniowe – od identyfikacji potencjalnych inwestycji, przez cały proces ich rozwoju i realizacji. Firma rozwija mieszkania na sprzedaż oraz zarządza budową projektów przeznaczonych na wynajem długoterminowy w ramach grupy TAG Immobilien AG. Projekty te są zarządzane przez Vantage Development.

Bycie liderem rynku to nie tylko odpowiedzialność za zrównoważony rozwój, ale również za ochronę danych i bezpieczeństwo cyfrowe na każdym etapie działalności. Cyfryzacja procesów, będąca kluczowym elementem strategii, wspiera efektywność operacyjną, przyczynia się do redukcji śladu węglowego i gwarantuje najwyższy poziom zabezpieczeń we wszystkich obszarach naszej działalności.

Zarówno w ROBYG, jak i Vantage, przykładamy ogromną wagę do cyberbezpieczeństwa, traktując je jako istotny element zrównoważonego rozwoju. Regularnie przeprowadzamy testy bezpieczeństwa, audyty wewnętrzne i zewnętrzne, a także testy penetracyjne aplikacji. Dbamy o jakość kopii zapasowych zgodnie z określonymi politykami, a co najważniejsze – przeprowadzamy regularne testy odtworzeniowe. Zapewnienie ciągłości działania firmy oraz ochrona danych są dla nas absolutnym priorytetem – kluczowe znaczenie ma odporność na ataki cybernetyczne oraz szybkość reakcji i działania.

Regularnie prowadzimy szkolenia z zakresu cyberbezpieczeństwa oraz kampanie phishingowe, aby zwiększać świadomość pracowników w zakresie zagrożeń. W dzisiejszych czasach szczególnie istotne jest budowanie odporności na ataki z wykorzystaniem technologii deepfake, ponieważ silniki AI umożliwiają tworzenie coraz bardziej realistycznych obrazów, wykorzystywanych w cyberatakach.

Inwestujemy w nowoczesne technologie, dbając jednocześnie o ich etyczne wykorzystanie oraz bezpieczeństwo danych naszych klientów. Rozwijamy nasze systemy i rozwiązania cyfrowe, aby usprawnić komunikację i efektywność obsługi.

ROBYG wdraża nowy system CRM dla sprzedaży mieszkań, integrując procesy w ramach jednej platformy. Nowy portal oraz aplikacja mobilna usprawnią obsługę posprzedażową, ograniczając emisje i zużycie papieru. Planowane jest również wdrożenie sztucznej inteligencji w przyszłych procesach.

Vantage Rent rozwija swój system CRM (Properto Rent 2.0), udoskonalając portal EBOK i aplikację mobilną. Narzędzia te umożliwią najemcom monitorowanie zużycia mediów i efektywniejsze zarządzanie kosztami. Dla nas oznaczają one cyfrową obsługę przekazań i odbiorów mieszkań, co zmniejsza zużycie papieru i wspiera gospodarkę obiegu zamkniętego.

DZP
więcej niż prawo

Cyberodporność łańcucha dostaw a ESG

Rosnące wymagania regulacyjne oraz zagrożenia cyfrowe sprawiają, że organizacje muszą patrzeć na cyberbezpieczeństwo w szerszym kontekście. Dyrektywa NIS 2, której implementacja w Polsce nastąpi poprzez nowelizację ustawy o krajowym systemie cyberbezpieczeństwa, rozszerza zakres stosowania przepisów dotyczących cyberbezpieczeństwa na nowe sektory gospodarki, a także nakłada na przedsiębiorców wymogi w zakresie wdrożenia środków zarządzania ryzykiem, co obejmuje też bezpieczeństwo łańcucha dostaw.

Zgodnie z dyrektywą NIS 2, podmioty kluczowe i ważne będą zobowiązane do oceny i zarządzania ryzykiem w cyberbezpieczeństwie również w relacjach z dostawcami. To istotne, gdyż wiele incydentów wynika z podatności w produktach i usługach stron trzecich. Dlatego podmioty kluczowe i ważne powinny uwzględniać jakość oraz odporność tych rozwiązań i oceniać, czy ich dostawcy spełniają minimalne standardy bezpieczeństwa. Dla dostawców ubiegających się o zamówienia u podmiotów kluczowych i ważnych oznacza to konieczność spełnienia określonych wymagań w zakresie cyberbezpieczeństwa – zarówno technologicznych, jak i organizacyjnych. Mogą być zobowiązani do przedstawienia dowodów na stosowanie odpowiednich zabezpieczeń, procedur zarządzania ryzykiem oraz reagowania na incydenty. Może to wiązać się z koniecznością posiadania certyfikatów, udziału w audytach oraz dostarczania dokumentacji potwierdzającej zgodność z minimalnymi standardami bezpieczeństwa. Niespełnienie tych wymogów może nawet skutkować wykluczeniem z postępowań przetargowych.

