intel liczy się to co w środku™

BEZPIECZEŃSTWO IT W DUŻYCH FIRMACH W POLSCE 2016

7,71/10
średnia ocena poziomu bezpieczeństwa IT wg menedżerów IT w dużych firmach w Polsce

27%
firm odnotowało incydent naruszenia bezpieczeństwa w ciągu ostatnich 6 miesięcy

40%
nie ma przygotowanego scenariusza awaryjnego na wypadek cyberataku

62%
wykorzystuje do uwierzytelniania tylko hasło

50%
planuje zwiększenie wydatków na bezpieczeństwo

Krzysztof Jonak
Dyrektor Intela
w regionie Europy Środkowo-Wschodniej

Cyfrowa rewolucja wkroczyła do każdej dziedziny życia. Za sprawą miliardów urządzeń podłączonych do sieci, milionów aplikacji i systemów, dostęp do informacji stał się szybszy i łatwiejszy niż kiedykolwiek wcześniej. Czerpiemy z tego w życiu prywatnym i w biznesie. Niestety ceną, jaką płacimy ze te przywileje, są zagrożenia, których do niedawna nawet sobie nie wyobrażaliśmy. W ciągu zaledwie 5 lat radykalnie zmieniły się metody, którymi posługują się sprawcy naruszeń, ich motywacje, a przede wszystkim skala działania.

W tym roku Intel podjął się przeprowadzenia badania w 250 dużych firmach działających na terenie Polski, Węgier, Rumunii i Czech. Wyniki, które szczegółowo prezentujemy w niniejszym raporcie, prowokują do ważnych pytań. Na ile firmy są przygotowane, by stawić czoła coraz bardziej zaawansowanym i przebiegłym technikom przestępców? Czy w strategiach uwzględniają te elementy systemu bezpieczeństwa, które odnoszą się do czynnika ludzkiego? Czy sięgają po innowacyjne rozwiązania służące uwierzytelnianiu, czy też pozostają przy metodach z minionych dekad? Te pytania nabierają szczególnego znaczenia w obliczu takich zjawisk, jak powszechna migracja ku chmurze obliczeniowej, eksplozja mobilności czy bezprecedensowy przyrost urządzeń przemysłowych podłączonych do sieci.

Zachęcam do zapoznania się z raportem, z nadzieją, że zawarte w nim wnioski, a także rekomendacje udzielone przez ekspertów Intela i Intel Security przyczynią się do podniesienia bezpieczeństwa w Państwa firmach.

Badanie zostało przeprowadzone przez Ipsos na zlecenie Intela w kwietniu i w maju 2016 roku. Wzięło w nim udział 80 respondentów z Polski, 50 z Rumunii, 70 z Węgier i 50 z Czech - decydentów IT z firm zatrudniających ponad 150 pracowników. Przedsiębiorstwa zaproszone do badania reprezentują wszystkie główne sektory gospodarki, w tym sektor publiczny.

STAN BEZPIECZEŃSTWA FIRM W OPINII POLSKICH MENEDŻERÓW IT:

- „Jesteśmy dobrze zabezpieczeni”
- „Nie notujemy znaczących incydentów naruszenia bezpieczeństwa”
- „Chcemy zwiększyć wydatki na ochronę przed atakami”

(NIE)BEZPIECZNY OPTYMIZM?

Większość polskich menedżerów IT deklaruje, że stosowane w ich firmach rozwiązania zapewniają wysoki, a nawet bardzo wysoki poziom bezpieczeństwa informatycznego. Co ciekawe, optymizm ten nie wyróżnia Polaków na tle menedżerów IT z innych krajów regionu.

7,71/10

Średnia ocena poziomu bezpieczeństwa IT wg osób, które są za nie odpowiedzialne w przypadku naszego kraju.

WYZWANIA BEZPIECZEŃSTWA

1

Poszerza się spektrum urządzeń i systemów, które mogą być celem ataków. Są to m.in. urządzenia mobilne, wearables i składniki Internetu rzeczy.

2

Działy IT są odpowiedzialne za kompleksową ochronę infrastruktury IT, która składa się z wielu elementów.

3

Firmy stają przed wyzwaniem egzekwowania polityki bezpieczeństwa obejmującej prywatne urządzenia pracowników (Bring Your Own Device).

4

Dominujące w polskich firmach tradycyjne, jednopoziomowe metody uwierzytelniania nie chronią w wystarczającym stopniu.

