CYBERBEZPIECZEŃSTWO POLSKICH FIRM 2021

#CyberMadeInPoland

BADANIE COMPUTERWORLD

CYBERBEZPIECZEŃSTWO POLSKICH FIRM 2021

Praca zdalna, cyfryzacja procesów w kolejnych sektorach rynku, (r)ewolucja Przemysu 4.0. Wszystko to sprawia, że cyberbezpieczeństwo przestało być jedynie problemem technicznych dla działów IT, a stało się niezbędnym elementem kalkulacji ryzyka biznesowego.

Zwiększona przestrzeń ataków oraz coraz bardziej wyrafinowane scenariusze ich zastosowań (np. ransomware) wymagają przedsięwzięcia konkretnych środków, aby właściwie zabezpieczyć zasoby informatyczne, a szerzej zapewnić ciągłość działania i dostępność usług IT nowoczesnej organizacji.

#CyberMadeInPoland

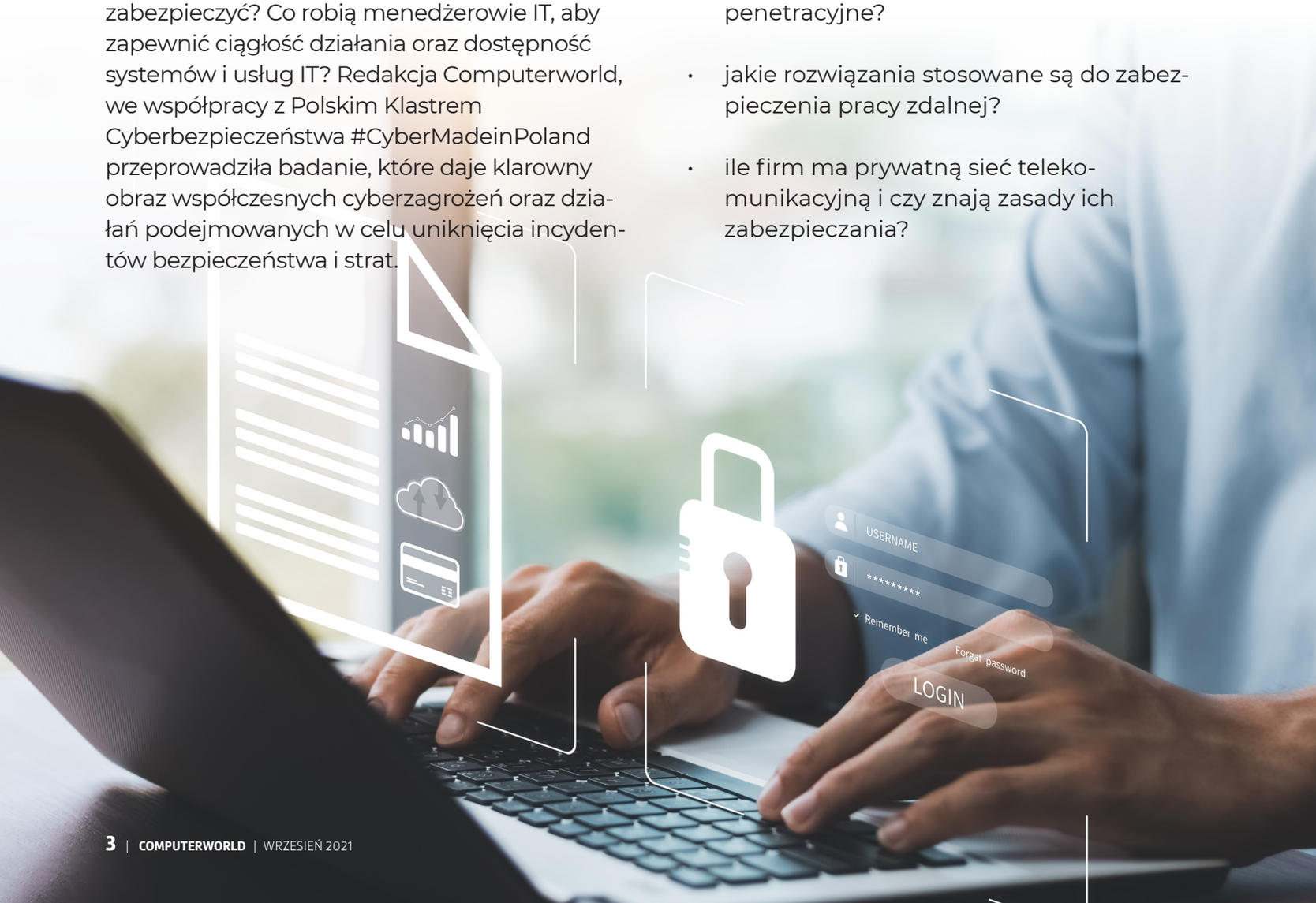
EXECUTIVE SUMMARY

W ostatnim roku co trzecia firma musiała zmierzyć się z naruszeniami cyberbezpieczeństwa. Najczęstszym zagrożeniem było działanie szkodliwego oprogramowania, w tym ransomware oraz klasyczne ataki sieciowe na infrastrukturę. W celu ochrony systemów i danych firmy sięgają po szereg rozwiązań technicznych – od typowych procedur bezpieczeństwa takich jak aktualizacje oprogramowania i regularny backup po rozwiązania z zakresu szyfrowania danych oraz monitorowania stacji roboczych pracowników.

Z jakimi incydentami cyberbezpieczeństwa zmagają się rodzime przedsiębiorstwa i instytucje publiczne? Jakie rozwiązania techniczne i organizacyjne stosują firmy, aby się przed nimi zabezpieczyć? Co robią menedżerowie IT, aby zapewnić ciągłość działania oraz dostępność systemów i usług IT? Redakcja Computerworld, we współpracy z Polskim Klastrem Cyberbezpieczeństwa #CyberMadeinPoland przeprowadziła badanie, które daje klarowny obraz współczesnych cyberzagrożeń oraz działań podejmowanych w celu uniknięcia incydentów bezpieczeństwa i strat.

Z raportu dowiesz się m.in.:

- czego dotyczyły zauważone incydenty cyberbezpieczeństwa?
- które rozwiązania techniczne i organizacyjne wpływają na bezpieczeństwo firmy?
- w jaki sposób organizacje zapewniają ciągłość działania oraz dostępność systemów i usług IT?
- jakie działania podejmują firmy, aby uniknąć incydentów bezpieczeństwa i strat?
- ile przedsiębiorstw korzysta z usług informatyki śledczej, ile prowadzi testy penetracyjne?
- jakie rozwiązania stosowane są do zabezpieczenia pracy zdalnej?
- ile firm ma prywatną sieć telekomunikacyjną i czy znają zasady ich zabezpieczania?



