CIONET DIGITAL EXCELLENCE

SECURITY EXCELLENCE RAPORT

RODO i inne przepisy – nowa rzeczywistość cybesecurity?
Polityka bezpieczeństwa – aktywna czy reaktywna?
Technologia, specjaliści, zagrożenia – jak wygląda agenda CSO?
Świadomy pracownik – fakt czy utopia?

SECURITY EXCELLENCE RAPORT

Program Security Excellence od początku, z sukcesem, tworzymy wspólnie z Wami. Razem z najwybitniejszymi znawcami tematu, w bardziej i mniej sformalizowany sposób, rozmawiamy o cyberbezpieczeństwie, dzielimy się doświadczeniami i najlepszymi praktykami podczas regionalnych spotkań w całej Polsce. Postanowiliśmy pójść o krok dalej i skatalogować nasze wspólne refleksje – przeprowadziliśmy ankietę wśród menedżerów tworzących strategię bezpieczeństwa w swoich organizacjach.

Z przyjemnością przedstawiamy wyniki badania, w którym pytaliśmy o najważniejsze zagrożenia, sposoby zapanowania nad nimi, obawy i plany związane z cyberbezpieczeństwem. O komentarze do wyników poprosiliśmy ekspertów w tej dziedzinie, którzy wnoszą do naszego opracowania swoją unikalną wiedzę i doświadczenie. Skoncentrowaliśmy się na trzech obszarach, zderzając zagadnienie cyberbezpieczeństwa z regulacjami, technologią i czynnikiem ludzkim.

Raport pokazuje, że temat cybersecurity jeszcze długo pozostanie numerem jeden w większości przedsiębiorstw – rośnie skala wyzwań, m.in. w związku z nowymi regulacjami prawnymi, ale liczba specjalistów w firmach pozostaje bez zmian. Tym ważniejsze jest więc budowanie świadomości, edukacja w tej dziedzinie i wymiana spostrzeżeń.

Zapraszamy do lektury!

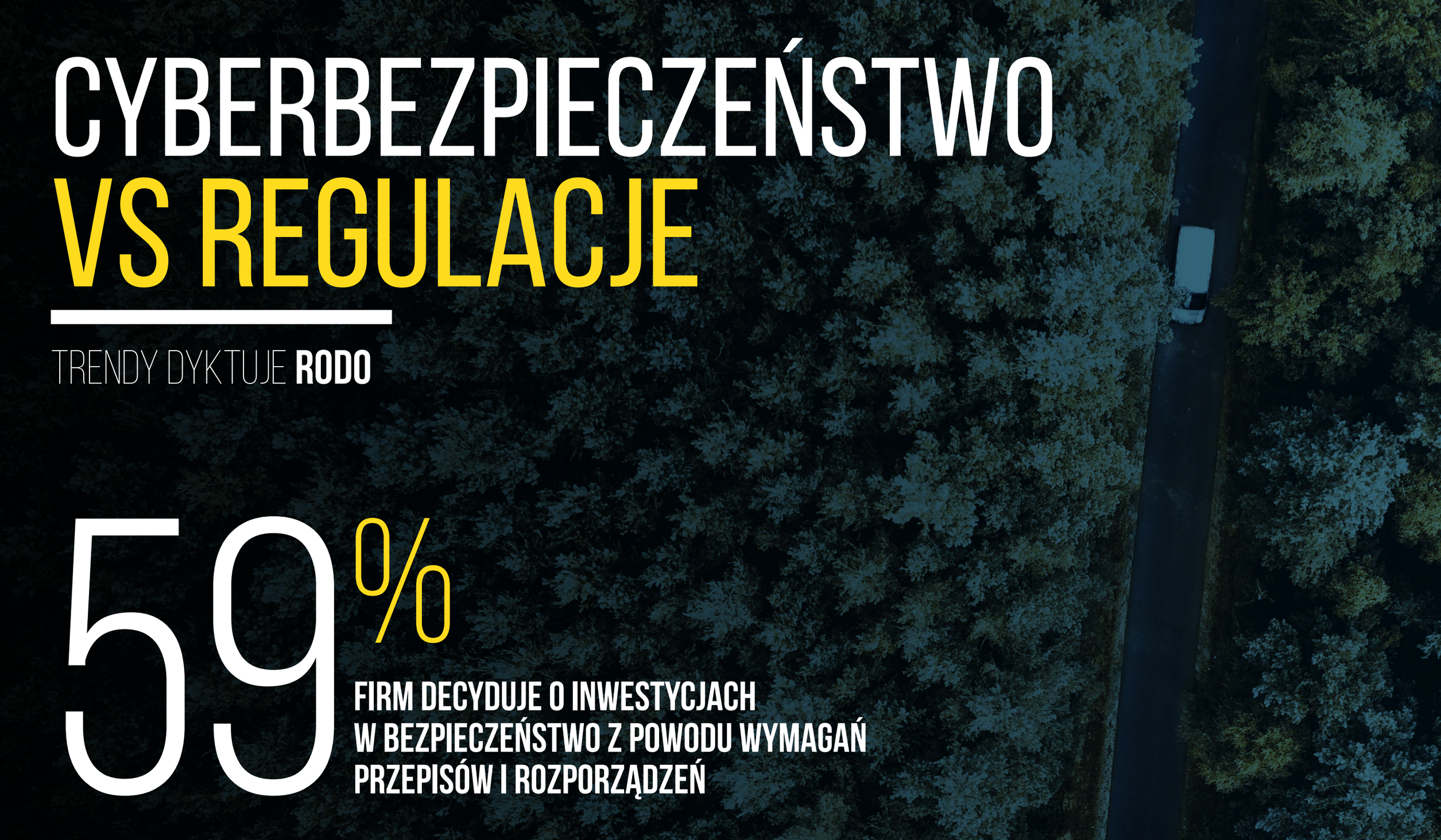
SPIS TREŚCI

CYBERBEZPIECZEŃSTWO VS REGULACJE

TRENDY DYKTUJE **RODO**

59%

FIRM DECYDUJE O INWESTYCJACH
W BEZPIECZEŃSTWO Z POWODU WYMAGAŃ
PRZEPISÓW I ROZPORZĄDZEŃ



Nowe przepisy i dyrektywy oznaczają ogromne zmiany w strategii bezpieczeństwa firm. To kolejne obowiązki, procedury, analizy i dokumentacje.

Poprzeczka jest coraz wyżej – w **85%** firm liczba zadań związanych z rozwojem i utrzymaniem systemów bezpieczeństwa wzrosła, jednocześnie aż w ponad połowie liczba pracowników odpowiedzialnych za rozwój i utrzymanie systemów bezpieczeństwa pozostała bez zmian.

W 57% FIRM NIE WZROSŁA LICZBA PRACOWNIKÓW ODPOWIEDZIALNYCH ZA BEZPIECZEŃSTWO

KOMENTARZ

Mec. Marcin Maruta,
kancelaria Maruta Wachta

RODO miało w ostatnim roku największy wpływ na zarządzanie bezpieczeństwem w firmach. Organizacje muszą poświęcić dużo czasu na analizę, gdzie i jakie dane mają, wiele firm do tej pory tego nie robiło. Dla licznych organizacji było to pierwsze zderzenie ze sformalizowaniem danych i okazał się to najbardziej kosztowny element procesu. Po raz pierwszy też bezpieczeństwo mogło wyjść przed szereg, na spotkaniach zarządu stało się tematem rozmów, ważnym obszarem inwestycji. Wcześniej bezpieczeństwo także było istotne, ale nie było przymusu legislacyjnego. Bezpieczeństwo z nice to have stało się must be.

Dwa lata temu, większość firm nie miała sformalizowanych procesów związanych z cyberbezpieczeństwem. Organizacje wykonały olbrzymią pracę w ciągu 24 miesięcy - to dobry początek, teraz te zagadnienia są brane pod uwagę już przy każdym nowym projekcie. Dzięki RODO część działów bezpieczeństwa wywalczyła sobie lepsze budżety i wyższą pozycję w firmie, wprowadziła nowe procedury.

Bezpieczeństwo z *nice to have* stało się *must be*

NOWE PROCESY

Firmy muszą formalizować procesy związane z zarządzaniem incydentami bezpieczeństwa, ale spora część jest dopiero na początku tej drogi

POSIADAM SFORMALIZOWANY PROCES ZARZĄDZANIA INCYDENTAMI BEZPIECZEŃSTWA

+

ZEWNĘTRZNY AUDYT BEZPIECZEŃSTWA TO CORAZ POPULARNIEJSZE ROZWIĄZANIE – STOSUJE JE JUŻ PONAD 50% ORGANIZACJI

KOMENTARZ

Piotr Żygadło,
Director of Solutions Department,
Dimension Data

W ciągu ostatniego roku działy bezpieczeństwa zostały obarczone zwiększającą się liczbą zadań m.in. z powodu nowych regulacji, które składają na nie także odpowiedzialność za ryzyko związane z prowadzenia biznesu. RODO wymaga skanowania, monitorowania zasobów zawierających dane osobowe. Jest to wyzwanie zwłaszcza w obszarze zasobów nieustrukturyzowanych. Organizacje mają ustawowy obowiązek raportowania wszelkich incydentów, konieczne jest wdrożenie odpowiednich rozwiązań i narzędzi.

Departamenty bezpieczeństwa, odpowiedzialne za wyciek danych, teraz odpowiadają też za monitoring sporej części procesów raportowania i to jest rzecz nowa – powoduje znaczący przyrost ilości pracy.

Przez ostatnie lata firmy wyraźnie spowolniły proces inwestycyjny, widzą powoli malejący zakres zamówień i wstrzymują inwestycje w rozwijanie składu osobowego, mimo wzrostu presji i ilości pracy.

Ludzie z obszaru bezpieczeństwa, poszukiwani przez rynek, są drodzy, przestają być osiągalni. Część firm wybiera outsourcing procesów związanych z cyberbezpieczeństwem do specjalistycznych firm. Niektórych instytucji, np. w sektorze medycznym po prostu nie stać na utrzymanie zespołu bezpieczeństwa i zapobieganie wyciekowi danych.

Rozwiązaniem może być poszukiwanie możliwości outsourcowania tych prac, znalezienia synergii. Regulacje bezpieczeństwa nakładają obowiązek raportowania do CERT, które jest w stanie skoordynować prace zespołów bezpieczeństwa z całego sektora np. finansowego przy atakach kierunkowych. To bardzo pozytywny sygnał – postępuje proces koordynacji.