ŚREDNIA OCENA POZIOMU BEZPIECZEŃSTWA IT

8,14 Czechy

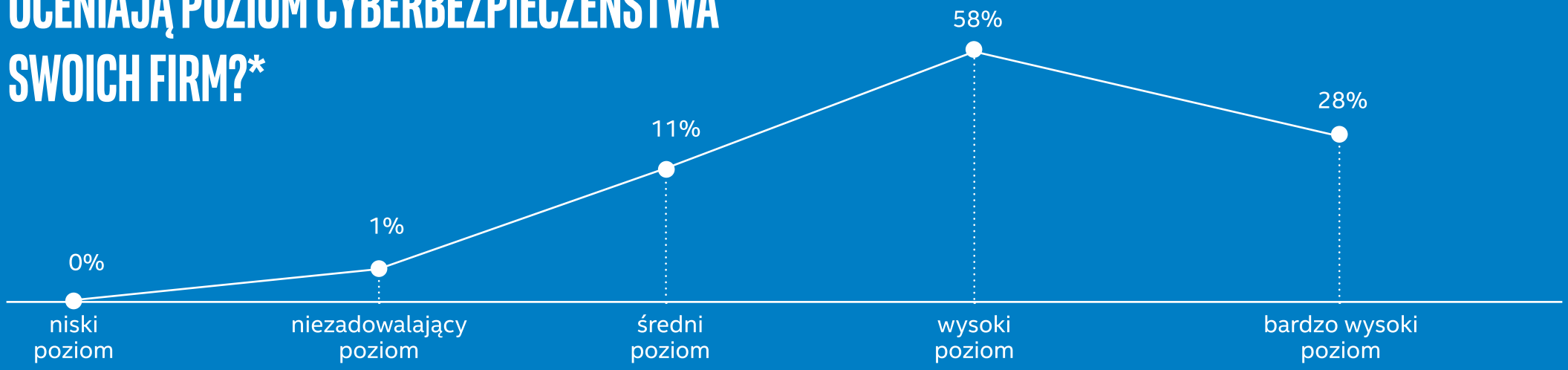
7,74 Rumunia

7,71 Polska

7,13 Węgry

Eksperci zarządzający IT w firmach nie utożsamiają jednak deklarowanego wysokiego poziomu zabezpieczeń z przekonaniem o gotowości odparcia wszystkich ataków ze strony cyberpodziemia. Dominuje zdroworozsądkowe przekonanie – to nie jest kwestia „czy", lecz „kiedy" nastąpi atak. Osoby odpowiedzialne za bezpieczeństwo IT podchodzą do tego zagadnienia strategicznie, starając się alokować dostępne środki tak, aby zabezpieczać kluczowe obszary, a w razie incydentu – minimalizować straty i szybko niwelować skutki.

JAK POLSCY MENEDŻEROWIE IT OCENIAJĄ POZIOM CYBERBEZPIECZEŃSTWA SWOICH FIRM?*



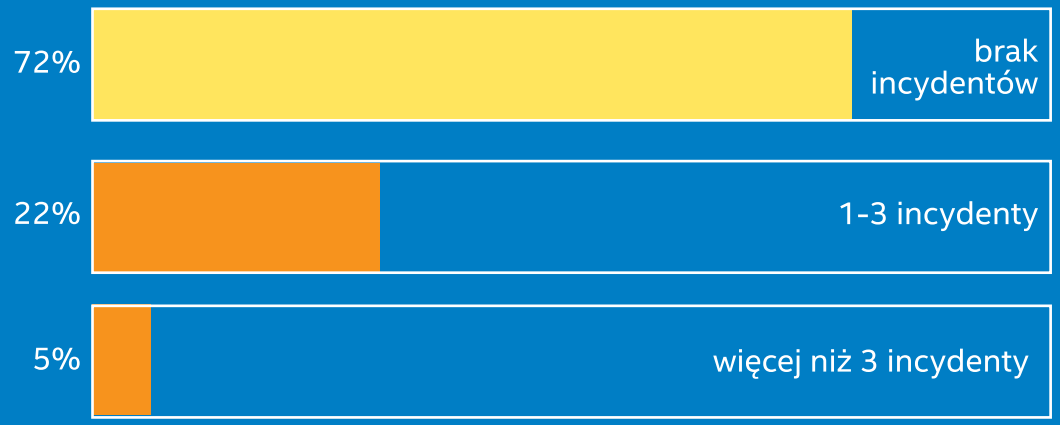
*Ze względu na przyjęte zaokrąglenia (<0,5) nie wszystkie wyniki sumują się do 100%.

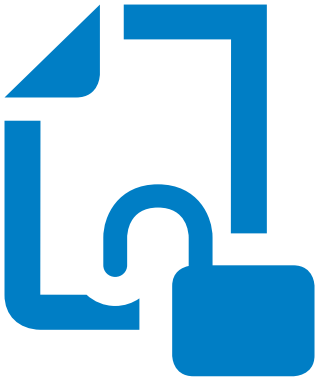
JAK W PRAKTYCE SPRAWDZAJĄ SIĘ STOSOWANE ZABEZPIECZENIA?

Polskie przedsiębiorstwa są celem cyberprzestępców, a decydenci IT są świadomi, że ich systemy zabezpieczeń mogą być podatne na ataki.

27%

polskich firm przyznało, że w ciągu ostatniego półrocza odnotowało incydent naruszenia bezpieczeństwa, z czego część - więcej niż trzy takie zdarzenia.





Firmy z regionu mają podobne statystyki dotyczące incydentów naruszenia bezpieczeństwa – takie przypadki zdarzyły się w ciągu minionego półrocza aż w 36% organizacji w Czechach, 29% na Węgrzech i 18% w Rumunii.

Znacznie mniejszy odsetek firm przyznaje się do poniesienia uszczerbku wskutek wycieku danych – na pytanie o ten rodzaj incydentów twierdząco odpowiedziało zaledwie 4% menedżerów IT z Polski.

94%

ankietowanych menedżerów IT twierdzi, że ich firma nie odnotowała wycieku danych w ciągu ostatnich 6 miesięcy

GOTOWI NA CZARNY SCENARIUSZ?