Robert Siudak,
CEO, Polski Klaster Cyberbezpieczeństwa
#CyberMadeInPoland

Z perspektywy roku 2021 możemy powiedzieć wprost: cyberbezpieczeństwo stanowi obecnie jedno z kluczowych wyzwań dla biznesu. Jednocześnie w ostatnich latach słyszymy wciąż powtarzane dwie tezy dotyczące stanu IT-sec w polskich firmach:

- *Brakuje budżetów na cyberbezpieczeństwo.*
- *Skala zagrożeń wciąż rośnie i jest coraz gorzej.*

Spróbuję Państwa przekonać, że obydwa stwierdzenia są jednak mitami. Jest w nich ziarno prawdy, ale przy bliższej analizie widać, że mają niewiele wspólnego z rzeczywistością polskich przedsiębiorców.

Po pierwsze, firmy alokują budżety tam, gdzie widzą kluczowe elementy dla swojej działalności. Jeśli CISO lub administrator IT mówi, że budżetu na cyberbezpieczeństwo brakuje, to tak naprawdę znaczy, że zarząd nie uznaje bezpieczeństwa danych i procesów za kluczową kwestię dla prowadzenia swojej firmy. Nawet najlepszy wynik finansowy przedsiębiorstwa w kolejnym roku nie wygeneruje w tym wypadku budżetu na IT-sec. Zmienić może to jedynie edukacja zarządu – samodzielna albo przyspieszona, niestety, np. poprzez udany cyberatak. Potwierdza to niniejszy raport. 86% ankietowanych przez nas przedstawicieli polskich firm uważa za ważne lub kluczowe regularne tworzenie kopii zapasowych oraz stosowanie oprogramowania antywirusowego. Jednocześnie to właśnie regularny backup (88%) oraz antywirus (85%) były wskazywane jako najczęściej obecne w badanych przedsiębiorstwach. Konkluzja jest prosta: tam gdzie jest świadomość potrzeby i wagi zagadnienia, pojawia się budżet na zakup rozwiązań lub usług.

Po drugie, skala i liczba cyberataków globalnie rzeczywiście rosną rok do roku. Nie oznacza to jednak, że każde z przedsiębiorstw w Polsce odczuwa ten wzrost w taki sam sposób. Kluczem do zrozumienia staje się tu analiza ryzyka oraz wpływu potencjalnych incydentów na funkcjonowanie przedsiębiorstwa. Dopiero opierając się na zrozumieniu realnej roli cyberbezpieczeństwa w swojej firmie, właściciele powinni podejmować decyzje oraz działania. Niestety, jak pokazały prezentowane w raporcie wyniki badania, podejście takie wciąż nie jest powszechne. Jedynie 41% firm prowadzi analizę wpływu na biznes (Business Impact Analysis, BIA), a 53% realizuje analizy ryzyka związane z ciągłością działania. Jednocześnie prawie wszystkie przedsiębiorstwa wdrożyły polityki związane z RODO (93%). Pokazuje to, że wymogi regulacyjne stanowią wciąż kluczowy impuls stymulujący przedsiębiorców do działania w zakresie procedur związanych z cyberbezpieczeństwem.

Podsumowując wyniki zaprezentowane w raporcie, to edukacja i regulacja są systemowymi działaniami, które pomogą zwiększyć cyberbezpieczeństwo polskich firm w kolejnych latach. W ramach Polskiego Klastra Cyberbezpieczeństwa #CyberMadeInPoland działamy aktywnie w obydwu zakresach. Zapraszam Państwa do lektury, a także do współpracy z #CyberMadeInPoland.

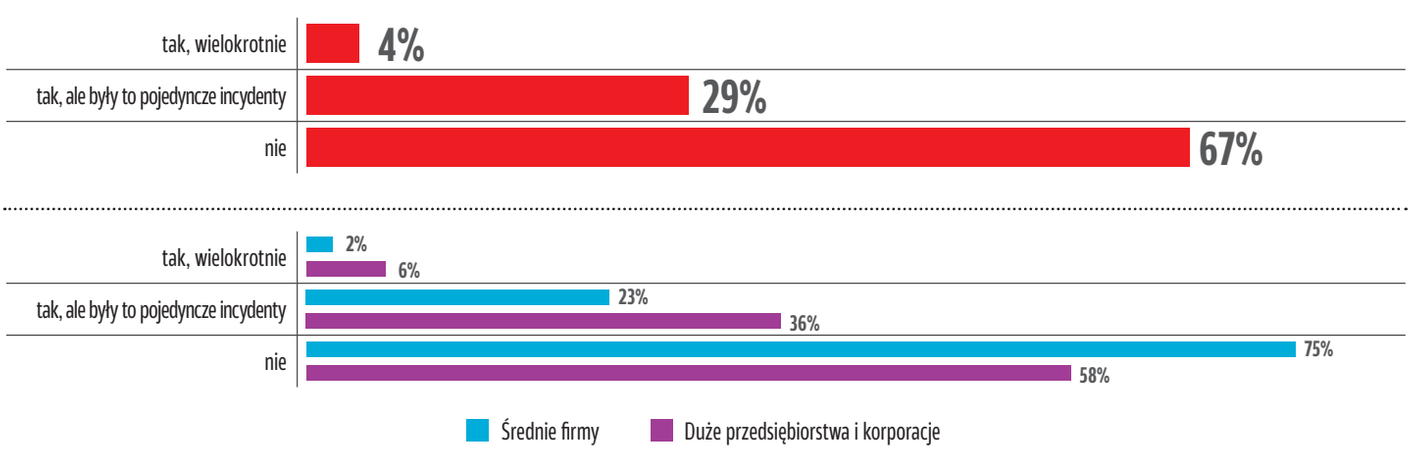
INCYDENTY BEZPIECZEŃSTWA

W ostatnim roku co trzecia firma musiała zmierzyć się z naruszeniami cyberbezpieczeństwa. Z zagrożeniami zauważalnie częściej zmagały się duże przedsiębiorstwa i korporacje, gdzie odsetek ten sięgnął aż 42 proc. Choć zazwyczaj były to pojedyncze incydenty (36% wskazań) to część firm z tej grupy (6%) odnotowała w tym okresie wielokrotne, notoryczne próby ataku na infrastrukturę i systemy IT.