82%

FIRM NIE MA WDROŻONYCH NARZĘDZI DO SKANOWANIA DANYCH OSOBOWYCH STRUKTURYZOWANYCH I NIEUSTRUKTURYZOWANYCH, KTÓRE POZWALAJĄ REGULARNIE INWENTARYZOWAĆ MIEJSCA ICH PRZECHOWYWANIA

Mec. Marcin Maruta,
kancelaria Maruta Wachta

Biorąc pod uwagę, że w naszym badaniu uczestniczyły duże, świadome przedsiębiorstwa, ten wynik budzi niepokój. Pokazuje, że mamy sporo do zrobienia. Przepisy wymagają od organizacji posiadania opisanego procesu, a w razie incydentów naruszenia bezpieczeństwa, proces ten może być audytowany. Nawet jeśli ten proces byłby niedoskonały, ale opisany, byłoby to podstawowe minimum. Jaka może być przyczyna takiego stanu rzeczy? Zakładam, że jest to brak czasu - wiele organizacji nagle zetknęło się z gigantyczną ilością wyzwań związanych z polityką prywatności i po prostu nie zdążyły wprowadzić nowych zasad w tym zakresie.

Ponad połowa firm korzysta z zewnętrznego audytu w zakresie bezpieczeństwa – imponujące. Tego typu audyty staną się jeszcze bardziej sformalizowane w przyszłości, w związku z kolejnymi przepisami wchodzącymi w życie, będą traktowane jako standard.

KOMENTARZ

KOMENTARZ

Piotr Żygadło,
Director of Solutions Department
Dimension Data

Firmy pójdą dwutorowo – część będzie stać na uruchomienie takich narzędzi, część będzie próbowała oddać to w outsourcing.

Łatwiej poradzić sobie z bazami danych ustrukturyzowanych, większość firm ma je zabezpieczone. Zbiory danych nieustrukturyzowanych to trudniejsze zagadnienie. Powoli buduje się świadomość w firmach, że posiadają nie tylko ustrukturyzowane zasoby, ale także szereg zbiorów dokumentów, które też zawierają dane osobowe. Część organizacji planuje inwestycje, część szuka rozwiązań – dane muszą podlegać regularnemu skanowaniu. Np. prośba klienta o usunięcie danych – wymaga indeksowania zasobów i wykasowania odpowiedniego rekordu. Przez najbliższe dwa lata firmy będą budować ten proces, obudowywać się narzędziami i usługami.

Przez najbliższe dwa lata **firmy będą tworzyć proces skanowania danych**, obudowywać się narzędziami i usługami

CYBERBEZPIECZEŃSTWO VS TECHNOLOGIE

Wyzwania związane z cyberbezpieczeństwem są coraz poważniejsze, ale najnowsze rozwiązania technologiczne pozwalają skutecznie zarządzać tym obszarem, przewidywać, eliminować czy osłabiać zagrożenia

+

Znaczna część inwestycji
to reakcja na najczęściej występujące zagrożenia

TOP ZAGROŻENIA

SOCJOTECHNIKA

OSZUSTWO (NP. KRADZIEŻ TOŻSAMOŚCI, E-MAIL)

SZKODLIWE OPROGRAMOWANIE, RANSOMWARE

NARUSZENIE OCHRONY DANYCH (WEWNĘTRZNE LUB ZEWNĘTRZNE)

TOP INWESTYCJE

ZARZĄDZANIE BEZPIECZEŃSTWEM

MONITORING I BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH

OCHRONA PUNKTÓW KOŃCOWYCH LUB URZĄDZEŃ MOBILNYCH

ROZWIĄZANIA UWIERZYTELNIAJĄCE

KOMENTARZ

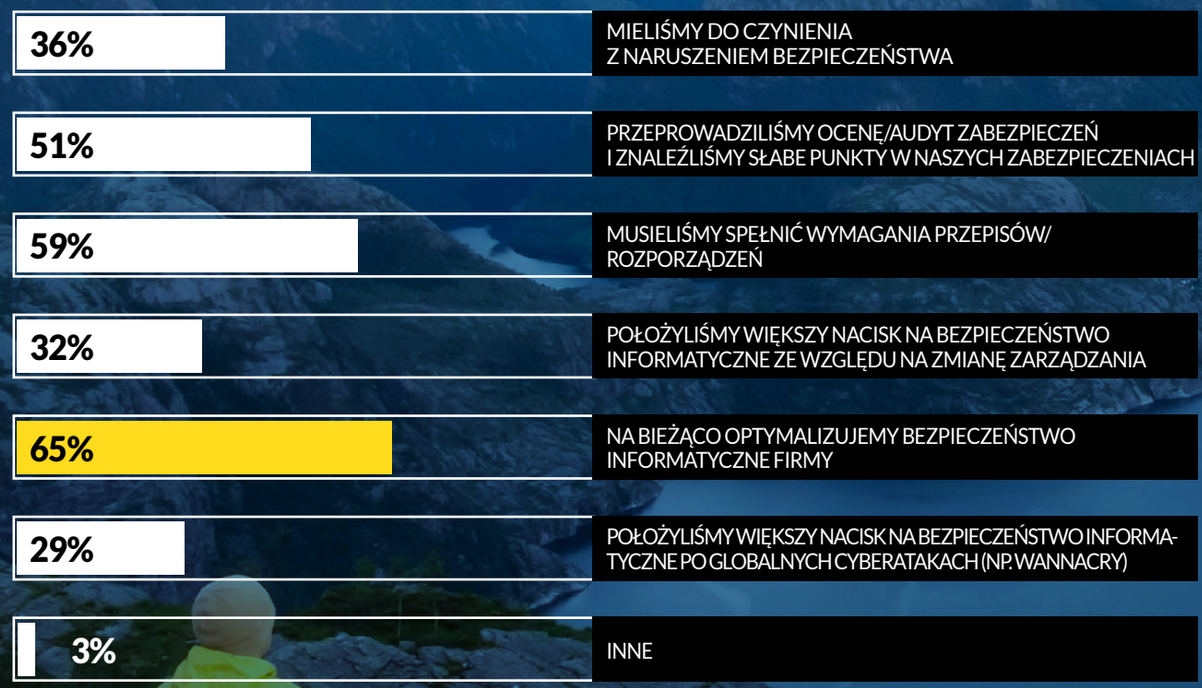
Jolanta Malak,
Regional Sales Director, Fortinet

Znaczna część inwestycji to reakcja na najczęściej występujące zagrożenia. Mają dotyczyć nie tylko pojedynczych rozwiązań, ale całych systemów zarządzania bezpieczeństwem czy analizy zagrożeń. Nowe regulacje wymuszają rozwiązania, które zapewnią zgodność z przepisami, zwłaszcza w kwestii monitoringu i przetwarzania danych osobowych. Inwestycje w bezpieczeństwo poczty e-mail, komunikatorów, punktów końcowych i urządzeń mobilnych to odpowiedź na popularność ataków typu ransomware oraz zabiegów socjotechnicznych. Systemy backupu i archiwizacji danych mają pomóc w przypadku ataków ransomware bądź kradzieży danych przez cyberprzestępców. Firmy chcą być przygotowane na każdą ewentualność i mieć odpowiednie zabezpieczenia.

SŁABE PUNKTY

WIĘKSZOŚĆ ORGANIZACJI STALE I NA BIEŻĄCO OPTYMALIZUJE BEZPIECZEŃSTWO FIRMY. DLA WIELU SILNYM BODŹCEM DO DZIAŁANIA JEST AUDYT ZABEZPIECZEŃ I ZNALEZIENIE SŁABYCH PUNKTÓW ORAZ WYMAGANIA PRZEPISÓW I ROZPORZĄDZEŃ

CZYNNIKI DECYZYJNE



*Respondenci odpowiadali na pytanie: Które z poniższych stwierdzeń kształtuje decyzje dotyczące inwestycji w bezpieczeństwo informatyczne w Twojej firmie? Wybierz wszystkie pasujące odpowiedzi

FIRMY WCIĄŻ INWESTUJĄ PRZEDE WSZYSTKIM REAKTYWNIE – ODPOWIADAJĄC NA ZAGROŻENIA, KTÓRE JUŻ SIĘ POJAWIŁY I SĄ ZNANE. DUŻY NACISK KŁADĄ TAKŻE NA OCHRONĘ DANYCH OSOBOWYCH, KTÓRĄ WYMUSZAJĄ NOWE PRZEPISY