Tylko 60% przedsiębiorstw w Polsce ma przygotowany scenariusz na wypadek cyberataku. Te statystyki wyglądają inaczej w grupie firm, które określiły swój poziom bezpieczeństwa jako wysoki lub bardzo wysoki – ponad 70% z nich przygotowało plan działania w obliczu ataku cyberprzestępców. Na tle regionu wyróżniają się Czechy, w których największy odsetek (84%) przedsiębiorstw opracował taką procedurę.

40%

firm w Polsce nie ma przygotowanego scenariusza postępowania na wypadek incydentu naruszenia bezpieczeństwa

OŚRODEK DECYZYJNY

Firmy mają coraz bardziej złożone środowiska IT, fizyczne i wirtualne, korzystają z chmury prywatnej i publicznej, infrastruktury mobilnej. Wyzwaniem staje się efektywne i optymalne kosztowo zarządzanie bezpieczeństwem tak różnorodnych zasobów. Zdecydowana większość organizacji decyduje się na centralne zarządzanie polityką bezpieczeństwa IT w ramach całej struktury, jedynie 14% dużych firm nie korzysta z tego typu mechanizmów, pozostawiając egzekwowanie polityki na poziomie indywidualnych departamentów/oddziałów.

86% firm ma scentralizowany mechanizm ustalania polityki bezpieczeństwa IT

BEZPIECZEŃSTWO DANYCH

FIRMA CENTRALNIE ARCHIWIZUJE DANE

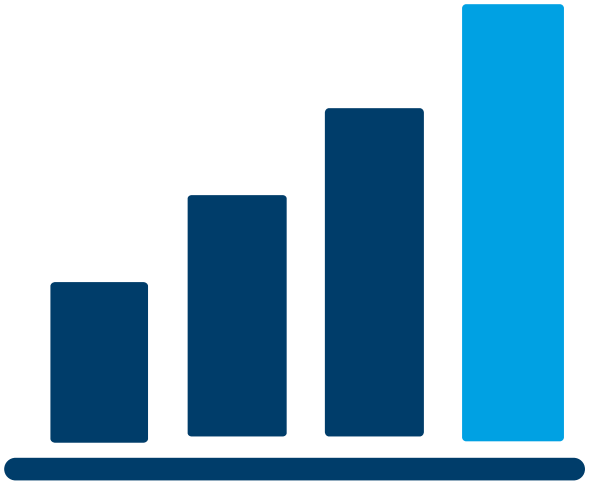
Polityka centralizacji ma odzwierciedlenie w podejściu do archiwizacji danych. Aż w 89% przedsiębiorstw działających w Polsce są ustanowione centralne reguły archiwizowania danych, a tylko w 11% archiwizowanie odbywa się na poziomie poszczególnych stacji/użytkowników. W regionie objętym badaniem Węgry są największym zwolennikiem. centralnego archiwizowania danych.

96% Węgry

92% Rumunia

89% Polska

88% Czechy



BUDŻETY W GÓRĘ

„Na zabezpieczenia można wydać dowolną sumę, ale bezpieczeństwa nie można kupić”

To prawda doskonale znana osobom zarządzającym IT. Niemniej, jak wykazuje badanie, decydenci mają świadomość, że bezpieczeństwo nie jest polem, w którym można pozwolić sobie na oszczędności. Co drugie przedsiębiorstwo w Polsce zamierza zwiększyć nakłady na bezpieczeństwo IT w ciągu najbliższych dwóch lat! Druga połowa deklaruje, że do 2018 roku utrzyma budżety na obecnym poziomie.

50%

firm w Polsce zamierza zwiększyć wydatki na bezpieczeństwo IT do 2018 roku

Rosnąca liczba urządzeń, jakimi się otaczamy (laptopy, smartfony, Smart TV, składniki Internetu rzeczy, wearables itp.), daje hakerom nowe pole działania. Na koniec 2015 r. na rynku było ok. 3,3 mld smartfonów z dostępem do Internetu[1]. Z badań McAfee Labs (dział badawczy Intel Security) z marca 2016 roku wynika, że w ciągu 6 miesięcy poprzedzających publikację tych analiz aż 3 miliony urządzeń zostało zaatakowanych przez malware pochodzący ze sklepów z aplikacjami. Cyberprzestępcy wykorzystują również fakt, że pracownicy używają prywatnych urządzeń do wykonywania obowiązków zawodowych i łączą się za ich pośrednictwem z firmowymi sieciami.

OBWIESZENI BACKDOORAMI

Według danych firmy ABI Research, do 2019 roku na świecie będzie używanych ponad 780 mln urządzeń typu smartwatch. Same w sobie być może nie są łakomym kąskiem dla cyberprzestępców, jednak synchronizujące się z tymi gadżetami aplikacje w smartfonach mogą stać się nowym celem ataków. Pozyskane informacje o zwyczajach czy lokalizacji użytkownika mogą uwiarygodnić hakerów, np. podczas prowadzenia ataków phishingowych (podstępnego wyłudzania danych użytkownika).