To podejście idealnie wpisuje się w pojęcie odpowiedzialności społecznej firm. W ramach strategii ESG, cyberodporność staje się elementem zarówno ładu korporacyjnego (G), jak i odpowiedzialności wobec społeczeństwa (S). Organizacje, które potrafią wykazać, że dbają o bezpieczeństwo danych, usług i informacji – również w całym łańcuchu dostaw – budują zaufanie i zwiększają swoją wiarygodność.

Z perspektywy ESG, cyberodporność łańcucha dostaw to nie tylko obowiązek, ale też szansa. Może zapewnić przewagę konkurencyjną i stanowić element raportowania niefinansowego. Coraz więcej organizacji uwzględnia cyberbezpieczeństwo w swoich ocenach dostawców, traktując je na równi z kwestiami środowiskowymi czy społecznymi. Dyrektywa NIS 2 wprowadza zatem nowe wymagania w zakresie zabezpieczenia całego łańcucha dostaw, które wzmacnia podejście ESG.

AUTORKI:

- r.pr. dr Aleksandra Auleytner, Szef Praktyki IP&TMT
- r.pr. Karolina Kulikowska-Gruszecka, Senior Associate, Praktyka IP&TMT

SOLET

Systemowe wsparcie procesów zrównoważonego rozwoju w oparciu o IBM® Envizi™

TOP 8 NARZĘDZIA RAPORTOWANIA ESG 2024 EDITION

ISO 20243
ISO 27018
ISO 27001
ISO 27701
CSA STAR

ZADBAJ O BEZPIECZEŃSTWO PROCESÓW ESG

- Stosuj uwierzytelnianie dwuskładnikowe (MFA)
- Zabezpieczaj fizyczny dostęp do infrastruktury IT
- Przeprowadzaj audyty cyberbezpieczeństwa w celu identyfikacji i ograniczania luk w zabezpieczeniach
- Regularnie aktualizuj plan reagowania na incydenty w przypadku potencjalnych ataków cybernetycznych
- Ograniczaj dostęp do zasobów na podstawie przypisanych ról, zgodnie z zasadą najmniejszych uprawnień
- Edukuj personel w zakresie rozpoznawania phishingu i innych zagrożeń cyberbezpieczeństwa
- Regularnie twórz kopie zapasowe swoich danych i testuj ich odtwarzanie
- Używaj narzędzi zapobiegających nieautoryzowanemu transferowi danych
- Szyfruj dane, chroń dane wrażliwe
- Aktualizuj na bieżąco wszystkie systemy i aplikacje

Polecane narzędzia IBM wspierające bezpieczeństwo organizacji:

- IBM QRadar SIEM
- IBM SOAR
- IBM Verify Identity Protection
- IBM Verify Governance
- Hashicorp Vault
- IBM Verify Privilege Vault
- IBM Verify Access
- IBM MaaS360

www.solet.pl

IBM Gold Partner

Dobre praktyki w zakresie cyberbezpieczeństwa i ochrony danych w Grupie Pekabex

W erze cyfryzacji, gdy organizacje przechowują i przetwarzają ogromne ilości danych, cyberbezpieczeństwo stało się fundamentem odpowiedzialności społecznej. Aspekt ten zyskuje na znaczeniu w ramach strategii ESG Grupy Pekabex, której integralną częścią jest dbanie o bezpieczeństwo cyfrowe i zgodność z przepisami dotyczącymi ochrony danych.

W naszej organizacji kładziemy szczególny nacisk na edukację pracowników w zakresie cyberbezpieczeństwa. Systematyczne przypomnienia o zagrożeniach oraz regularne szkolenia to fundament naszej strategii ochrony danych. Nawet najlepsze systemy zabezpieczeń nie wystarczą, jeśli pracownicy nie będą świadomi ryzyka.

Dział IT Pekabex przeprowadza regularne szkolenia, obejmujące nie tylko podstawowe zasady bezpieczeństwa, ale także szczegółowe scenariusze zagrożeń. Pracownicy są szkoleni w zakresie rozpoznawania prób phishingu oraz bezpiecznego korzystania z systemów IT. Prowadzimy również testy symulujące rzeczywiste ataki, co pozwala na weryfikację gotowości zespołów do reagowania na incydenty.

Kolejnym kluczowym elementem strategii jest przeprowadzanie regularnych audytów bezpieczeństwa oraz testów penetracyjnych. Działania te pozwalają na bieżąco oceniać skuteczność wdrożonych rozwiązań oraz wykrywać luki w zabezpieczeniach. W tym celu wykorzystujemy narzędzia do symulacji ataków, które pomagają nam sprawdzić, jak organizacja reaguje w sytuacjach kryzysowych.