Jolanta Malak,
Regional Sales Director, Fortinet

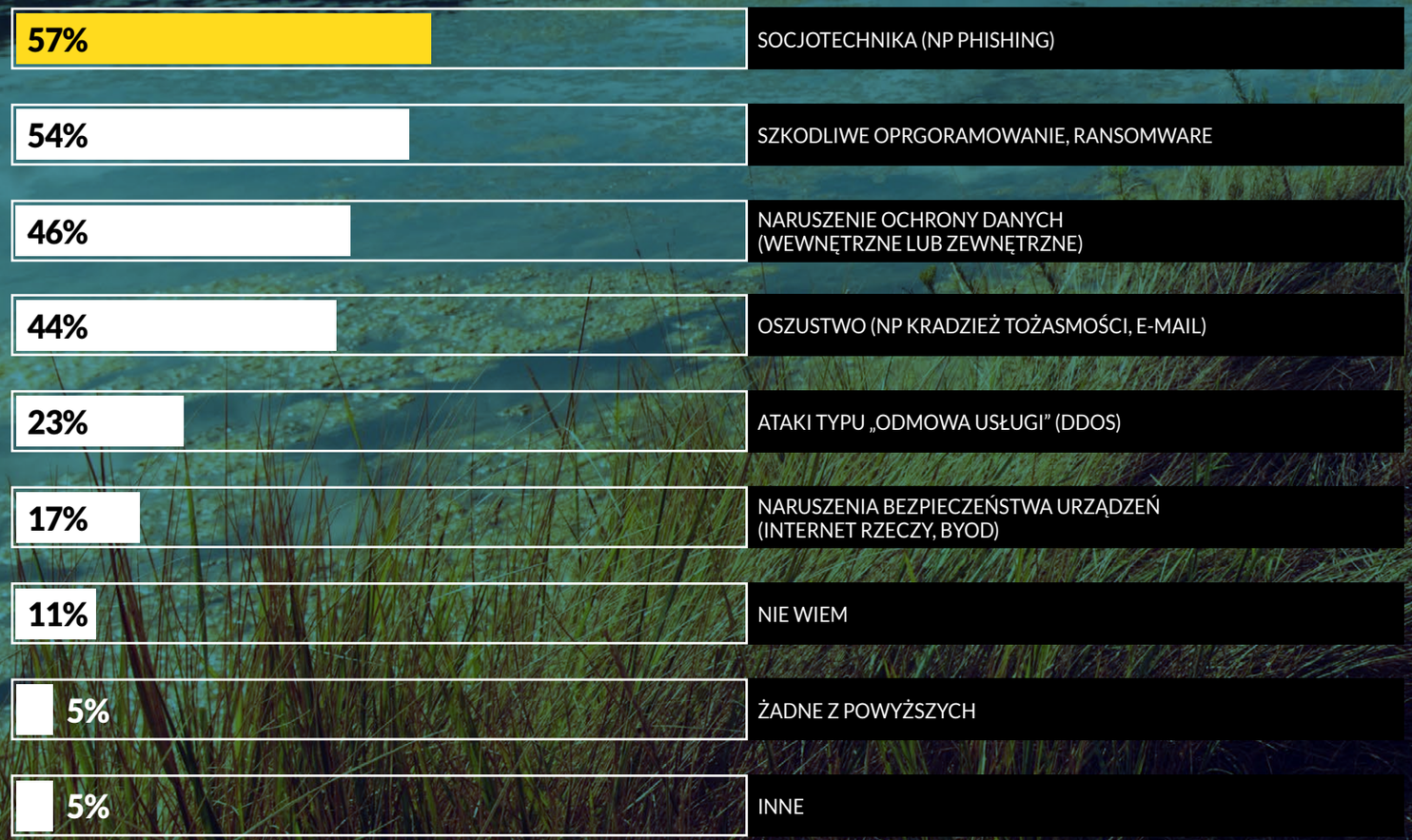
Firmy inwestują w bezpieczeństwo IT, przede wszystkim na bieżąco optymalizując rozwiązania i systemy zabezpieczeń. Duże znaczenie ma wzrost presji ze strony organów regulacyjnych – przy wysokich karach finansowych, już od dolnej granicy, zarząd jest zmuszony do zainteresowania się tematem cyberbezpieczeństwa, szczególnie w związku z wejściem w życie RODO.

Cyberbezpieczeństwo to obecnie sprawa firmy jako całości. Zmiana modelu zarządzania, zatrudnienie nowych specjalistów i wyniki audytów prowadzą do decyzji o zwiększeniu nakładów na ten cel.

Informacje o globalnych atakach oraz własne doświadczenia naruszenia bezpieczeństwa zwracają uwagę zarządów na cyberbezpieczeństwo. Kwestie z nim związane wykraczają poza działy IT.

SOCJOTECHNIKA JEST DOCENIANA JAKO DOMINUJĄCE ZAGROŻENIE PRZEZ WIĘKSZOŚĆ ORGANIZACJI – SILNIE WIĄŻE SIĘ Z OBAWĄ O NARUSZENIE OCHRONY DANYCH. ZABEZPIECZENIE SYSTEMÓW PRZED SZKODLIWYM OPROGRAMOWANIEM JEST JUŻ OD WIELU LAT DZIAŁANIEM OCZYWISTYM I RUTYNOWYM

RANKING ZAGROŻEŃ



*respondenci odpowiadali na pytanie: Na które z poniższych zagrożeń Twoja firma jest obecnie w dalszym ciągu narażona najbardziej? Wybierz wszystkie pasujące odpowiedzi

KOMENTARZ

Tomasz Orłowski,
Kierownik Zespołu Produktów ICT, NETIA

Większość firm zbudowała już podstawowy pancerz ochronny i teraz poszukuje metod jego wzmacniania, poprzez dobór bardziej proaktywnych metod prewencji i detekcji zagrożeń. Widać duże zainteresowanie audytami, testami bezpieczeństwa, nowoczesnymi technikami monitoringu sieci i systemów (SOC, SIEM), czy aktywnego wyszukiwania, gromadzenia i analizowania informacji o zagrożeniach (tzw. threat intelligence). W ramach poszukiwania nowych metod walki z cyberprzestępczością, firmy coraz częściej pytają o narzędzia działające w sposób niekonwencjonalny. Rośnie zainteresowanie rozwiązaniami wykorzystującymi metody sztucznej inteligencji (AI) czy mechanizmy uczenia maszynowego (machine learning). Zdecydowana większość dużych firm rozumie już, że największym źródłem zagrożeń jest często czynnik ludzki - nieświadomy pracownik, najsłabsze ogniwo w łańcuchu zabezpieczeń. Świadomość ludzkich ułomności i możliwości popełniania błędów prowokuje do coraz popularniejszego przeprowadzania specjalistycznych szkoleń i symulacji ataków socjotechnicznych, a także wzmacniania mechanizmów ochrony, czuwających bezpośrednio nad środowiskiem informatycznym użytkownika końcowego (tzw. end-point protection). Wzrasta przy tym jednocześnie zainteresowanie zaawansowanymi systemami ochrony poczty firmowej (anty-malware, anty-phishing), która jest obecnie najczęstszym obiektem ataków.

W nierównej walce ze skutkami działalności cyberprzestępczej zdecydowanie więcej możliwości ochrony jest w dużych firmach, które dedykują specjalne budżety na realizację swojej strategii bezpieczeństwa IT i stale zwiększają zatrudnienie specjalistów w tym obszarze. Duże przedsiębiorstwa stać również na budowanie i utrzymanie zespołów SOC; większość z nich deklaruje posiadanie sformalizowanego procesu monitorowania i zarządzania incydentami bezpieczeństwa. Działania te są akcelerowane przez konieczność dostosowania do nowych regulacji (RODO czy KSC) oraz przez widmo ewentualnych konsekwencji za brak zgodności.

MIMO, ŻE NAJWIĘKSZE OBAWY BUDZĄ ATAKI SOCJOTECHNICZNE, W CIĄGU OSTATNICH DWÓCH LAT FIRMY NAJCZĘŚCIEJ NĘKANE BYŁY ATAKAMI WYKORZYSTUJĄCYMI SZKODLIWE OPROGRAMOWANIE

Z KTÓRYMI Z PONIŻSZYCH ZAGROŻEŃ BEZPIECZEŃSTWA MIAŁA DO CZYNIENIA TWOJA FIRMA W CIĄGU OSTATNICH 2 LAT?

Jolanta Malak,
Regional Sales Director, Fortinet

Najczęstsze zagrożenie, z jakim spotykały się firmy, to złośliwe oprogramowanie oraz ransomware. Uważać trzeba także na zabiegi socjotechniczne stosowane przez cyberprzestępców (jak np. phishing) i oszustwa. Problemem są wewnętrzne naruszenia bezpieczeństwa danych. Biorąc pod uwagę to oraz skalę ataków z wykorzystaniem socjotechniki, trzeba inwestować w szkolenia pracowników i podnosić ich świadomość cyberhigieny.

Co czwartą firmę dotknął atak typu DDoS, który powoduje przestoje w pracy firmy i również generuje poważne straty. Naruszenia bezpieczeństwa IoT oraz przedmiotów przynoszonych przez pracowników do firmy (BYOD) zdarzają się stosunkowo rzadko. Zetknęło się z nimi tylko 13% badanych.

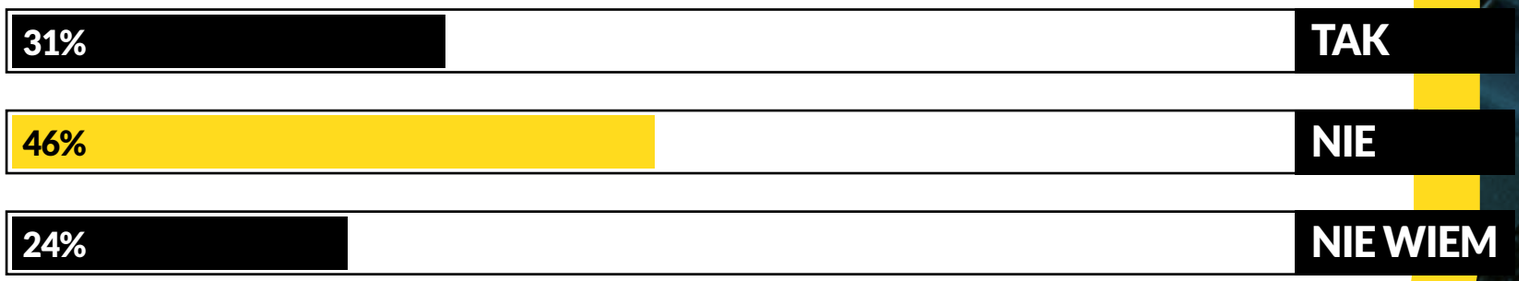
Co dziesiąty badany nie potrafił odpowiedzieć, czy w jego firmie doszło do naruszenia bezpieczeństwa informatycznego. Często niestety firmy nie mają świadomości, że dochodzi do takiej sytuacji, a naruszenie jest wykrywane dopiero przez podmioty zewnętrzne. Średnia liczba dni, które mijają od zaistnienia ataku do jego wykrycia wzrosła z 201 w 2016 roku do 206 w roku ubiegłym*.

*Źródło: Securityweek

POLITYKA OBRONNA

NIEMAL CO TRZECIA FIRMA W CIĄGU OSTATNIEGO ROKU ZAOBSERWOWAŁA PRZYPADKI WYKRYCIA PRZEZ DZIAŁ IT ZŁOŚLIWEGO OPROGRAMOWANIA. JEDNAK DANE TE NIE SĄ DO KOŃCA MIARODAJNE, PONIEWAŻ ZALEDWIE 61% ORGANIZACJI PROWADZI STATYSTYKĘ INCYDENTÓW BEZPIECZEŃSTWA

CZY ZDARZYŁY SIĘ PRZYPADKI WYKRYCIA ZŁOŚLIWEGO OPROGRAMOWANIA KONTAKTUJĄCEGO SIĘ Z SIECIĄ C&C POZA FIRMĄ?



KOMENTARZ

Łukasz Bromirski,
CTO, CISCO

Jest to wynik zbieżny z ostatnimi badaniami Cisco Annual Security Report - w którym wskazywaliśmy że ok. 30% firm globalnie a ok. 45% firm w Polsce było w stanie wykryć złośliwe oprogramowanie pracujące w botnecie. Odpowiedź "nie wiem" też wskazuje na trend - nadal dużo firm nie widzi lub nie jest w stanie z pełnym przekonaniem stwierdzić, że jest w stanie obserwować cały ruch.