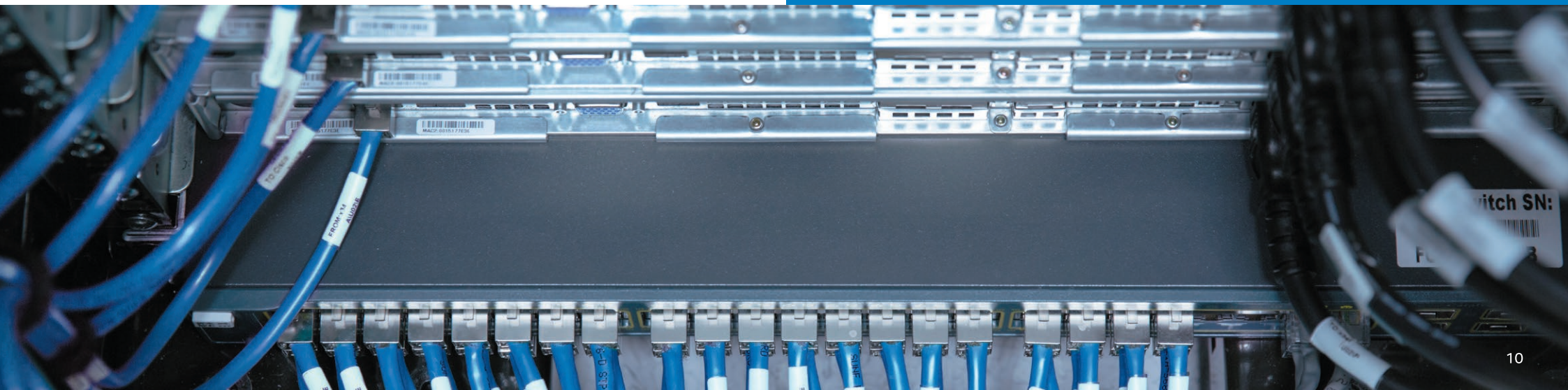
[1] Źródło: McAfee Labs Threads Predictions 2016.

PRZESTĘPCY ZAGLĄDAJĄ POD SYSTEM

Specjaliści zwracają uwagę na fakt, że w najbliższych latach należy spodziewać się także upowszechnienia nowego rodzaju zagrożeń – ataków na warstwę sprzętową. Coraz częściej za cel obierany jest kod, który zarządza pracą danego urządzenia poniżej systemu operacyjnego (firmware, BIOS/UEFI). Taki atak może doprowadzić np. do całkowitego unieruchomienia sprzętu lub otworzyć drogę do uderzenia w system operacyjny. W 2015 roku głośnym echem odbiły się doniesienia o działalności grupy przestępczej, która stworzyła i skutecznie wykorzystywała narzędzia umożliwiające m.in. podmianę firmware'u dysków twardych czy routerów. Z kolei członkowie innej grupy zaoferowali prawdopodobnie pierwsze na świecie komercyjne narzędzie umożliwiające rootkitowy atak na UEFI, czyli następcę BIOSu w świecie PC.

RANSOMWARE, CZYLI KUP SWOJE PLIKI

Wszystko wskazuje na to, że jednym z najdynamiczniej rozwijających się „segmentów rynku" będą działania z wykorzystaniem oprogramowania ransomware i towarzyszące im żądania okupu. Polegają one na zdalnym zaszyfrowaniu plików na dyskach ofiary czy uniemożliwieniu normalnego dostępu do systemu operacyjnego. Przewiduje się, że celem takich ataków staną się zwłaszcza instytucje finansowe, dla których kluczowa jest ciągłość działania. Według analiz McAfee Labs, złośliwe oprogramowanie szyfrujące dane Crypto Wall 3 wypracowało dla swoich twórców ponad 325 mln USD przychodu z zapłaconych okupów.



TO NIE JEST TEORIA SPISKOWA

Już samo sformułowanie „zmowa aplikacji” (app collusion) brzmi niepokojąco, ale musimy się z nim oswoić – McAfee Labs zaobserwowało takie działania już w ponad 5 tys. wersji aplikacji mobilnych. Cyberprzestępcy wiążą ze sobą kilka aplikacji, aby skoordynować ataki i przechwycić dane użytkownika, przejąć pliki czy zainstalować dodatkowe oprogramowanie. Dla firmy mogą z tego płynąć poważne konsekwencje: kradzież informacji, pieniędzy czy tzw. nadużycie usługi, kiedy zainstalowana aplikacja bez wiedzy użytkownika uzyskuje rozszerzone uprawnienia, mogąc przejąć kontrolę nad usługą systemową i otrzymywać polecenia od innych aplikacji, aby koordynować szkodliwe działania.

WIRUSY XXL

Kolejnym szybko rozwijającym się trendem cyberprzestępczym są makrowirusy, które do replikowania wykorzystują język programowania makr w popularnych aplikacjach. Dołączają swój kod najczęściej do dokumentów pakietu Office. Liczba nowych próbek makrowirusów stale rośnie, nawet o 42% kwartalnie. Na ogół atakują sieci korporacyjne poprzez kampanie spamowe.