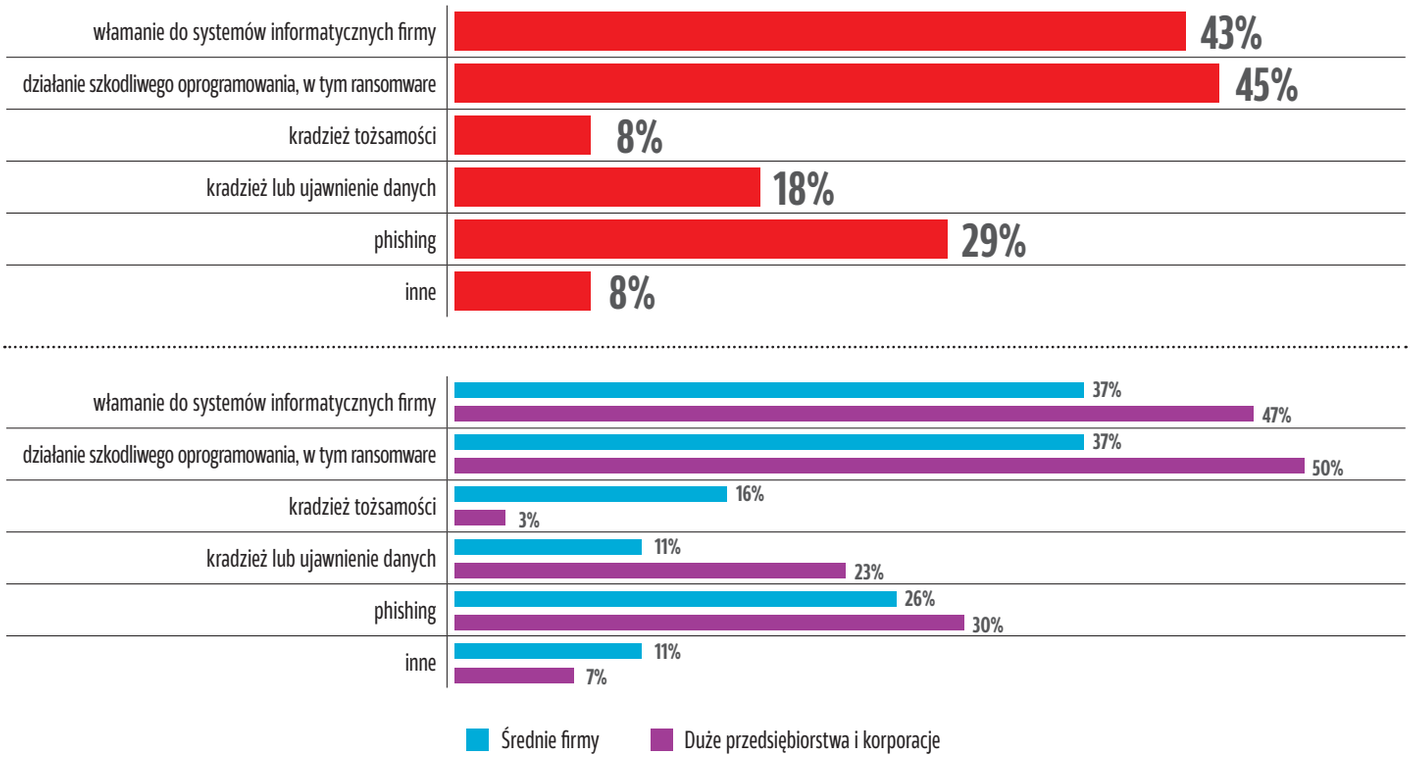
Największym problemem okazuje się być działanie szkodliwego oprogramowania, w tym ransomware. Aż 45 proc. firm zauważyło tego typu zagrożenia w swojej sieci. 43 proc. przedsiębiorstw musiało w ostatnich 12 miesiącach zmierzyć się z włamaniami do systemów informatycznych. Incydenty te były wyraźnie częściej dostrzegane przez duże firmy i korporacje, niż ich mniejszych konkurentów.

Dla wszystkich w ostatnich 12-miesiącach istotnym wyzwaniem okazał się także phishing. Na dostrzeżone próby oszustwa związane z wyłudzeniem informacji wskazało łącznie 29 proc. respondentów. Na liście istotnych zagrożeń cyberbezpieczeństwa znalazła się jeszcze kradzież lub ujawnienie danych. Wśród innych odpowiedzi ankietowanych dominowały zaś incydenty związane z atakami DDoS.

CZY W OSTATNICH 12-MIESIĄCACH FIRMA MIERZYŁA SIĘ Z NARUSZENIAMI CYBERBEZPIECZEŃSTWA?



CZEGO DOTYCZYŁY ZAUWAŻONE INCYDENTY CYBERBEZPIECZEŃSTWA?



Grzegorz Michałek,
współzałożyciel i prezes zarządu,
Arcabit/mks_vir

Wykazane w raporcie wyniki doskonale korespondują z przeprowadzanymi przez specjalistów Arcabit i mks_vir analizami aktywności szkodliwego oprogramowania, szczególnie w kontekście zagrożeń z rodziny ransomware i prób wyłudzania danych (phishing). Nasze doświadczenia dodatkowo wskazują, że głównym wektorem ataku jest poczta elektroniczna, będąca nośnikiem dla ponad 70% prób uruchomienia szkodliwego kodu w atakowanych systemach. W przypadku zagrożeń szyfrujących i wykradających dane należy dodatkowo zaakcentować, że skuteczny atak nie wymaga uzyskania przez malware uprawnień administracyjnych. Nasze analizy pokazują również, że współczesne szkodliwe oprogramowanie, aktywne w polskiej cyberprzestrzeni, jest coraz częściej doskonale przygotowane pod kątem językowym i idealnie wykorzystuje nasze lokalne realia.

W związku z tym nieodpowiednie lub niedostateczne, nieukierunkowane na polski rynek środki ochrony nie są w stanie w czasie rzeczywistym reagować na nowe warianty zagrożeń, co – zwłaszcza w przypadku mniej doświadczonych użytkowników – otwiera łatwy kanał ataków dla cyberprzestępców.

33% wszystkich i aż 42% dużych przedsiębiorstw zmagało się w ostatnim roku z naruszeniami cyberbezpieczeństwa

6% dużych firm doświadczyło wielokrotnych ataków

45% zagrożeń cyberbezpieczeństwa dotyczyło działania szkodliwego oprogramowania

43% firm odnotowało próby włamania do systemów informatycznych

29% ogółu firm zauważyło próby wyłudzenia informacji (phishing)

Karol Suchocki,
Breach Response Manager, Cyber Security Center

Obsługa incydentów związanych z cyberbezpieczeństwem to proces złożony, wymagający współpracy specjalistów wielu dziedzin: IT, bezpieczeństwa, prawa, PR itd. Nasze doświadczenie pokazuje, że coraz więcej firm opracowuje plany ciągłości działania oraz plany odtwarzania po awarii. Wciąż nie jest jednak doceniana wartość planów reakcji na incydenty.

Podczas obsługi incydentów widzimy, że skutkuje to podejmowaniem ad hoc decyzji nieskutecznych, lub wręcz szkodzących rozwiązaniu problemu. Brak takich planów to również brak świadomości tego, jakie faktycznie działania należy podjąć przy konkretnym typie incydentu, jakich specjalistów zaangażować i z jakimi kosztami trzeba będzie się zmierzyć. Krytyczne jest zaplanowanie współpracy z kontrahentami podczas obsługi incydentu. Dotyczy to przede wszystkim dostawców usług IT oraz podmiotów mających dostęp do infrastruktury lub poufnych danych przedsiębiorstwa. Zapewnienie zapisów kontraktowych definiujących odpowiedzialność oraz zasady współpracy w razie incydentu to krok we właściwym kierunku.