To chleb powszedni. Robimy to regularnie, zaraz po tym jak producent wypuści łatki i mamy do tego celu odpowiednie zasoby

62%

Ostateczność. Łatamy tylko najbardziej krytyczne systemy. Cała reszta musi zaczekać

5%

Aktualizowanie systemów stoi w pewnym sensie w sprzeczności z podstawowym zadaniem zespołów IT, jakim jest utrzymanie ciągłości działania systemów

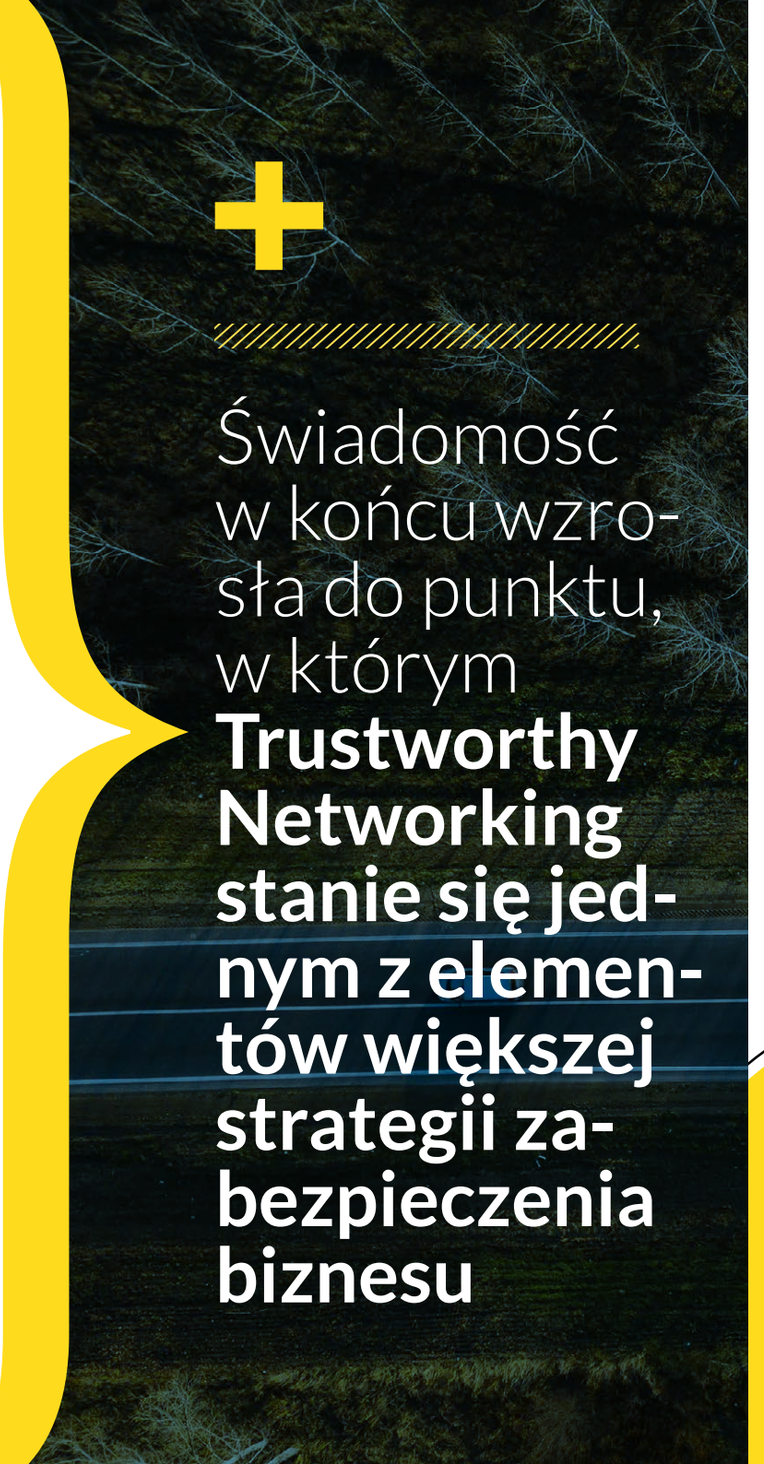
KOMENTARZ

Andrzej Sawicki,
Sales Engineer, Trend Micro

Zarządzanie aktualizacjami to problem w wielu firmach. Jestem pozytywnie zaskoczony wynikami badania, które pokazują, że coraz więcej organizacji w poważny sposób podchodzi do tego zagadnienia. Wymaga ono dużych nakładów pracy oraz czasu, które przekładają się na koszty. Aktualizowanie systemów stoi w pewnym sensie w sprzeczności z podstawowym zadaniem zespołów IT, jakim jest utrzymanie ciągłości działania systemów. Każda aktualizacja bowiem niesie za sobą ryzyko przestoju, bo stanowi ingerencję w dobrze działające aplikacje oraz systemy. Tym bardziej cieszy tak wysoki odsetek ankietowanych, którzy deklarują, że dysponują zasobami do tego, aby regularnie przeprowadzać aktualizacje.

KONTROLA NAJWYŻSZĄ FORMĄ ZAUFANIA

FIRMY SĄ W POŁOWIE DROGI W STOSOWANIU FILOZOFII ZERO TRUST I MODELU SECURITY-IN--DEPTH W PLANOWANIU I BUDOWANIU SYSTEMU BEZPIECZEŃSTWA TELEINFORMATYCZNEGO. W SKALI 1 DO 5 OCENIAJĄ STOSOWANIE TEGO MODELU NA 2.5. JEDNOCZEŚNIE WIĘKSZOŚĆ MA PRZEKONANIE, ŻE UŻYWANE OPROGRAMOWANIE JEST PEWNE I NIE ZOSTAŁO W ŻADEN SPOSÓB ZMODYFIKOWANE



\+

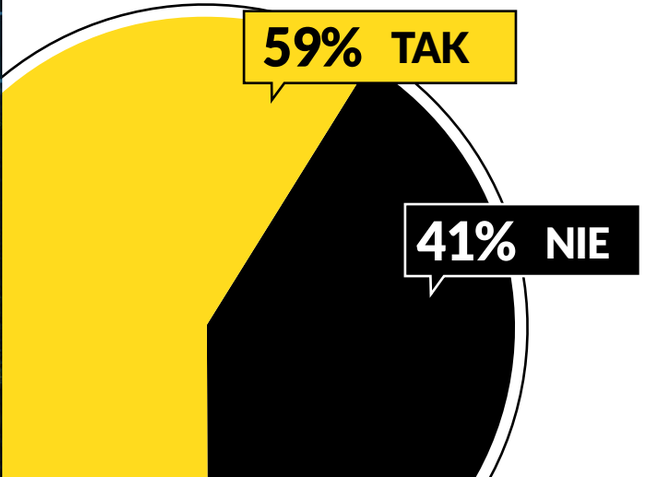
Świadomość w końcu wzrosła do punktu, w którym **Trustworthy Networking stanie się jednym z elementów większej strategii zabezpieczenia biznesu**

KOMENTARZ

Łukasz Bromirski,
CTO, CISCO

Jest to temat nowy, o którym dyskusja się dopiero rozpoczyna. Dyskusje, które rozpoczął artykuł w Bloombergu dotyczący rzekomego osadzenia przez chińskich szpiegów sprzętowych implantów w płytach Super Micro spowodowały, że nagle wszyscy zrozumieli, jak wielkim zagrożeniem może być tego typu modyfikacja. Ciekawe jest tak mocne stwierdzenie "tak, jestem pewien", ponieważ firmy w Polsce z reguły nie prowadzą badania sprzętu oraz audytów kodu przed wprowadzeniem rozwiązań jako elementów systemów produkcyjnych. Interesujące jest jednak aż 41% "nie, nie jestem pewien" - i to jest temat, którym będziemy się zajmować. Od wielu lat poruszaliśmy temat Trustworthy Networking i wygląda na to, że świadomość w końcu wzrosła do punktu, w którym temat ten stanie się jednym z elementów większej strategii zabezpieczenia biznesu.

CZY SPRZĘT I OPROGRAMOWANIE W FIRMIE POCHODZI OD PRODUCENTÓW I NIE ZOSTAŁO W ŻADEN SPOSÓB ZMODYFIKOWANE?



CHMURA PUBLICZNA? OSTROŻNIE

W FIRMACH WCIĄŻ NIEWIELKI ODSETEK APLIKACJI ZNAJDUJE SIĘ W CHMURZE PUBLICZNEJ, ALE GDY WZROŚNIE ZAUFANIE DO BEZPIECZEŃSTWA TEGO MODELU – WZROŚNIE TAKŻE PROPORCJA ZASOBÓW UMIESZCZANYCH W CHMURZE

PROCENT APLIKACJI W FIRMIE W CHMURZE PUBLICZNEJ

10%

Piętą achillesową cyfrowej transformacji **jest cyberbezpieczeństwo**

KOMENTARZ

Marius Baczynski,
Regional Sales Manager, ZSCALER

Piętą achillesową cyfrowej transformacji jest cyberbezpieczeństwo. Rosnące geometrycznie tempo migracji aplikacji do chmury oraz wszechobecna mobilność powodują, że internet staje się nową siecią korporacyjną, a to z kolei wiąże się z ogromnymi wyzwaniami w obszarze bezpieczeństwa i zaufania. Dla wielu organizacji obawy związane właśnie z cyberbezpieczeństwem w dużej mierze hamują tempo migracji do chmury.

Z badania wynika, że ponad połowa firm nie lokuje swoich zasobów w chmurze. Pozostała połowa umieszcza tam średnio ok. 20% zasobów. Wiele firm nadal nie migruje do chmury i pozostaje w starej rzeczywistości, np. z powodu braku regulacji prawnych bądź bardzo skomplikowanych przepisów, braku zaufania i poczucia bezpieczeństwa. Wyniki badania pokazują, że gdyby firmy miały większe zaufanie do bezpieczeństwa w chmurze, aż 6% z nich byłoby skłonnych przenieść tam nawet 66% aplikacji, a co czwarta firma co najmniej 50%.

W licznych organizacjach nadal obowiązuje „stara szkoła", która mówi, że kwestii związanych z cyberbezpieczeństwem nie można powierzyć na zewnątrz. W pozostałych firmach świadomość potężnych korzyści wynikających z przeniesienia się do nowej, cyfrowej rzeczywistości wyzwala zupełnie nowy poziom tolerancji na kwestie możliwych zagrożeń – decyzje o przesunięciu mniej krytycznych aplikacji do chmury stają się oczywiste. Połowa firm boi się eksperymentować, ale połowa już działa w nowej rzeczywistości. Dostawcy cyberzabezpieczeń najnowszej generacji wychodzą temu trendowi naprzeciw i wspierają organizacje w przejściu do nowego modelu działania.