ŚWIAT UCIEKA DO CHMURY

Migracja do środowisk chmurowych jest globalnym trendem. Według badań* przeprowadzonych przez McAfee Labs, dział badawczy Intel Security, wśród 1 200 szefów IT na całym świecie, w perspektywie 16 miesięcy aż 80% budżetów działów informatycznych będzie wydatkowanych na rozwiązania chmurowe! Już dzisiaj prawie każda duża firma korzysta w pewnym zakresie z chmury prywatnej, publicznej lub hybrydowej. Na tym tle polscy menedżerowie IT ostrożnie inwestują w migrację do cloudu.

34% działających w Polsce przedsiębiorstw korzysta z rozwiązań chmurowych. Jest to charakterystyczne dla naszego regionu – w Czechach odsetek ten wynosi 44%, na Węgrzech 36%, najmniejszy zaś jest w Rumunii - 28%.

Według uczestników badania, w Polsce najpopularniejsza jest chmura prywatna, ale zgodnie ze światowymi trendami częste staje się także wykorzystanie chmury hybrydowej.

* Raport "Blue Skies Ahead" The State of Cloud Adoption, Intel Security, 2016.

34% firm w Polsce korzysta z chmury

- 44%
- 36%
- 34%
- 28%

Z JAKIEGO RODZAJU CHMURY KORZYSTA FIRMA?*

	PRYWATNA	HYBRYDOWA	PUBLICZNA
Polska	56%	26%	19%
Węgry	60%	24%	16%
Rumunia	57%	21%	21%
Czechy	41%	36%	23%

GŁÓWNE OBAWY DOTYCZĄCE CHMURY

Obawy o bezpieczeństwo składowanych danych i zgodność z regulacjami to główne czynniki, które powstrzymują firmy przed szerszym wykorzystaniem środowisk chmurowych – nie tylko w Polsce. Eksperci Intel Security odnotowują rosnące zaufanie do chmury – w skali globalnej aż o 77% w porównaniu do ubiegłego roku – jednak nadal zaledwie 13% firm gotowych byłoby na migrację danych poufnych. Wyzwaniem stojącym przez dostawcami technologii jest więc edukowanie i wskazywanie właściwych metod ochrony dla środowisk chmurowych. Wyzwaniem dla menedżerów IT jest rozprzestrzenianie się tzw. szarej strefy IT, czyli nieautoryzowanego przez kierownictwo wykorzystania przez działy biznesowe rozwiązań chmurowych. Często przywoływanym przykładem są usługi telekonferencyjne dostępne w chmurze, których użycie, niepoprzedzone weryfikacją bezpieczeństwa, ściąga ryzyko na systemy IT przedsiębiorstwa.

*Ze względu na przyjęte zaokrąglenia (<0,5) nie wszystkie wyniki sumują się do 100%.

Nowe procesory Intel Xeon – szybsze i wydajniejsze przetwarzanie w chmurze

Rodzina procesorów Intel® Xeon® E5 zapewnia wyższą wydajność przetwarzania w chmurze dzięki o 20% większej liczbie rdzeni i ilości pamięci podręcznej w porównaniu z poprzednią generacją.[2] Ponadto nowe procesory Intel Xeon obsługują szybszą pamięć i obejmują inne zintegrowane technologie przyspieszające przetwarzanie szeregu obciążeń serwera, sieci i pamięci masowej. Zapewniają także udoskonalenia w zakresie bezpieczeństwa, takie jak izolowanie obciążeń, egzekwowanie reguł bezpieczeństwa i szybsza kryptografia – to wszystko w celu zapewnienia skuteczniejszej ochrony danych.

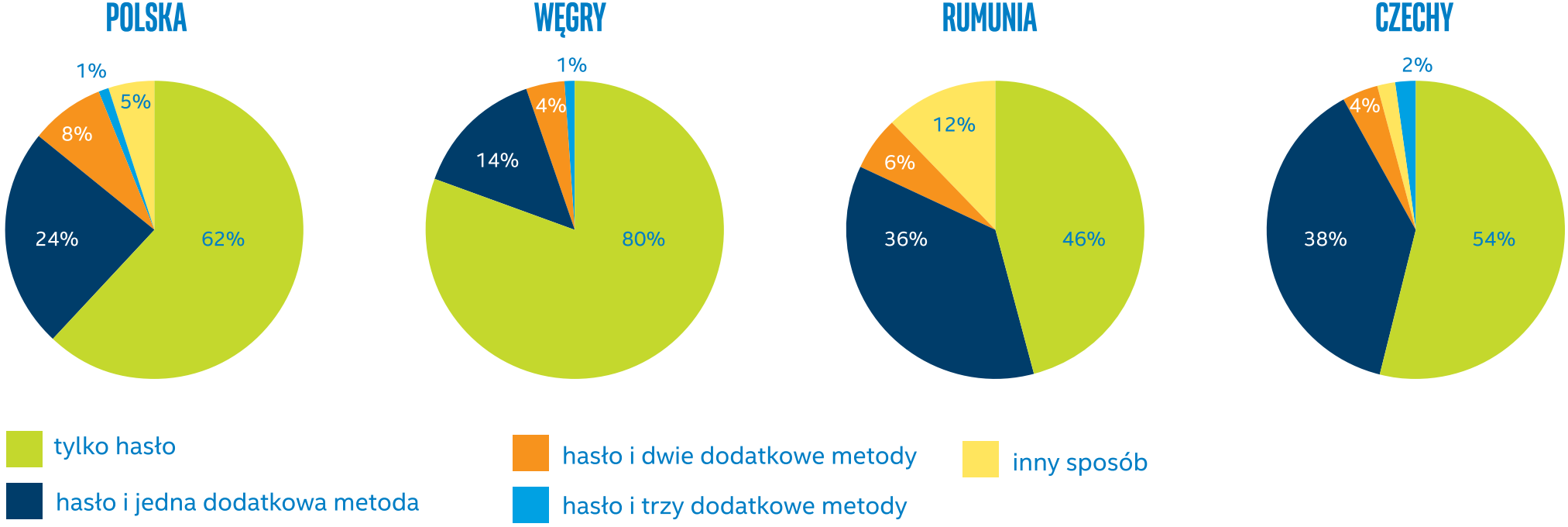
[2]Rodzina procesorów Intel® Xeon® E5-2600 (22C, 55M Cache) w porównaniu z rodziną Intel® Xeon® E5-2600 v3 (18C, 45M Cache).