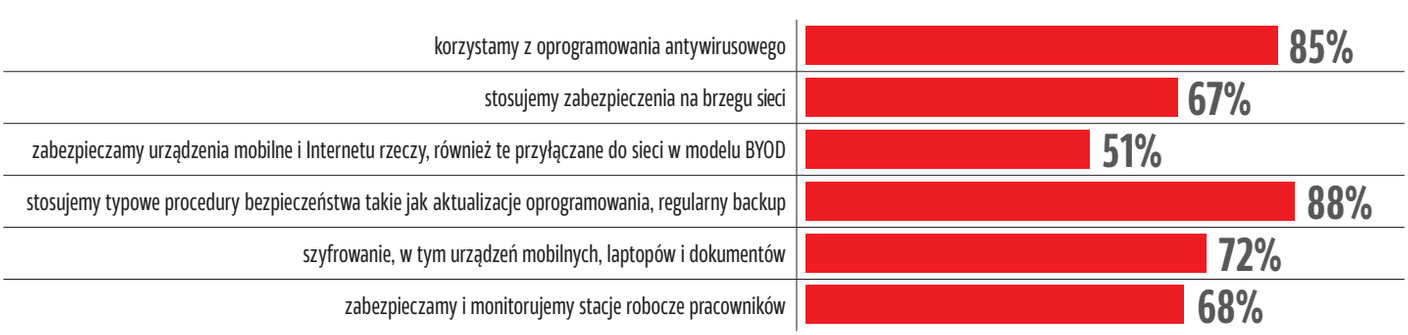
TECHNICZNE ŚRODKI OCHRONY

Firmy stosują szereg komplementarnych rozwiązań technicznych w celu ochrony systemów i danych przed szkodliwym oprogramowaniem. Najważniejszym aspektem ochrony zdaje się być stosowanie typowych procedur bezpieczeństwa takich jak aktualizacje oprogramowania i regularny backup. Zasadę tę, jako punkt wyjścia do zapewnienia cyberbezpieczeństwa, wyznaje 88 proc. ankietowanych przedsiębiorstw. 85 proc. firm korzysta z oprogramowania antywirusowego.

Poziom adopcji innych rozwiązań technicznych w zakresie ochrony informatycznej można uznać nawet jeśli nie za wysoki to na pewno za akceptowalny. 72 proc. ankietowanych przedsiębiorstw wykorzystuje mechanizmy szyfrowania do zabezpieczania danych i dokumentów na urządzeniach mobilnych i laptopach. 68 proc. firm zabezpiecza i monitoruje stacje robocze pracowników.

Co prawda 67 proc. firm stosuje zabezpieczenia na brzegu sieci, ale już tylko co druga zabezpiecza urządzenia mobilne i Internetu rzeczy, w tym te przyłączane do sieci w modelu BYOD. Jak łatwo zauważyć, te kwestie ochrony, choć bardzo istotne z perspektywy cyberbezpieczeństwa całej organizacji, nadal traktowane są przez menedżerów IT nieco po macoszemu.

JAKIE TECHNICZNE ROZWIĄZANIA W CELU OCHRONY PRZED SZKODLIWYM OPROGRAMOWANIEM STOSOWANE SĄ W FIRMIE?



Piotr Wojtasik,
certyfikowany inżynier, Axence

Stosowanie wskazanych w badaniu zabezpieczeń to fundamenty cyberochrony. Świadome organizacje stosują również urządzenia na brzegu sieci, monitorują sieć i użytkowników oraz wdrażają szkolenia pracowników. Niestety, mimo tych środków atakujący często włamują się do firm.

Posiadane rozwiązania umożliwią odpowiednie przygotowanie sieci i stacji roboczych, minimalizując ryzyko popularnych wektorów ataków. Dział IT powinien przygotować takie narzędzia i procedury, które pozwolą zamienić nieszczelny komputer w standardowej konfiguracji w wzmocnioną twierdzę do pracy z wrażliwymi danymi, np. poprzez stosowne blokady i polityki uprawnień. Znając zasady działania najpowszechniejszych ataków malware, ransomware czy phisihingu, możemy blokować lub ograniczać ukryte pobieranie plików, uruchamianie skryptów oraz procesów systemowych, fałszywe linki czy niebezpieczne załączniki. Tak powstają „parasole ochronne", które skutecznie wspierają tradycyjne antywirusy. Tworzenie bezpiecznego środowiska IT od strony użytkownika jest możliwie przy odpowiednim wdrożeniu rozwiązań do zarządzania IT takich jak nasze Axence nVision®.

Należy pamiętać także, że wdrożenie środków ochrony oraz stosowne procedury pozwalają minimalizować straty i kary (np. RODO). Ograniczanie dostępów do zasobów, minimalizacja przetwarzania danych, monitorowanie incydentów, zarządzanie zasobami IT (w tym kontrola aktualizacji oprogramowania), szyfrowana komunikacja oraz praca wg zasady ograniczonego zaufania – to tylko niektóre punkty rozszerzonego elementarza IT.

88% firm stosuje typowe procedury bezpieczeństwa takie jak aktualizacje oprogramowania i regularny backup

85% przedsiębiorstw korzysta z oprogramowania antywirusowego

51% zabezpiecza urządzenia mobilne i Internetu rzeczy

OCENA WAŻNOŚCI ROZWIĄZAŃ TECHNICZNYCH I ORAGANIZACYJNYCH

Wybór środków technicznych nie jest przypadkowy i co więcej prawdopodobnie wcale nie wynika z powtarzanych jak mantra przesłanek o ograniczonych budżetach. Na pytanie o ocenę stopnia ważności rozwiązań technicznych i organizacyjnych pod kątem ich wpływu na cyberbezpieczeństwo firmy ankietowani wymieniali najczęściej te same środki i narzędzia, które stosują w swoich sieciach obecnie.