Firmy nadal boją się wdrożeń w chmurze, ale jednocześnie od kilku lat coraz szybciej rośnie odsetek jej użytkowników

CZEMU ORGANIZACJE OBAWIAJĄ SIĘ CHMURY? NIEMAL CO TRZECIA FIRMA UWAŻA, ŻE TRACI W TEN SPOSÓB KONTROLĘ NAD ZASOBAMI

CZY W CHMURZE SKŁADNIKI I RELACJE MIĘDZY PRACOWNIKAMI PRACUJĄCYMI ZDALNIE, SIECIĄ FIRMOWĄ I WYBRANĄ CHMURĄ SĄ W PEŁNI WIDOCZNE?

KOMENTARZ

Łukasz Bromirski,
CTO, CISCO

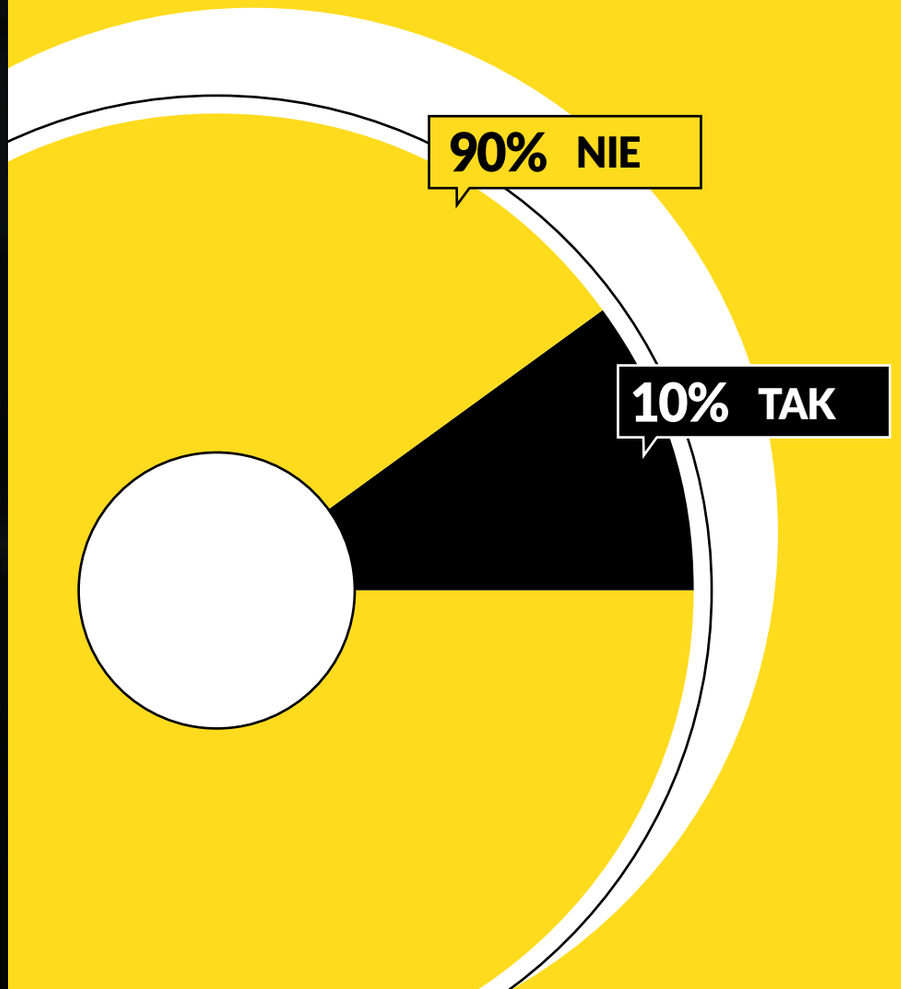
Firmy nadal boją się wdrożeń w chmurze, ale jednocześnie odsetek rozpoczynający korzystanie z niej z perspektywy ostatnich 4 lat rośnie dosyć dynamicznie. Publiczne chmury dopiero od niedawna zaczynają oferować proste mechanizmy zapewniające możliwość zajrzenia w ruch pomiędzy instancjami maszyn wirtualnych, jest to zatem dosyć ciekawe w kontekście odpowiedzi aż 26% respondentów na "tak".

CYBERBEZPIECZEŃSTWO VS CZŁOWIEK

Człowiek jest najsłabszym ogniwem łańcucha bezpieczeństwa. Najłatwiej ulega presji socjotechnicznej i popełnia błędy – wciąż dopiero uczymy się korzystania z nowych technologii w możliwie najbezpieczniejszy sposób. Urządzenia mobilne sprawiły, że granica między życiem prywatnym i służbowym zaciera się

Wprawdzie tylko **10%** firm przyznaje, że pracownicy wynoszą dane poza granice ich sieci, ale znaczna część organizacji mogła po prostu nie wykryć tego typu incydentów. Jeśli taki problem się już pojawi, oznacza bardzo poważne wyzwanie nie tylko dla działu bezpieczeństwa, ale dla całej firmy

CZY W CIĄGU OSTATNIEGO ROKU ZAOBSERWOWAŁEŚ PRZYPADKI, W KTÓRYCH PRACOWNICY LUB OPROGRAMOWANIE ZŁOŚLIWE PRZERZUCAŁO DANE POZA SIEĆ FIRMY?



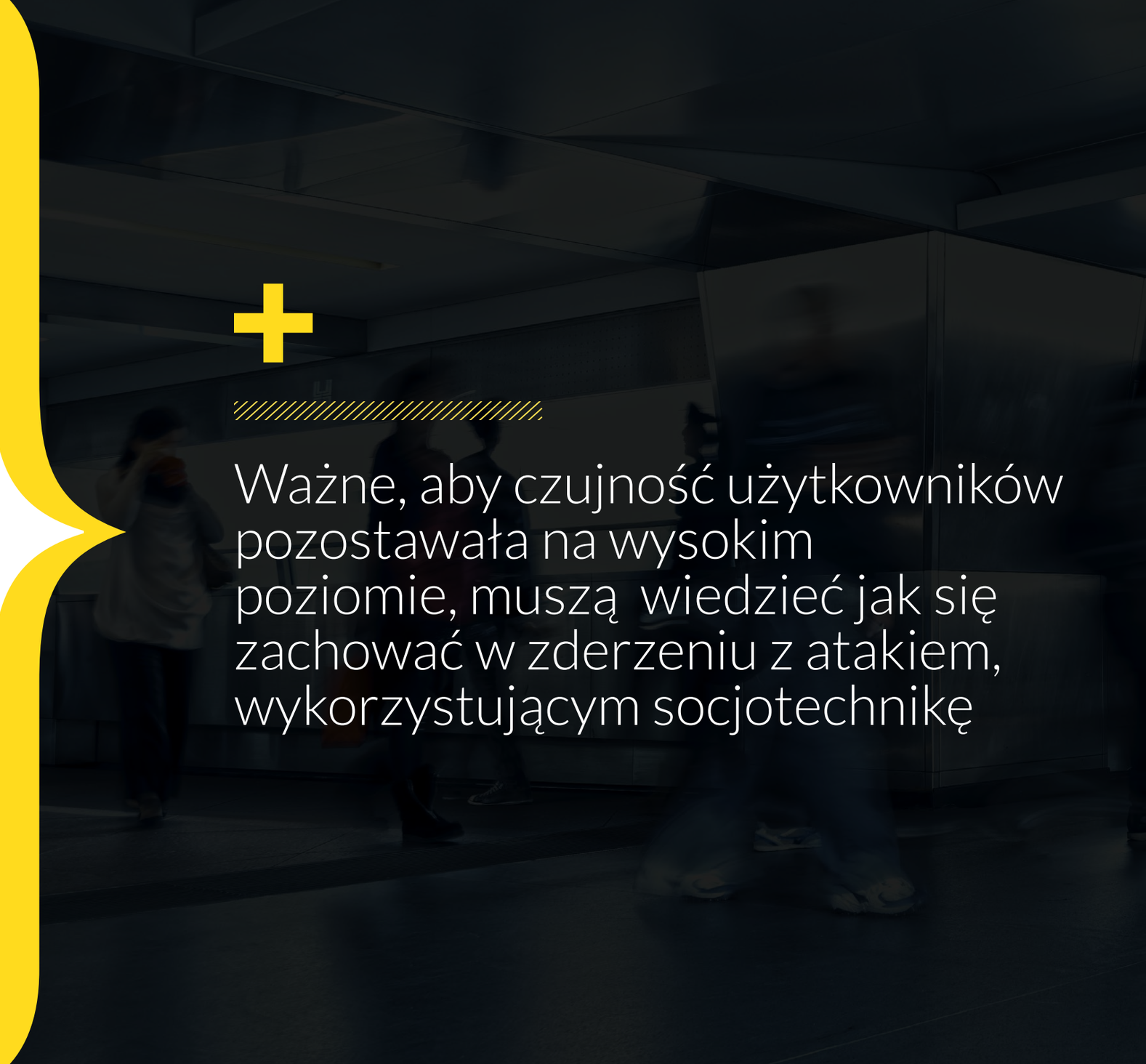
KOMENTARZ

Mec. Marcin Maruta,
kancelaria Maruta Wachta

Wynik wskazuje na pozytywny trend – o ile jest to rzeczywista proporcja incydentów, a z incydentami jest ten kłopot, że najpierw trzeba je wykryć by odpowiedzieć na takie pytania. W praktyce ochrona własności intelektualnej, zabezpieczenie przed wyciekiem danych, kradzież przez pracowników czy współpracowników to duże wyzwanie dla firm. Skoro, przy pełnej świadomości niekompletności takiej statystyki, 10% firm odnotowało takie incydenty, to znaczy, że jest to istotny problem, którego nie można lekceważyć. A problem ze złośliwym oprogramowaniem to w ogóle jakiś koszmar – i dla IT i dla prawników i dla compliance.

TWIERDZA SZYFRÓW?