UWIERZYTELNIANIE I ZARZĄDZANIE DOSTĘPEM

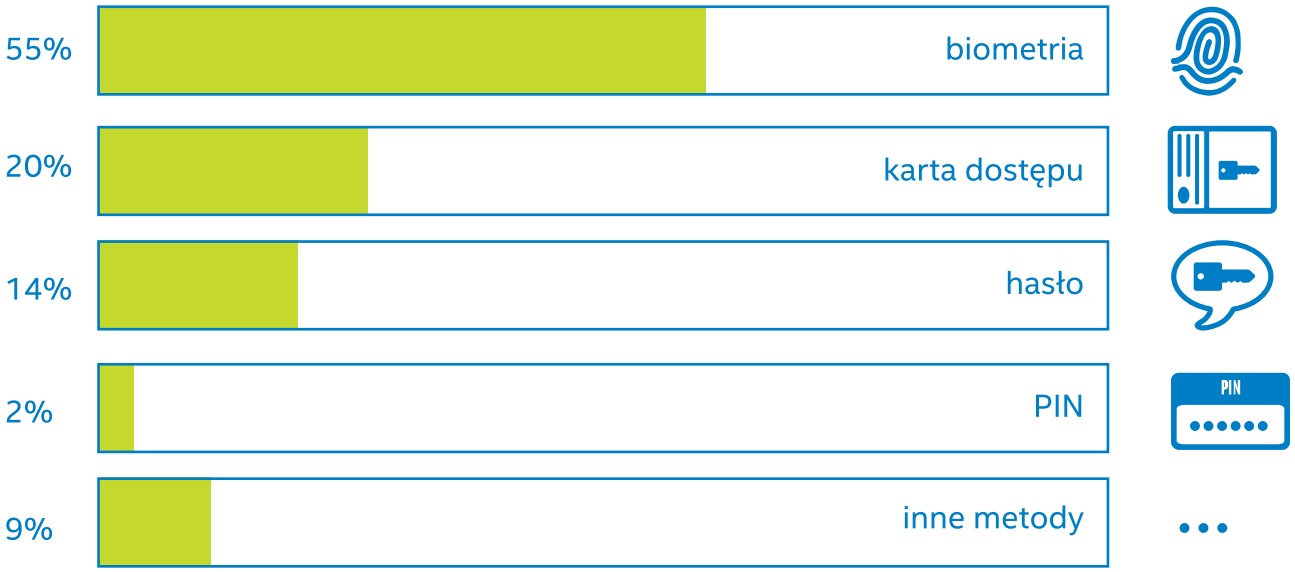
Najsłabszym elementem systemu bezpieczeństwa jest człowiek i jego działanie. Przedsiębiorstwa mają złożone polityki dostępu do zasobów i danych, ale często zapominają o dość oczywistym ogniwie tego łańcucha – należytej ochronie samych urządzeń końcowych. W Polsce wciąż 62% przedsiębiorstw używa tylko jednego i to najmniej doskonałego stopnia zabezpieczeń w uwierzytelnianiu użytkownika – hasła. Zaledwie co czwarta firma wymaga jeszcze drugiego poziomu weryfikacji, zaś tylko 8% – hasła i dwóch dodatkowych metod. To zdecydowanie za mało przy takiej skali zagrożeń. Na Węgrzech zabezpieczenie zasobów tylko hasłem jest jeszcze częstsze – stosuje je aż 80% przedsiębiorstw.

62% przedsiębiorstw używa tylko jednego stopnia zabezpieczeń w uwierzytelnianiu użytkownika – hasła.

METODY IDENTYFIKACJI STOSOWANE W FIRMIE*



NAJBEZPIECZNIEJSZE METODY UWIERZYTELNIANIA WEDŁUG POLSKICH MENEDŻERÓW IT



55%

decydentów IT uważa biometrię za najbezpieczniejszą metodę weryfikacji tożsamości

Faktyczny stan zabezpieczeń różni się od stanu świadomości menedżerów. Większość z nich zdaje sobie sprawę ze słabości zabezpieczania zasobów jedynie hasłem. Ponad połowa uważa, że najbezpieczniejszą metodą potwierdzenia tożsamości użytkownika jest biometria.