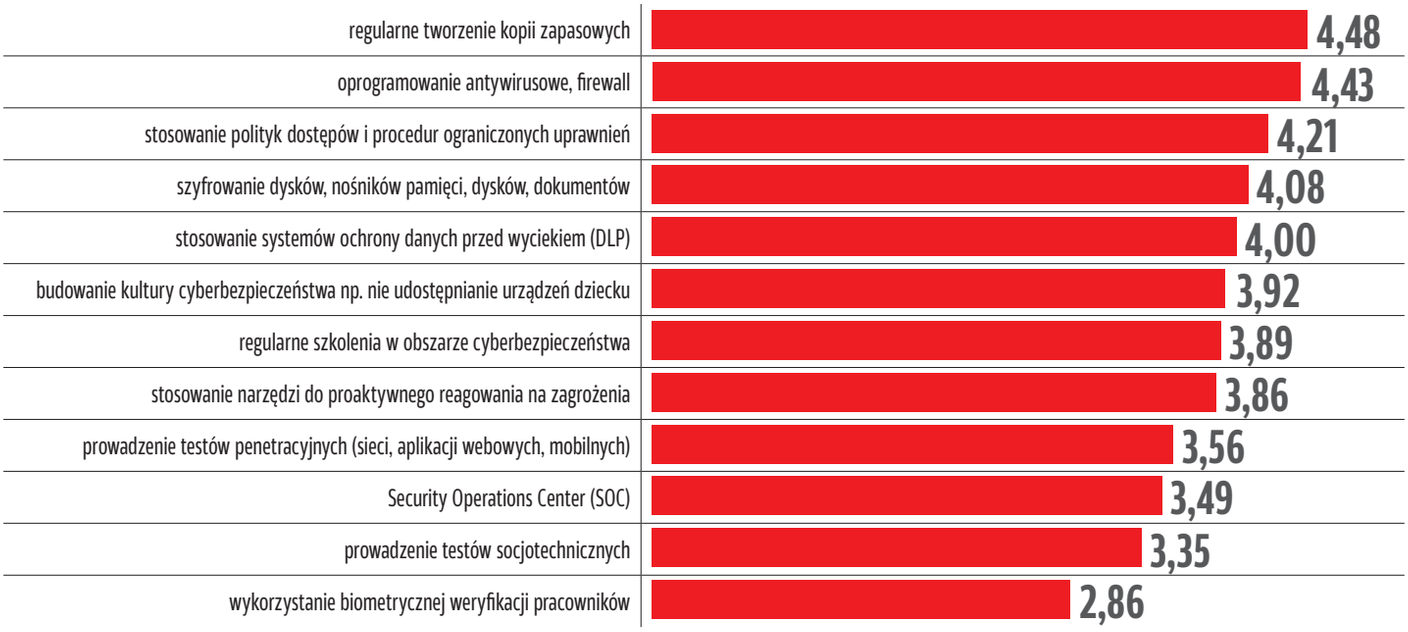
Za niezwykle istotne ankietowani uznali regularne tworzenie kopii zapasowych oraz stosowanie oprogramowania antywirusowego i zapór sieciowych. Środki te jako ważne lub kluczowe dla cyberbezpieczeństwa systemów i danych wskazało odpowiednio po 86% respondentów.

86% ankietowanych uważa za ważne lub kluczowe regularne tworzenie kopii zapasowych oraz stosowanie oprogramowania antywirusowego i zapory sieciowej

80% respondentów wysoko ocenia stosowanie polityk dostępów i procedur ograniczonych uprawnień dla zachowania wymaganego poziomu cyberbezpieczeństwa firmy

OCENA STOPNIA WAŻNOŚCI ROZWIĄZAŃ TECHNICZNYCH I ORGANIZACYJNYCH POD KĄTEM WPŁYWU NA CYBERBEZPIECZEŃSTWO FIRMY

odpowiedzi w skali od 1 do 5, gdzie 1 najmniej istotny, 5 najbardziej ważny



Marek Ujejski,
IT Security Expert, CISM,
CPDSE – COIG

Wyniki ankiety wskazują, że firmy nadal koncentrują się na najprostszych zabezpieczeniach, nawet tych podstawowych. Wskazuje to na fakt, że prawdziwy poziom bezpieczeństwa sektora (zakładając, że stanowią reprezentatywną próbkę) jest bardzo niski. Zamierzone kierunki inwestowania (rozwiązania antywirusowe, backup, sprzętowe zapory sieciowe, zabezpieczenia fizyczne) znacznie wyprzedzają bardziej zaawansowane zabezpieczenia (outsourcing usług zajmujących się bezpieczeństwem, ochrona w chmurze).

W przypadku outsourcingu usług istnieje zasadne domniemanie, że pytanie zostało źle sformułowane, najwyraźniej wiele firm nie kojarzy tego typu usług z rozwiązaniem typu Security Operation Center. Tezę tę potwierdzają moje doświadczenia, mogę na ich podstawie stwierdzić, że w wielu firmach pojęcie to jest nieznane lub błędnie rozumiane. Pozytywne jest to, że firmy potwierdzają zamiar szkolenia swoich pracowników w zakresie bezpieczeństwa.

Zwraca uwagę fakt, że firmy umiarkowanie akcentują potrzebę wykonywania audytów i testów penetracyjnych. Z tym działaniem organizacje zdążyły się już oswoić i oprócz uczestnictwa w szkoleniach widzą potrzebę ich wykonywania.

Usługi bezpieczeństwa, zwłaszcza typu SOC, są wymuszane przepisami prawa i tylko objęcie szerszej kategorii podmiotów klauzulą operatora usługi kluczowej jest w stanie przyspieszyć ten proces.

Za trzeci kluczowy obszar zapewnienia bezpieczeństwa sieciowego ankietowani uznali stosowanie polityk dostępów i procedur ograniczonych uprawnień. Kwestia ta zyskała wysoką notę 4,21 punktów w 5 stopniowej skali ważności. Do istotnych rozwiązań technicznych w tym zakresie respondenci zaliczyli jeszcze szyfrowanie dysków, nośników pamięci, dysków, dokumentów oraz stosowanie systemów ochrony danych przed wyciekiem (DLP). Narzędzia do proaktywnego reagowania na zagrożenia zdają się być ważne, ale już nie kluczowe.

W opinii ankietowanych istotne są również podejmowane działania organizacyjne takie jak budowanie świadomości i zagrożeń oraz kultury cyberbezpieczeństwa w organizacji (np. nie udostępnianie dziecku urządzeń), a także regularne szkolenia w tym obszarze.

Bezpieczeństwo to złożone zagadnienie, które wymaga holistycznego podejścia, również w zakresie testowania wdrożonych środków technicznych i organizacyjnych firmy. Problem w tym, że ankietowani w dość umiarkowany sposób postrzegają konieczność weryfikacji skuteczności stosowanych środków ochrony poprzez prowadzenie testów penetracyjnych (sieci, aplikacji webowych, mobilnych) czy testów socjotechnicznych.

Piotr Kudrys,
Product Owner,
Proget

PROGET

Cyberbezpieczeństwo to jedna z gałęzi, szeroko rozumianego IT, która jest w stanie pochłonąć każdy budżet. Zawsze można wprowadzić jakiś dodatkowy system i procedury, które będą chronić naszych użytkowników oraz nasze dane. Mnogość dostępnych rozwiązań oraz obszarów które zabezpieczają, jest bardzo szeroka i dlatego odpowiednie rozłożenie dostępnych środków jest kluczem do względnie wysokiego poziomu zabezpieczenia danych firmowych.