EDUKACJA, POWSZECHNA ŚWIADOMOŚĆ I ODPOWIEDNIE OPROGRAMOWANIE – TO PODSTAWOWE ZASADY HIGIENY POCZTY ELEKTRONICZNEJ W WIĘKSZOŚCI ORGANIZACJI



+

Ważne, aby czujność użytkowników pozostawała na wysokim poziomie, muszą wiedzieć jak się zachować w zderzeniu z atakiem, wykorzystującym socjotechnikę

JAK ZARZĄDZASZ BEZPIECZEŃSTWEM POCZTY ELEKTRONICZNEJ?

1%	BEZPIECZEŃSTWO ODDAJEMY W RĘCE UŻYTKOWNIKÓW. TO ONI POWINNI DECYDOWAĆ CO MOŻE NAM ZASZKODZIĆ, A CO NIE
16%	MAMY BARDZO SKUTECZNIE SYSTEMY OCHRONY POCZTY. SPAM I PHISHING NAS NIE DOTYCZY
70%	STAWIAMY NA SZKOLENIE UŻYTKOWNIKÓW ORAZ DOBRE SYSTEMY BEZPIECZŃSTWA. NA KONIEC DNIA TO I CZŁOWIEK I MASZYNA MUSZĄ ZADZIAŁAĆ POPRAWNIE, ABY NIE DOPUŚCIĆ DO INFEKCJI
0%	KASUJEMY Z POCZTY WSZYSTKO CO DA SIĘ SKASOWAĆ, POZA CZYSTYM TEKSTEM. NIC NAM NIE MOŻE ZASZKODZIĆ
13%	JESTEŚMY CHRONIENI, BO POCZTĘ MAMY W CHMURZE. TAM DOSTAWCA USŁUGI ODPOWIADA ZA NASZE BEZPIECZEŃSTWO

KOMENTARZ

Andrzej Sawicki,
Sales Engineer, Trend Micro

Inwestowanie w nowoczesne i skuteczne zabezpieczenia to ważny element strategii ochrony poczty. Niestety czasem nawet najlepsze produkty potrafią zawieść. Dlatego ważne jest, aby czujność użytkowników pozostawała na wysokim poziomie, muszą wiedzieć jak się zachować w zderzeniu z atakiem, wykorzystującym sztukę socjotechniki. Należy ich regularnie szkolić i wystawiać na próbę, symulując ataki socjotechniczne, aby w praktyce wiedzieli, jak je odpierać. Zresztą pracownicy często wdzięczni są za tego typu szkolenia, gdyż one pozwalają im pozostać bezpiecznymi, także w życiu prywatnym.

POLITYKA HASEŁ JEST KOLEJNYM, NIE TYLKO TEGOROCZNYM, MUST HAVE BEZPIECZNEJ ORGANIZACJI. WIĘKSZOŚĆ OSÓB TWIERDZI, ŻE MA DOBRZE ZABEZPIECZONE HASŁA, TYMCZASEM PO SPRAWDZENIU OKAZUJE SIĘ, ŻE ŚREDNIO ZAAWANSOWANEMU HAKEROWI UDAJE SIĘ JE ZŁAMAĆ W KILKA SEKUND

Dziesiątki haseł wciąż są słabym ogniwem, nie tylko w ludzkiej pamięci, ale także w systemach bezpieczeństwa. Jednak nadal nie wszystkie firmy zmuszają swoich pracowników do tworzenia bezpiecznych i unikatowych haseł, większość nawet nie udostępnia do tego odpowiednich narzędzi.

Widać spory chaos i brak strategii wdrażania bezpieczeństwa, ponieważ część z podejmowanych działań jest, krótko mówiąc, bez sensu

KOMENTARZ

Piotr Konieczny,
CISO, Niebezpiecznik.pl

Wyniki ankiety lekko mnie zdziwiły. Z jednej strony są bardzo pozytywne, bo pokazują, że polskie firmy myślą o bezpieczeństwie i działają w kierunku jego zwiększenia. Z drugiej strony widać spory chaos i brak strategii wdrażania tego bezpieczeństwa, ponieważ część z podejmowanych działań jest, krótko mówiąc, bez sensu.

Większość ankietowanych przyznała, że wymaga od swoich pracowników korzystania z unikatowych haseł (65 vs 28) do różnych usług. To świetnie! Ale z drugiej strony te firmy nie dają pracownikom żadnych narzędzi do generowania takich haseł i ich bezpiecznego przechowywania, czyli tzw. managerów haseł (66 vs 33).

Co to oznacza dla współczesnego pracownika, który ma obowiązek korzystania z średnio 30-40 różnych haseł? Że tworzone przez niego hasła będą bardzo słabe. Naprawdę tragiczne.

Z doświadczenia płynącego z ataków na polskie firmy, jakie w ostatnich latach przeprowadził mój zespół bezpieczeństwa, mogę ujawnić to, jak takie zarządzanie hasłami wygląda w każdej firmie jaką atakowaliśmy, która nie wymagała używania managerów haseł od swoich pracowników.

W skrócie, pracowników można podzielić na takich, którzy tworzą hasła wpadające w 2 kategorie:

- **Przewidywalne.** Bazujące zazwyczaj na ulubionym dla pracownika słowie, plus kolejnych cyfrach i zwrotach. Np. Koteczek1poczta, Koteczek2vpn, Koteczek3windows. Problem? Jeśli pracownik z sukcesem zostanie „sphishowany" na jednej z usług, to atakujący to OD RAZU domyśli się „algorytmu" pracownika i spróbuje haseł „Koteczek(1-99)(nazwa_innej_usługi)" do wszystkich znanych mu firmowych usług.
- **Nieprzewidywalne.** Te hasła są zupełnie różne i niepowiązane ze sobą, ale przez to ciężko je zapamiętać. No bo kto ma głowę do pamiętania 30 różnych haseł? Wtedy hasła znaleźć można, zazwyczaj w formie niezaszyfrowanej, w plikach hasla.txt lub hasla.doc na komputerze ofiary.

Podsumowując, wiele firm traci czas na tłumaczenie jakie hasło powinno być dobre (silne, długie, zawierające różne znaki, unikatowe, itp.) - ale pracownicy i tak nie będą się do tych rad stosować. Bo wygoda dla ludzi jest ważniejsza niż bezpieczeństwo.

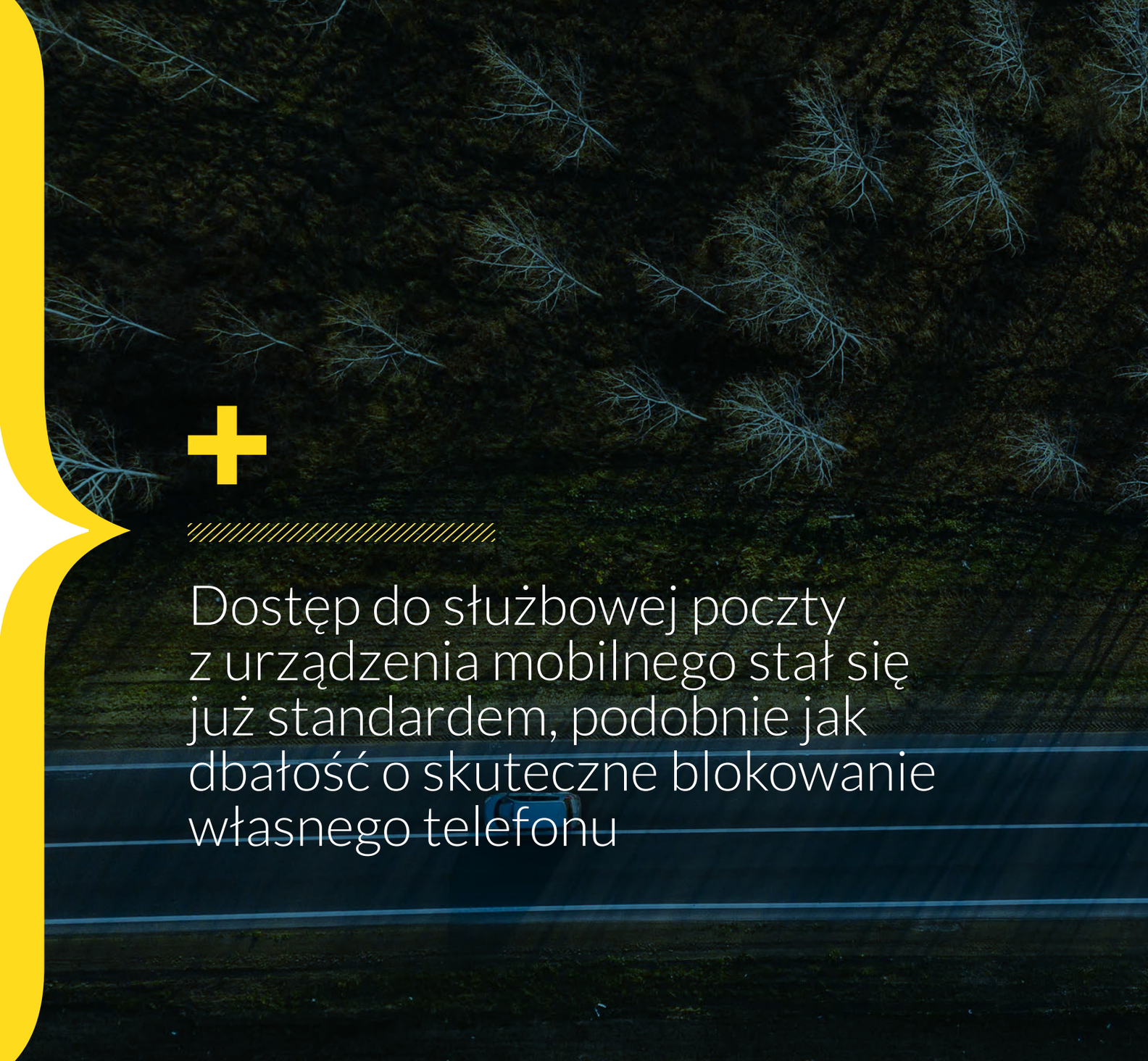
Efekt bezpiecznej polityki haseł można jednak uzyskać inną, zdecydowanie skuteczniejszą radą: „Pracowniku! Stosuj manager haseł!".

Dostarczenie pracownikowi managera haseł (który jest prosty w obsłudze, zwłaszcza jeśli integruje się z przeglądarką) nie kosztuje wiele lub jest całkowicie darmowe, jeśli firma wykorzysta „brzydsze" oprogramowanie Open Source. Do tego krótki instruktarz, nawet w formie dwuminutowego filmiku nagranego przez dział IT i już problem generowania różnych silnych haseł i konieczność ich pamiętania mamy z głowy. Drodzy CSO, przestańcie więc mówić pracownikom o silnych hasłach - mówcie im o managerach haseł.