Według raportu SANS Institute „IT Security Spending Trends", w 2016 r. na pierwszym miejscu wydatków firm na obszar bezpieczeństwa znalazły się właśnie narzędzia związane z dostępem i uwierzytelnianiem. Wyzwaniem jest dostosowanie rozwiązań potwierdzenia tożsamości do stopnia ryzyka związanego z dostępem do systemu czy przeprowadzeniem transakcji. Jednak wszystkie rozwiązania powinny być łatwe w użyciu, tak aby pracownicy czy klienci nie zaczęli ich omijać. Użytkownicy chętnie korzystają z rozwiązań, które np. zwalniają ich z obowiązku pamiętania kolejnych haseł. Polityka wewnętrznego bezpieczeństwa w dojrzałych organizacjach jest coraz częściej spójna z polityką chroniącą bezpieczeństwo transakcji z klientami.

*Ze względu na przyjęte zaokrąglenia (<0,5) nie wszystkie wyniki sumują się do 100%.

OCHRONIĆ TOŻSAMOŚĆ

Cyberprzestępcy mają coraz bardziej zaawansowane metody łamania haseł i doskonalą swoje umiejętności socjotechniczne. Ich celem najczęściej jest przechwycenie danych logowania i zdobycie dostępu do firmowych komputerów i zasobów.

Nie da się zbudować infrastruktury całkowicie odpornej na zagrożenia. W dobie powszechnej mobilności i niezliczonej ilości sprzętu, z jakiego korzystamy w celach prywatnych i zawodowych, kluczowe staje się skuteczne zabezpieczenie dostępu do urządzeń końcowych. Nie mniej istotne w tym kontekście jest zapewnienie wymiany informacji i współpracy między elementami sieci zabezpieczeń.

Z badania przeprowadzonego przez Intela w Polsce wynika, że większość przedsiębiorstw stosuje jednoelementową weryfikację tożsamości użytkownika za pomocą hasła, mimo świadomości, iż jest to najmniej skuteczny sposób ochrony. Taki stan rzeczy to zapewne wypadkowa różnych czynników – przyjętej w danej organizacji praktyki, dostępnych rozwiązań technicznych, zakładanych kosztów ich wdrożenia i utrzymania czy wreszcie określonych doświadczeń z incydentami bezpieczeństwa.

Praktyka wykorzystywania kilkuznakowych haseł zmienianych raz na kilka miesięcy (a czasem rzadziej) jest nieadekwatna do skali obecnych zagrożeń oraz ewentualnych szkód, jakie może wyrządzić nieautoryzowany dostęp do zasobów przedsiębiorstwa.

Arkadiusz Krawczyk
Dyrektor Regionalny w Intel Security Poland

intel Security

TRZY POZIOMY UWIERZYTELNIANIA

Rolą dostawców jest wpierać klientów w dążeniu do minimalizowania ryzyka cyberataku. Jednym z ciekawszych rozwiązań w tym obszarze jest wspomagana sprzętowo technologia wielopoziomowego uwierzytelniania Intel Authenticate. Z jej zalet można korzystać na komputerach wyposażonych w procesory Intel Core vPro szóstej generacji. Technologia ta umożliwia bezpieczne logowanie do komputerów i firmowej sieci dzięki wykorzystaniu kliku elementów identyfikacyjnych: „to, co znasz" (kod PIN), „to, co masz" (urządzenie mobilne użytkownika) oraz „to, kim jesteś" (biometria). Wielopoziomowy model uwierzytelniania Intel Authenticate przenosi koncepcję ochrony danych na wyższy poziom wygody korzystania i bezpieczeństwa.

Dane do uwierzytelniania użytkownika przechowywane i obsługiwane są całkowicie w warstwie sprzętowej, poza udziałem systemu operacyjnego. Administratorzy mogą elastycznie zarządzać procesem uwierzytelniania użytkowników w firmie, odejmując lub dodając kolejne poziomy identyfikacji.

Nowe narzędzia do wykrywania zagrożeń i zapobiegania incydentom pomagają rozwiązać problem związany z narastającym wciąż zagrożeniem ze strony cyberprzestępców. Skuteczność zabezpieczeń można poprawić poprzez udoskonalenie współpracy, komunikacji i automatyzacji między różnymi obszarami w obrębie organizacji, a przede wszystkim pomiędzy istniejącymi już w firmie zabezpieczeniami.

Krzysztof Jonak
Dyrektor Intela
w regionie Europy Środkowo-Wschodniej

INSTRUKCJA BEZPIECZEŃSTWA

Tradycyjne zabezpieczenia przechowują dane uwierzytelniania w warstwie oprogramowania, przez co łatwiej je przechwycić. Intel Authenticate przechowuje te informacje w warstwie sprzętowej, zmniejszając ryzyko wycieku. Nowy komputer biznesowy z procesorem Intel Core vPro szóstej generacji zapewnia większe bezpieczeństwo tożsamości użytkownika.

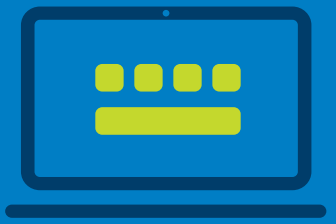
Przykład trzypoziomowej weryfikacji tożsamości z wykorzystaniem mechanizmów Intel Authenticate i komputerów bazujących na procesorach Intel Core vPro szóstej generacji.