W ramach działań ESG bezpieczeństwo danych postrzegamy w Grupie Pekabex jako element odpowiedzialności organizacji wobec pracowników, klientów oraz całego społeczeństwa. Transparentność działań w zakresie ochrony danych buduje zaufanie wśród interesariuszy.

W dzisiejszym świecie, gdzie dane stały się jednym z najcenniejszych zasobów, odpowiednia ochrona przed zagrożeniami cyfrowymi jest niezbędna dla zapewnienia długoterminowego sukcesu organizacji. Dobre praktyki z zakresu cyberbezpieczeństwa, takie jak systematyczne szkolenia, audyty czy wdrażanie nowoczesnych rozwiązań IT, stanowią podstawę skutecznego zarządzania ryzykiem. W kontekście ESG, dbanie o bezpieczeństwo danych to także wyraz społecznej odpowiedzialności firmy, która nie tylko przestrzega przepisów, ale również dba o zaufanie i dobro swoich interesariuszy.

EnergySolution

Bezpieczny smart metering w praktyce ESG

Smart metering to system składający się z liczników cyfrowych, koncentratorów, platform komunikacyjnych i aplikacji analitycznych. Kluczową cechą jest ciągły pomiar, przesył i analiza danych o zużyciu mediów – bez potrzeby manualnych odczytów. Przedsiębiorstwa zyskują w ten sposób precyzyjne profile energetyczne, co pozwala optymalizować zużycie, ograniczać emisje i koszty.

W kontekście raportowania ESG smart metering to narzędzie niezbędne. Umożliwia wyliczenie wskaźników emisyjnych (np. GHG Scope 2), dokumentowanie oszczędności oraz monitorowanie KPI środowiskowych. Warunkiem skuteczności jest jednak niezawodność i bezpieczeństwo danych. Bez ich integralności system ESG traci wiarygodność. Stąd rola cyberbezpieczeństwa jako fundamentu całej infrastruktury.

Techniczne dobre praktyki w ochronie systemów smart meteringu:

1. Segmentacja warstw OT/IT. Stosuj VLAN-y i strefy DMZ by oddzielić sieć urządzeń pomiarowych od systemów administracyjnych i biurowych.

2. Szyfrowanie transmisji danych. Wykorzystuj bezpieczne protokoły (TLS 1.3, IPsec, MQTTs) na każdym etapie przesyłu, by chronić poufność danych. W celu ochrony integralności zastosować inne metody, jak np. funkcja skrótu (hash) czy HMAC.

3 Autoryzacja i MFA. Stosuj kontrolę dostępu opartą na rolach (RBAC), wieloskładnikowe uwierzytelnianie (MFA) oraz monitoring aktywności (SIEM, SOC).

4. Detekcja i reakcja na incydenty (EDR/NDR). Zastosuj systemy wczesnego wykrywania zagrożeń (EDR, NDR), które identyfikują manipulacje, ataki DoS i inne anomalie w czasie rzeczywistym.

5. Zgodność z normami i regulacjami. System powinien spełniać wymagania ISO/IEC 27001, NIST CSF, dyrektywy NIS2 oraz RODO – dane pomiarowe mogą zawierać informacje osobowe.
6. Zapewnić kopię bezpieczeństwa, możliwość szybkiego odtwarzania środowiska po awarii oraz architekturę HA.

Bezpieczne wdrożenie smart meteringu to nie tylko krok w kierunku cyfryzacji, ale również gwarancja jakości danych w raportach ESG, odporności operacyjnej i zgodności z regulacjami. Firmy, które inwestują w nowoczesne, a zarazem bezpieczne technologie pomiarowe, zyskują przewagę w raportowaniu i realnie wspierają transformację energetyczną.

W dobie cyfrowej transformacji, kiedy przedsiębiorstwa na całym świecie coraz bardziej polegają na technologiach informacyjnych, zagrożenia cybernetyczne stają się jednym z kluczowych wyzwań dla firm każdej wielkości. Skuteczna ochrona przed cyberatakami wymaga nie tylko zaawansowanych technologii, ale także strategicznego podejścia opartego na kompleksowej ocenie ryzyka.

Dun & Bradstreet, jako lider w dziedzinie zarządzania ryzykiem, podkreśla znaczenie globalnych ocen ryzyka w planach cyberbezpieczeństwa. Zrozumienie i analiza ryzyka na poziomie międzynarodowym pozwala firmom lepiej przygotować się na potencjalne zagrożenia oraz skutecznie nimi zarządzać. Globalna perspektywa umożliwia identyfikację słabych punktów w łańcuchu dostaw, ocenę podatności na ataki w różnych regionach oraz dostosowanie strategii ochrony do specyfiki lokalnych rynków.