I wiedzę tę przekażcie jak najszybciej, bo tzw. „reuse" haseł (lub domyślenie się hasła na podstawie poprzedniego) to jedna z przynoszących najwięcej strat technik z jakich w trakcie ataku korzystają włamywacze. Warto więc poprawnie się przed nią zabezpieczyć. Zwłaszcza, że nic to nie kosztuje, a zatem będzie się dało pogodzić z kolejnym wnioskiem płynącym z ankiety - tylko 1/3 ankietowanych firm ma jakikolwiek budżet na edukację swoich pracowników.

BEZPIECZNI I MOBILNI?

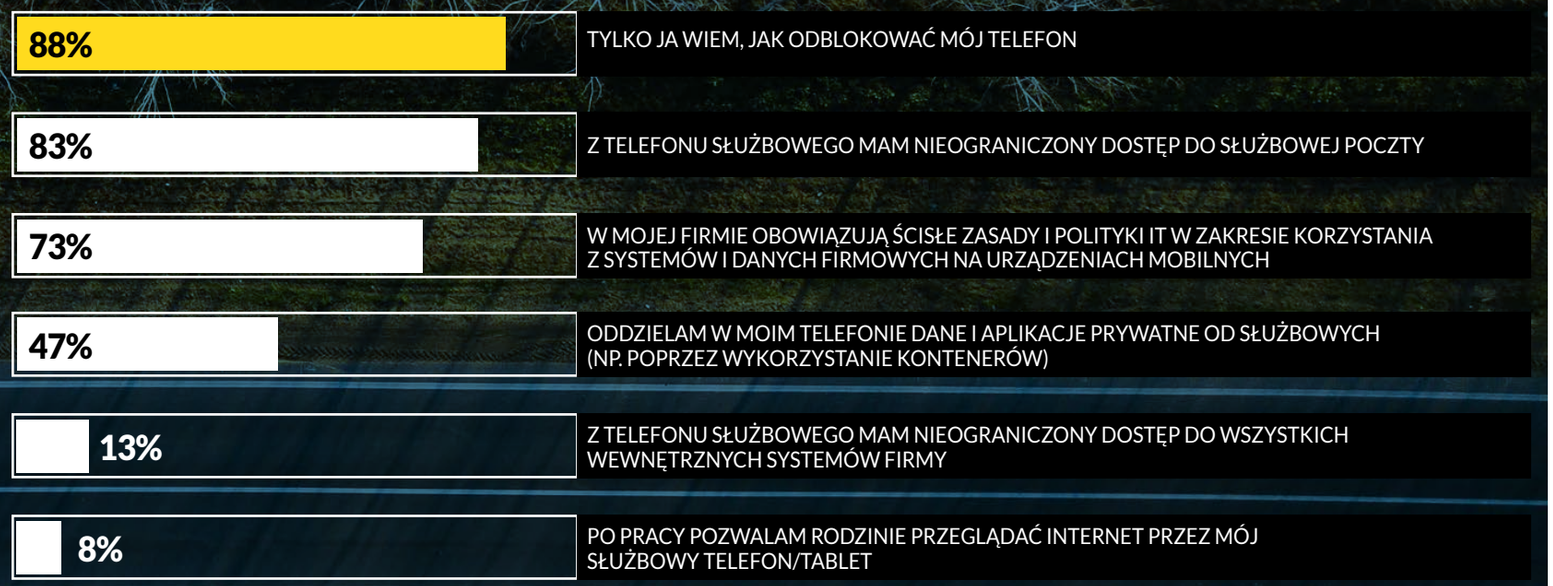
ŚWIADOMOŚĆ ZWIĄZANA Z BEZPIECZEŃSTWEM KORZYSTANIA Z ROZWIĄZAŃ MOBILNYCH JEST CORAZ WYŻSZA – W WIĘKSZOŚCI FIRM OBOWIĄZUJĄ ŚCISŁE ZASADY DOTYCZĄCE TEGO OBSZARU, A TYLKO NIEWIELE ORGANIZACJI POZWALA NA NIEOGRANICZONY DOSTĘP DO WSZYSTKICH WEWNĘTRZNYCH SYSTEMÓW Z TELEFONU



+

Dostęp do służbowej poczty z urządzenia mobilnego stał się już standardem, podobnie jak dbałość o skuteczne blokowanie własnego telefonu

POLITYKA MOBILNOŚCI



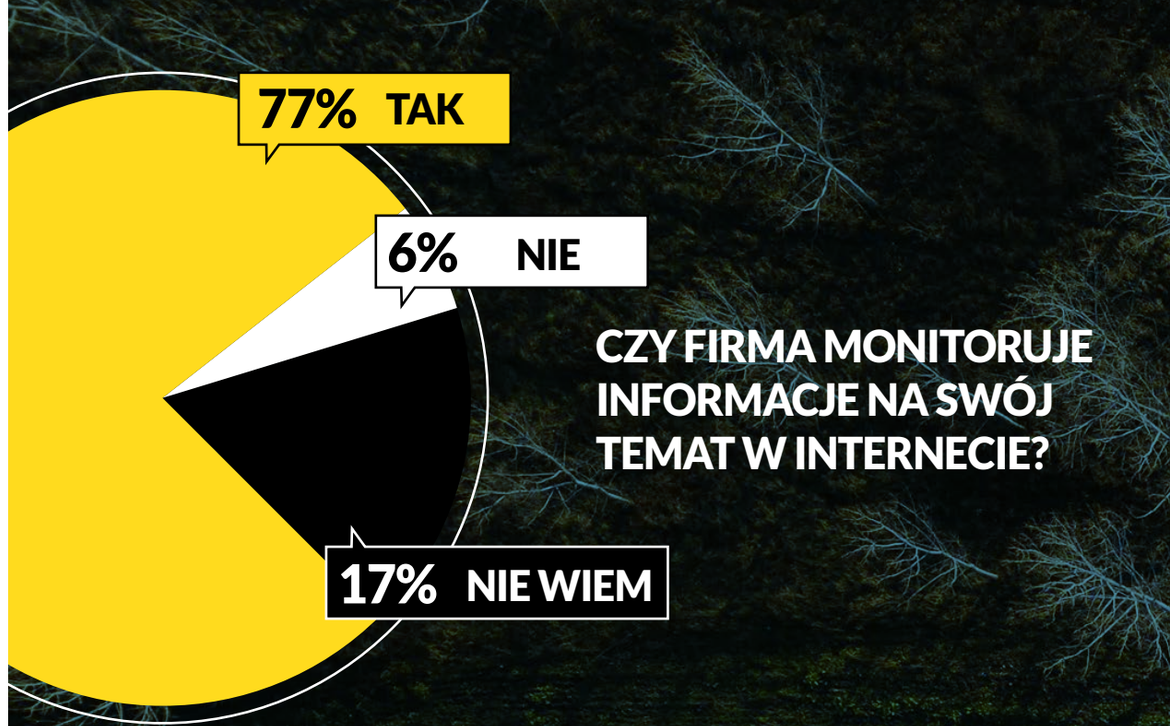
KOMENTARZ

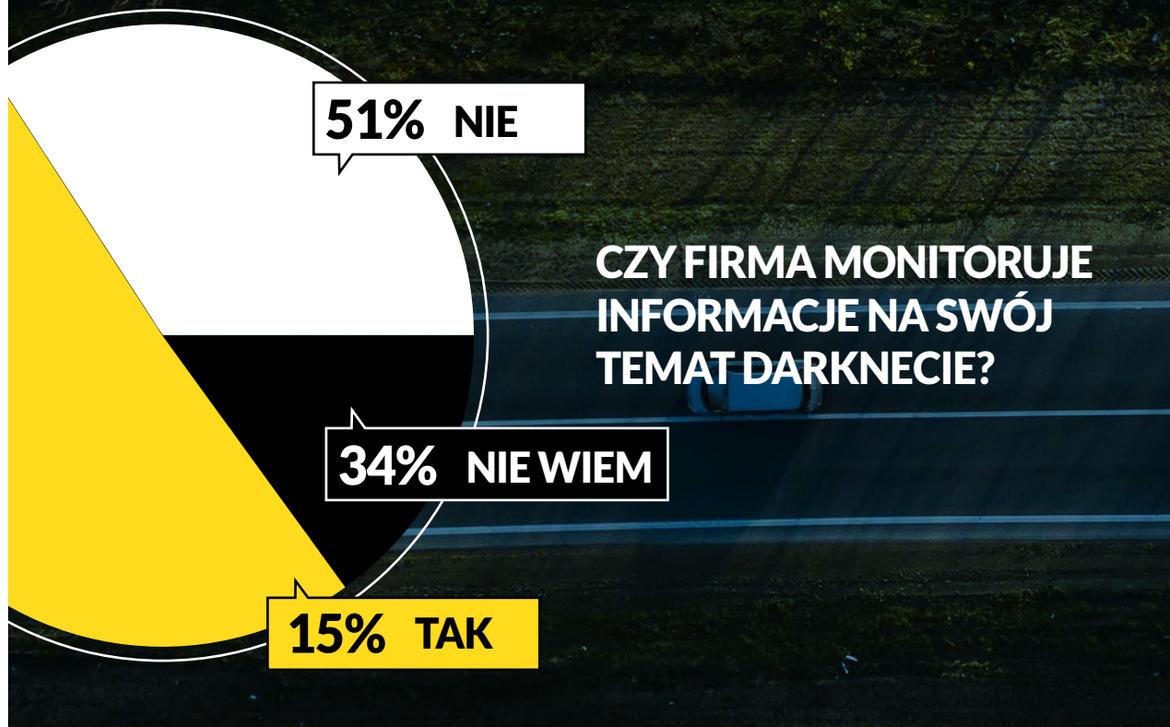
Renata Bilecka,
Technology Engagement Manager,
Samsung