Ostatnie lata pokazały, że stara teza: „Człowiek jest najsłabszym ogniwem systemu", wciąż jest aktualna. Dlatego większość z zabezpieczeń ocenianych przez respondentów jako kluczowe jest skoncentrowana na użytkownikach i ich urządzeniach. Urządzenia końcowe to najczęstszy cel ataków, więc wysoka ocena ważności rozwiązań dla końcówek jest w pełni uzasadniona i nikogo nie powinna zaskakiwać.

W sytuacji, gdy „mleko już się rozlało", niewiele udaje się zrobić. Pozostaje jedynie żmudna analiza, co mogło zostać narażone i jak poważny był incydent. Między innymi dlatego tak ważne jest odpowiedzialne udzielanie dostępu tylko do danych, które są niezbędne danemu użytkownikowi. To dość prosta metoda ograniczenia potencjalnych szkód, na jakie będziemy narażeni w przypadku skutecznego ataku.

I na koniec nasza ostatnia deska ratunku: kopie zapasowe. W sytuacjach krytycznych tylko one pozwalają przywrócić utracone dane i zachować ciągłość działania procesów biznesowych. Niezaprzeczalnie to regularne tworzenie kopii zapasowych jest filarem, na którym opiera się wiele firm.

Wielu respondentów uważa, że istnienie wydzielonego działu Security Operations Center (SOC) jest ważne z perspektywy cyberbezpieczeństwa (ocena 3,49 punktów w 5-stopniowej skali ważności), ale na jego powołanie i prowadzenie nie zawsze mogą pozwolić sobie wszystkie firmy. Pewnym sposobem na obejście niektórych ograniczeń zdaje się zakup usługi typu SOC na zewnątrz (outsourcing). Tak robi 21 proc. ankietowanych firm.

Ponad 77% ankietowanych uważa za ważne stosowanie narzędzi do proaktywnego reagowania na zagrożenia

21% ankietowanych korzysta z outsourcingowego modelu i kupuje usługi typu Security Operations Center na zewnątrz

CIĄGŁOŚĆ I DOSTĘPNOŚĆ SYSTEMÓW

Od zapewnienia ciągłości działania oraz dostępności systemów IT zależy funkcjonowanie każdej nowoczesnej organizacji. Przestoje generują bezpośrednie koszty, np. związane z niezrealizowanymi zamówieniami, oraz rodzą długofalowe, negatywne konsekwencje dla postrzegania firmy na rynku.

W rezultacie 83 proc. organizacji podejmuje szereg działań mających na celu osiągnięcie pożądanego poziomu dostępności systemów informatycznych. Nawiasem mówiąc: oznacza to, że aż 17 proc. ankietowanych przedsiębiorstw nie podejmuje w tym kierunku żadnych działań.

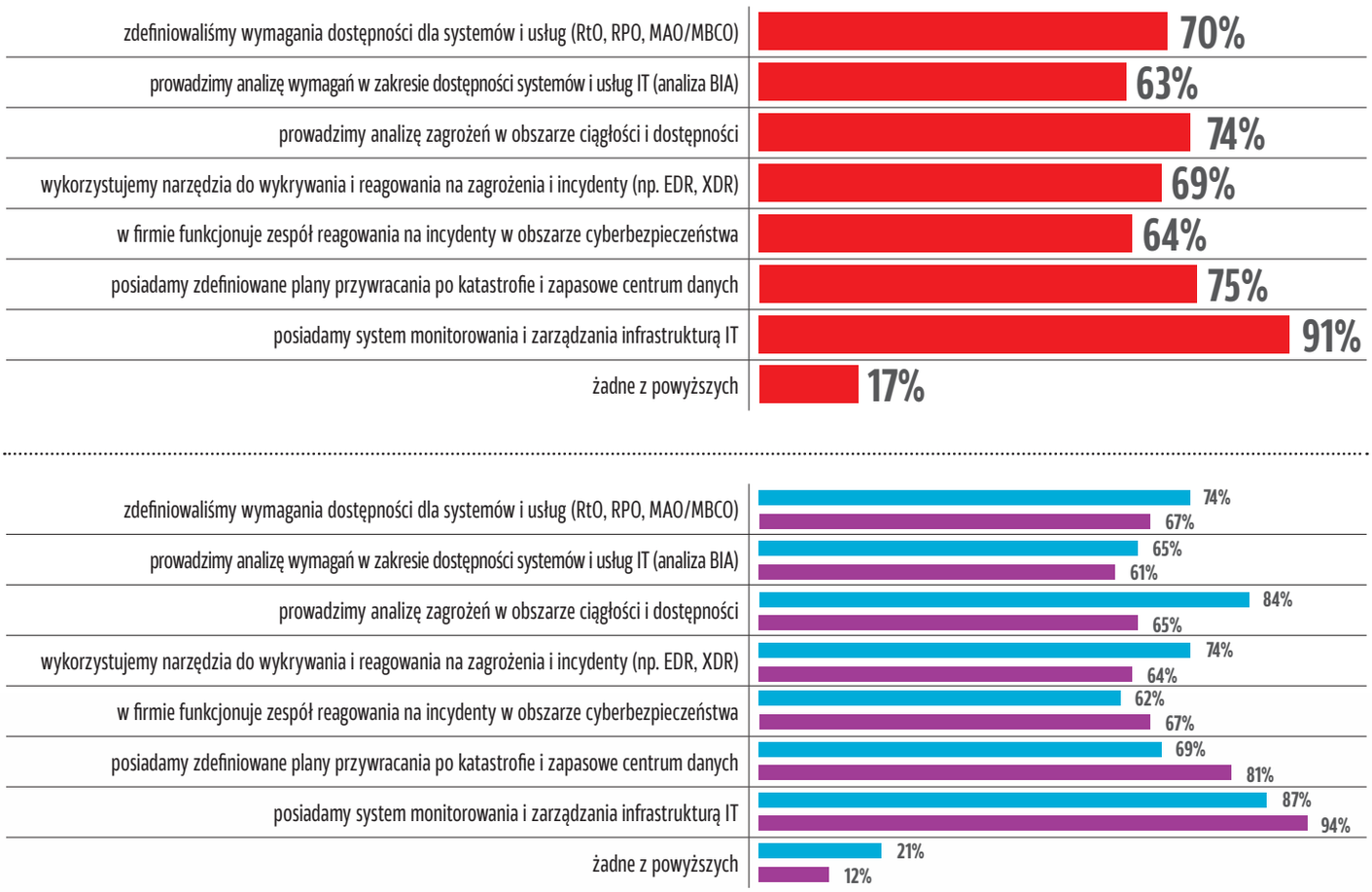
91 proc. firm ma wdrożony system monitorowania i zarządzania infrastrukturą IT. Przeciętnie trzy na cztery (75%) podmioty zdefiniowały plan przywracania po katastrofie, którego kluczowym elementem jest zapasowe centrum danych. W dużych przedsiębiorstwach odsetek ten sięga 81 proc.