1

Uruchomienie specjalnej aplikacji na telefonie (Intel Authenticate Mobile Application), poprzez którą pracownik uwierzytelnia się w komputerze dzięki połączeniu Bluetooth

2

Zeskanowanie odcisku palca w czytniku linii papilarnych na komputerze



3

Wprowadzenie dodatkowego PIN-u (okno do jego wprowadzenia również obsługiwane jest bezpośrednio sprzętowo, poza warstwą systemu operacyjnego). Wyświetlane są cyfry w losowej kolejności, wybiera się je bez użycia klawiatury. Dzięki temu logowanie jest zabezpieczone przed keyloggerami czy tzw. screen scrapingiem.

REKOMENDACJE

BEZPIECZEŃSTWO

- Bezpieczeństwo IT musi stać się priorytetem dla wszystkich firm. To obszar, w którym nie warto oszczędzać.
- Każda organizacja powinna być świadoma tego, że może stać się ofiarą cyberprzestępców. Pozostaje tylko pytanie, kiedy to nastąpi i jakie przyniesie skutki.
- Wszystkie firmy powinny opracować **scenariusz awaryjny na wypadek cyberataku.**
- Bezpieczeństwo IT to **nie tylko oprogramowanie**, ale także **sprzęt.** Wiele technologii pomagających zabezpieczyć dane znajduje się w urządzeniach.
- Warto inwestować w najlepsze dostępne technologie, które ochronią cenne firmowe dane. Wymiana starego sprzętu na nowy wiąże się nie tylko z oszczędnościami czy większą wydajnością, ma także pozytywny wpływ na poziom bezpieczeństwa IT.
- Przedsiębiorstwa powinny w skuteczny i kompleksowy sposób zabezpieczać wszystkie elementy infrastruktury – również **urządzenia końcowe** (komputery i smartfony pracowników).
- Kluczowe jest zapewnienie **wymiany informacji i współpracy** między poszczególnymi elementami sieci zabezpieczeń – analiza zachowań użytkowników i procesów zachodzących w firmie pozwala na szybkie wykrycie wszelkich nieprawidłowości.

AKTUALNE TRENDY

- Ewolucja rozwiązań chmurowych sprawiła, że **cloud computing** stanowi dziś **bezpieczne i niezawodne uzupełnienie** tradycyjnej infrastruktury IT.
- Nie da się uniknąć pewnych trendów, takich jak Bring Your Own Device czy chmura. Niewątpliwie wpływają one pozytywnie na **wydajność pracowników i całej organizacji**, firmy muszą jednak być właściwie przygotowane na ich wprowadzenie.

UWIERZYTELNIANIE

- Nowoczesne rozwiązania sprzętowe jak Intel Authenticate pozwalają **lepiej zabezpieczyć proces uwierzytelniania pracowników**, a przez to skuteczniej chronić dane firmy.

BEZPIECZEŃSTWO IT W EUROPIE ŚRODKOWO-WSCHODNIEJ

intel liczy się to co w środku

MANAGEROWIE IT ZBYT OPTYMISTYCZNIE OCENIAJĄ BEZPIECZEŃSTWO SWOICH FIRM

7,64/10 Średnia ocena bezpieczeństwa firm w regionie według managerów IT.

- 7,71/10
- 8,14/10
- 7,13/10
- 7,74/10

28% przedsiębiorstw doświadczyło w ostatnich 6 miesiącach naruszenia bezpieczeństwa IT (ataków złośliwego oprogramowania, nieautoryzowanego dostępu do danych, wycieku danych itp.)

1/3 dużych firm w regionie nie ma przygotowanego scenariusza awaryjnego na wypadek cyberataku.

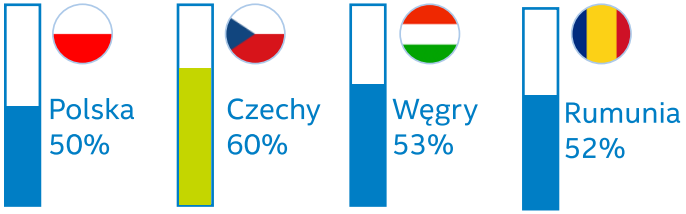
NISKI POZIOM BEZPIECZEŃSTWA FIRMOWYCH KOMPUTERÓW

62% przedsiębiorstw w regionie zabezpiecza dostęp do komputerów **jedynie za pomocą hasła.**

- 62%
- 54%
- 80%
- 46%

Jednocześnie tylko 14% badanych uważa hasło za najbezpieczniejszą metodę uwierzytelniania. Managerowie IT najbardziej ufają **BIOMETRII** (to najlepsze zabezpieczenie wg **55%** badanych).

Ponad **POŁOWA** firm w regionie planuje w najbliższych latach zwiększyć wydatki na bezpieczeństwo IT.



JEŚLI CHMURA... TO PRYWATNA

35% dużych firm w regionie korzysta z usług chmurowych.

- 34%
- 44%
- 36%
- 28%

Najbardziej popularna jest chmura prywatna.

	Prywatna	Hybrydowa	Publiczna
Polska	56%	26%	19%
Czechy	41%	**36%**	**23%**
Węgry	**60%**	24%	16%
Rumunia	57%	21%	21%