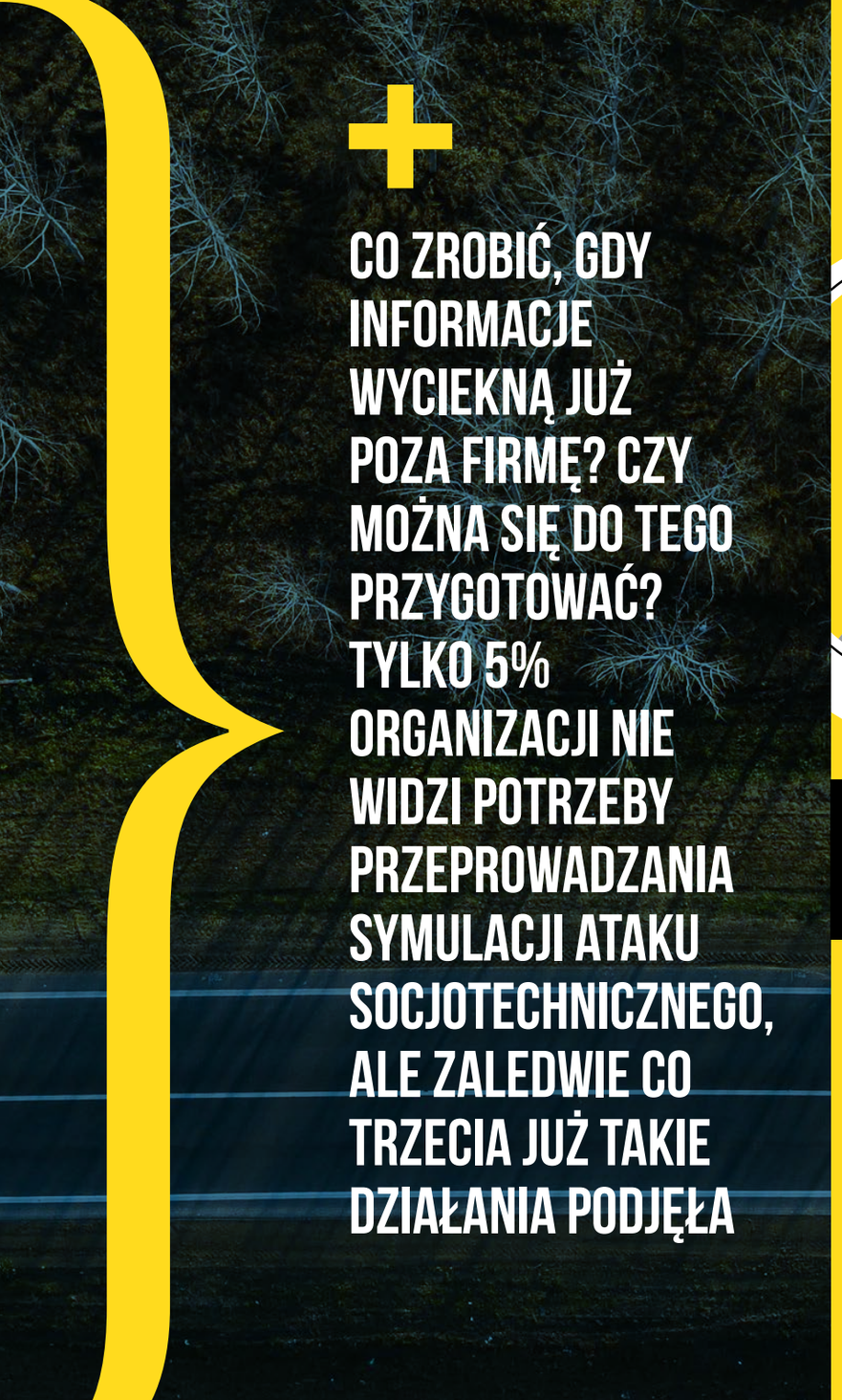
Smartfony cieszą się coraz większym zaufaniem firm. Dzięki nim (i tabletom) wiele procesów biznesowych można uprościć i potocznie mówiąc oderwać od biura. Dziś, gdy dynamika biznesu jest większa niż kiedykolwiek, a do każdej decyzji potrzebne są sprawdzone i dostępne właściwie z każdego miejsca na świecie dane – narzędzia mobilne są kluczowe do osiągnięcia sukcesu. Czy w parze ze swobodą i wygodą pracy idzie bezpieczeństwo? Zapytaliśmy o to uczestników badania Security Excellence, z których ponad 83% potwierdziło, że może swobodnie korzystać m.in. ze służbowej poczty ze swoich urządzeniach mobilnych i że w ich firmach obowiązują jasne polityki bezpieczeństwa IT w zakresie korzystania z urządzeń mobilnych (ponad 73%). Te rezultaty plasują polskich przedsiębiorców na podium w klasyfikacji europejskiej, gdzie ogólne wyniki w zakresie świadomości zagrożeń mobilnych są znacznie niższe (46% w Europie wg badania Blurred World 2018). Mimo tego, nasza produktywność mobilna jest wciąż dość niska – a to z uwagi na fakt, że niewiele działań biznesowych (poza pocztą służbową) realizujemy poprzez urządzenia mobilne – tu wciąż jest spore pole do popisu i podniesienia wydajności pracy zdalnej. Zaledwie 18% naszych respondentów może już dziś w pełni zarządzać swoim biznesem z urządzeń mobilnych. Zarządzanie szeroką gamą procesów i systemów biznesowych z poziomu smartfona niesie ze sobą szerokie wymagania bezpieczeństwa – zarówno ze względu na dobro firmy, która mobilnie przetwarza dane, jak i przepisy RODO uwzględniające także urządzenia mobilne. Tylko 47% uczestników badania przyznało, że korzysta z rozwiązań bezwzględnie wspierających bezpieczeństwo i szyfrowanie służbowych danych, czyli kontenerów. Dlatego cały czas promujemy ideę konteneryzacji.

CZY NA PEWNO ZNASZ PLOTKI NA SWÓJ TEMAT?

REPUTACJA I ZAUFANIE TO WALUTA BIZNESOWA, KTÓREJ KURS STOI NIEZMIENNIE WYSOKO. WARTO WIEDZIEĆ, CZY NP. KONKURENCJA LUB BYŁY PRACOWNIK ROZPUSZCZA NA TEMAT NASZEJ FIRMY ZŁOŚLIWE, SZKODLIWE INFORMACJE. WIĘKSZOŚĆ ORGANIZACJI MONITORUJE TO, CO POJAWIA SIĘ O NICH W INTERNECIE. DARKNET JEDNAK POZOSTAJE DLA PONAD POŁOWY STREFĄ NIEZNANĄ

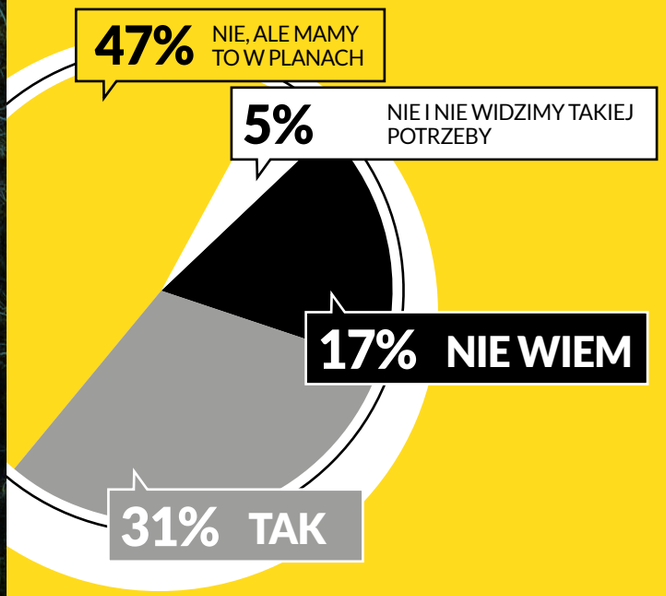






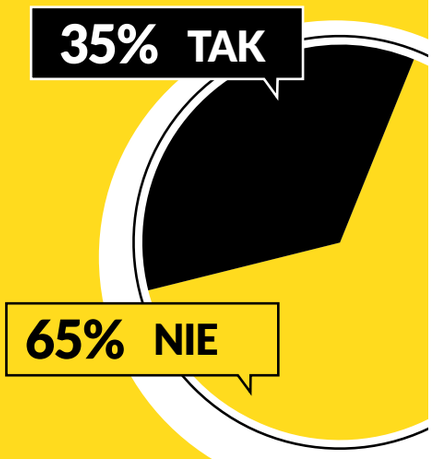
CO ZROBIĆ, GDY INFORMACJE WYCIEKNĄ JUŻ POZA FIRMĘ? CZY MOŻNA SIĘ DO TEGO PRZYGOTOWAĆ? TYLKO 5% ORGANIZACJI NIE WIDZI POTRZEBY PRZEPROWADZANIA SYMULACJI ATAKU SOCJOTECHNICZNEGO, ALE ZALEDWIE CO TRZECIA JUŻ TAKIE DZIAŁANIA PODJĘŁA

CZY FIRMA KIEDYKOLWIEK PRZEPROWADZIŁA ZEWNĘTRZNĄ SYMULACJĘ ATAKU SOCJOTECHNICZNEGO?



WIĘKSZOŚĆ FIRM, MIMO ŚWIADOMOŚCI ZAGROŻEŃ ZWIĄZANYCH Z BRAKIEM ODPOWIEDNIEGO PRZESZKOLENIA, WCIĄŻ NIE PRZEZNACZA BUDŻETU NA EDUKACJĘ PRACOWNIKÓW W ZAKRESIE OCHRONY DANYCH – DOTYCZY TO ZARÓWNO PRACOWNIKÓW TECHNICZNYCH JAK I NIETECHNICZNYCH

CZY ORGANIZACJA POSIADA OSOBNY BUDŻET NA EDUKACJĘ PRACOWNIKÓW W KONTEKŚCIE BEZPIECZEŃSTWA I OCHRONY DANYCH?



KOMENTARZ

Piotr Konieczny,
CISO, Niebezpiecznik.pl

Brak budżetu na szkolenie pracowników to fatalna informacja. Większość współczesnych ataków rozpoczyna się od phishingu, czyli socjotechniki na pracownikach. To pracownik jest pierwszą linią obrony i „białkowym firewallem" który może wykryć atak. A pracownika trzeba szkolić. I to nie raz, a regularnie. Dobrym pomysłem są nie tylko suche szkolenia (prezentacje) ale również symulacje prawdziwych ataków. Dlatego pocieszające jest to, że aż 47% firm ma to w planach. Pytanie skąd wezmą na to środki...

Badanie zostało przeprowadzone przez CIONET i Digital Excellence wśród ok. **170** menedżerów odpowiedzialnych za obszar bezpieczeństwa


DIGITAL EXCELLENCE
CIONET
WWW.SECURITYEXCELLENCE.PL
cisco
dimension data
FORTINET
MARUTA\ NETIA
Niebezpiecznik
SAMSUNG
TREND MICRO
zscaler