70 proc. ogółu i aż 74 proc. średniej wielkości organizacji zdefiniowało wymagania dostępności dla systemów i usług (RtO, RPO, MAO/MBCO). 74 proc. wszystkich firm prowadzi analizę zagrożeń w obszarze ciągłości i dostępności, zaś

63 proc. dokonuje regularnych analiz wymagań w zakresie dostępności systemów i usług IT (analiza BIA).

Kwestie zapewnienia ciągłości działania firmy traktują z należytą powagą, o czym świadczy wysoki poziom adopcji innych rozwiązań i narzędzi z tego obszaru. 69 proc. przedsiębiorstw wykorzystuje narzędzia do wykrywania i reagowania na zagrożenia i incydenty (np. EDR, XDR). W 64 proc. organizacji funkcjonuje dedykowany zespół reagowania na incydenty w obszarze cyberbezpieczeństwa.

W JAKI SPOSÓB FIRMA ZAPEWNIA CIĄGŁOŚĆ DZIAŁANIA ORAZ DOSTĘPNOŚĆ SYSTEMÓW I USŁUG IT?



Marcin Marczewski,
prezes Resilia sp. z o.o.

Resilia
architekci odporności biznesu

Z roku na rok widzimy coraz większe zainteresowanie ciągłością działania i zarządzaniem dostępnością systemów IT. Wyniki badania potwierdzają nasze obserwacje: aż 70% firm posiada zdefiniowane parametry dostępności systemów informatycznych.

Miejmy nadzieję, że pozytywne doświadczenia przedsiębiorstw, które wdrożyły te rozwiązania, spowodują wzrost zainteresowania wśród organizacji, które nie podejmują podobnych praktyk. Na podstawie badania i własnych doświadczeń można zaryzykować stwierdzenie, że część firm nie zdefiniowała wymagań w sposób formalny i nadal wprowadzenie tego typu rozwiązań stanowi dla nich poważne wyzwanie.

Biorąc pod uwagę poziom sformalizowania aspektów zapewnienia ciągłości oraz przygotowania planów odtwarzania po awariach IT, można przypuszczać, że właściwe podejście do określenia wymagań dotyczących ciągłości usług ICT wdrożyło jeszcze mniej firm.

Dodatkowe zapewnienie ciągłości działania stanowią ubezpieczenia. Zwłaszcza w kontekście zabezpieczenia środków finansowych na pokrycie szkód w sprzęcie czy kosztów odtworzenia działalności biznesowej oraz wspierającej ją infrastruktury ICT. Ubezpieczanie się na tego typu okoliczności nie jest jednak powszechne.

W przypadku awarii lub katastrofy sytuacja ta rodzi ryzyko niemożliwych do uniesienia strat finansowych, wizerunkowych czy prawnych, a zauważmy, że tylko 25% firm zaplanowało w budżecie środki na opracowanie planów BCP i DRP.

Firmy, które stawiają na rozwiązania z zakresu ciągłości i dostępności systemów IT, są bardziej konkurencyjne, rozwijają się szybciej i bezpieczniej. Pamiętajmy, że praktyki te przeznaczone są dla wszystkich: korporacji, MŚP, organizacji publicznych i non profit.

91% firm zaimplementowało system monitorowania i zarządzania infrastrukturą IT

75% ogółu i 81% dużych przedsiębiorstw ma zdefiniowane plany przywracania po katastrofie i zapasowe centrum danych

70% firm zdefiniowało wymagania dostępności dla systemów i usług (RtO, RPO, MAO/MBCO)

FORMALNE ASPEKTY ZARZĄDZANIA BEZPIECZEŃSTWEM

Kwestie związane z zapewnieniem ciągłości działania i dostępności systemów informatycznych wymagają umocowania na poziomie formalnych dokumentów. Punktem wyjścia jest sformalizowanie najbardziej podstawowych procesów, w tym zdefiniowanie w dokumentach procedur wynikających z regulacji prawnych i standardów branżowych.

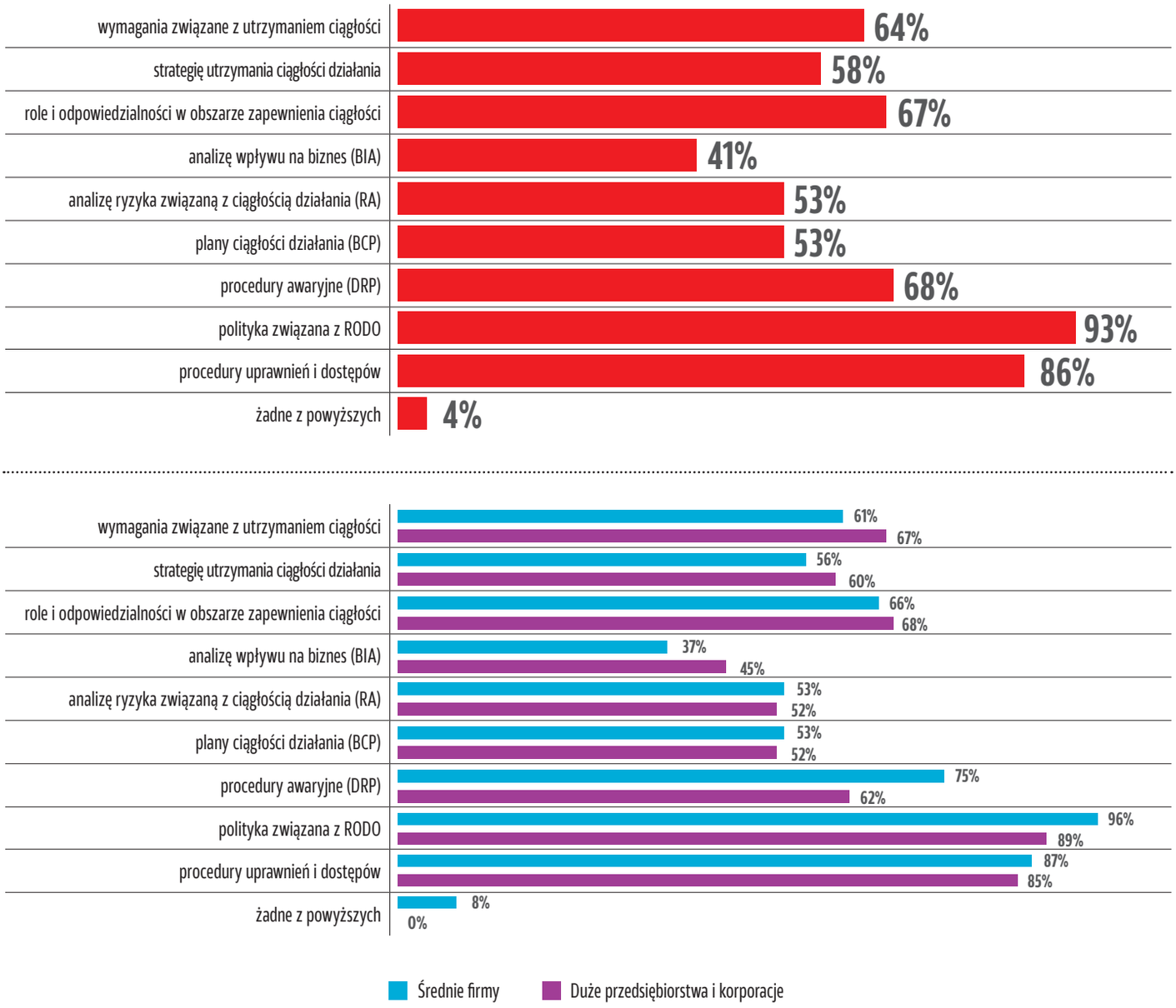
W rezultacie aż 93 proc. ankietowanych przedsiębiorstw przygotowało, zatwierdziło i wdrożyło politykę ochrony danych osobowych (RODO). Wymagania te zostały nałożone przez prawo, a wpływ na wysoki poziom adopcji regulacji RODO mają zapewne wysokie kary za ich nieprzestrzeganie.