W kontekście zarządzania ryzykiem cybernetycznym, kluczowe jest wdrożenie kompleksowych planów, które uwzględniają zarówno aspekty technologiczne, jak i organizacyjne. Skuteczne zarządzanie ryzykiem wymaga ciągłego monitorowania zagrożeń, regularnych audytów bezpieczeństwa oraz edukacji pracowników w zakresie najlepszych praktyk. Firmy powinny także inwestować w nowoczesne rozwiązania technologiczne, takie jak systemy wykrywania i zapobiegania włamaniom, aby minimalizować ryzyko naruszeń danych.

Ochrona przed cyberzagrożeniami to nie tylko kwestia technologii, ale także kultury organizacyjnej. Budowanie świadomości wśród pracowników na temat potencjalnych zagrożeń oraz promowanie odpowiedzialnych zachowań w sieci są nieodzownymi elementami skutecznej strategii bezpieczeństwa. Regularne szkolenia, symulacje ataków oraz jasne procedury postępowania w przypadku incydentów mogą znacząco zwiększyć odporność organizacji na cyberataki.

W obliczu rosnącej liczby i złożoności zagrożeń cybernetycznych, przedsiębiorstwa muszą przyjąć proaktywne podejście do zarządzania ryzykiem. Integracja globalnych ocen ryzyka z kompleksowymi planami cyberbezpieczeństwa, inwestycja w nowoczesne technologie oraz budowanie kultury bezpieczeństwa w organizacji to kluczowe kroki na drodze do ochrony przed cyberzagrożeniami. Dzięki temu firmy mogą nie tylko zabezpieczyć swoje dane i zasoby, ale także zyskać przewagę konkurencyjną na rynku, budując zaufanie klientów i partnerów biznesowych.

Justyna Jarzębowska
Marketing Manager Poland, Dun&Bradstreet

Omega Group – odporność na zagrożenia cyfrowe

Omega Group stale inwestuje we wzmacnianie odporności organizacyjnej na cyberzagrożenia. W obliczu dynamicznych zmian technologicznych i coraz bardziej zaawansowanych ataków koncentrujemy się na implementacji skutecznych mechanizmów prewencyjnych i reaktywnych.

Kluczowe elementy strategii bezpieczeństwa
Jednym z filarów naszej strategii jest model Zero Trust (ZT EITTM), oparty na zasadzie "nieufności domyślnej" – żadna osoba ani urządzenie nie są automatycznie zaufane, co pozwala na maksymalne zabezpieczenie dostępu do zasobów.

- **Zastosowane rozwiązania Ochrona sieci bezprzewodowej (Wireless Iron DomeTM)** – zapewnia kontrolę i ochronę Wi-Fi, kluczową w środowiskach komercyjnych i instytucjonalnych.
- **Ochrona przed atakami zewnętrznymi** – wykorzystujemy Scrubbing Center A10 Networks do zapobiegania i minimalizacji skutków ataków DDoS.
- **Zabezpieczenie danych** – stosujemy backupy krytycznych zasobów, szyfrowanie transmisji oraz mechanizmy kontroli dostępu wspierane sztuczną inteligencją.
- **Zdalny dostęp przez VPN** – dostęp do infrastruktury możliwy jest wyłącznie przez tunele VPN, co zabezpiecza dane przed przechwyceniem
- **Rozwój kompetencji cyfrowych –** szkolenia i kampanie edukacyjne zwiększają świadomość cyberbezpieczeństwa.

Zgodność z regulacjami
Nasze rozwiązania są zgodne z normami branżowymi i regulacyjnymi, wzmacniając zaufanie interesariuszy.

Rekomendowane zasady cyberbezpieczeństwa
- **Zarządzanie hasłami** – stosowanie silnych, unikatowych haseł, regularna zmiana.
- **Menadżery haseł** – certyfikowane narzędzia eliminują ryzyko ujawnienia danych.
- **Zabezpieczenia sieciowe (firewall)** – filtrowanie ruchu ogranicza nieautoryzowany dostęp.
- **Ocena ryzyka** – okresowe analizy identyfikują słabe punkty i aktualizują zabezpieczenia.
- **Kopie zapasowe** – regularny backup danych zapewnia ciągłość działania.
- **Szyfrowanie danych** – chroni wrażliwe informacje przed przechwyceniem i manipulacją.

Osiągnięte wyniki
Nasze działania zwiększają bezpieczeństwo infrastruktury i zasobów, budując jednocześnie zaufanie interesariuszy i podnosząc dojrzałość organizacji w zarządzaniu cyberzagrożeniami.

www.polskiestowarzyszenieesg.pl