86 proc. firm zdefiniowało procedury uprawnień i dostępów, a wiec to kto i na jakich zasadach może uzyskiwać dostęp do danych i systemów informatycznych firmy. To oczywiście pokłosie wpływu, jaki mechanizmy kontroli dostępu (techniczne i organizacyjne) wywierają na cyberbezpieczeństwo organizacji.

Właściwie zdefiniowany proces zapewnienia ciągłości działania wymaga opracowania i wdrożenia w życie szeregu innych dokumentów definiujących wymagania, ryzyka oraz potencjalne skutki przestojów i niedostępności systemów. 64 proc. firm zdefiniowało wymagania, a 58 proc. strategię utrzymania ciągłości działania. 67 proc. sformalizowało zaś role i odpowiedzialności w tym obszarze.

Kluczem do wdrożenia strategii zapewnienia ciągłości działania jest nakreślenie sposobu funkcjonowania organizacji oraz

FORMALNE DOKUMENTY, KTÓRE ZDEFINIOWANO, TZN. OPRACOWANO, ZATWIERDZONO I WDROŻONO, W FIRMIE



zachodzących w niej procesów w kontekście analizy ryzyka (Risk Analysis, RA) oraz analizy wpływu funkcji biznesowej (a właściwie ich zakłócenie lub przerwanie) na działalność firmy (Business Impact Analysis, BIA). Również po to, aby określić wskaźniki RTP/RPO, czyli dopuszczalny czas przywrócenia procesów w sytuacji kryzysowej oraz akceptowalny poziom utraty danych w czasie. 53 proc. przedsiębiorstw prowadzi analizę ryzyka związaną z ciągłością działania (RA), a 41 proc. analizę wpływu na biznes (BIA).

53 proc. firm opracowało plan ciągłości działania (BCP), czyli schemat działań do podjęcia na wypadek istotnej awarii lub katastrofy. 68% zdefiniowało zaś procedury awaryjne (DRP), będące składową planu BCP, opisujące procedury, które należy wykonać w przypadku wystąpienia takich zdarzeń.

Paweł Henig,
dyrektor operacyjny,
Trusted Information Consulting

Wyniki badania potwierdzają, że dokumentacja najczęściej powstaje w celu spełnienia wymagania prawnego (polityka związana z RODO). Niestety, praktyka audytora utwierdza mnie w przekonaniu, że zapewnienie zgodności jest najczęściej jedynym celem opracowania takich formalnych dokumentów. Oznacza to, że zapominamy, czemu te dokumenty, a właściwie, mówiąc językiem normatywnym, „udokumentowane informacje", mają służyć.

Cyberbezpieczeństwo to zadanie zespołowe, a zespół jest tak sprawny, jak sprawnie się komunikuje. Udokumentowane informacje są podstawową formą komunikacji zespołu. Dlatego po pierwsze muszą być napisane w sposób czytelny i zrozumiały. Muszą przekazywać te informacje, które są potrzebne i istotne. Nie powinny zawierać szumu informacyjnego, czyli dużej ilości tekstu, który nic konkretnego nie wnosi, a jedynie utrudnia dotarcie do istotnej informacji, czyli opóźnia komunikację, lub wręcz ją uniemożliwia. Doświadczenie pokazuje, że często, niestety, mamy syndrom wieży Babel.

Chociaż udokumentowane informacje są podstawową formą komunikacji zespołu, to każda forma komunikacji, zarówno werbalna, jak i niewerbalna, jest istotna. Przekaz musi być spójny. Dlatego tak ważne jest, aby ci, którzy wydają dokumenty, sami się do nich stosowali. W języku normatywnym nazywamy to zaangażowaniem kierownictwa.

Niestety, odpowiedź na powyższe pytania wykracza poza możliwości niniejszego badania. Wnioskujemy na podstawie poszlak. Każdy jednak powinien zastanowić się nad tymi zagadnieniami.

93% firm przygotowało, zatwierdziło i wdrożyło politykę ochrony danych osobowych (RODO)

86% przedsiębiorstw zdefiniowało procedury uprawnień i dostępów

53% organizacji prowadzi analizę ryzyka związaną z ciągłością działania (RA), a 41 proc. analizę wpływu na biznes (BIA)

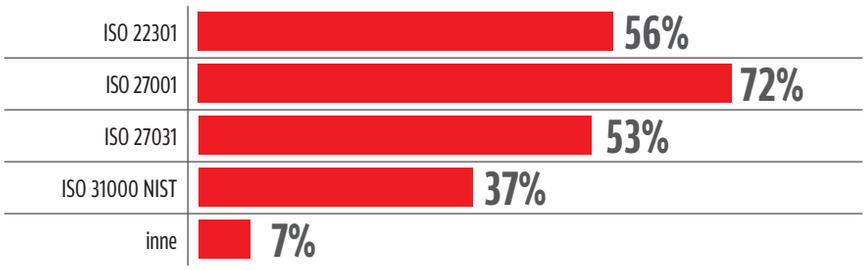
CERTYFIKACJE I STANDARDY ZAPEWNIENIA CIĄGŁOŚCI DZIAŁANIA

Motorem napędowym oraz potwierdzeniem działań podejmowanych w celu zapewnienia ciągłości działania są certyfikacje oraz postępowanie zgodnie ze standardami czy dobrymi praktykami w tym obszarze. 63 proc. ogółu i 74 proc. największych przedsiębiorstw i korporacji wdrożyło i certyfikowało co najmniej jeden międzynarodowy standard (framework) w obszarze zapewnienia ciągłości działania i bezpieczeństwa informacji IT.

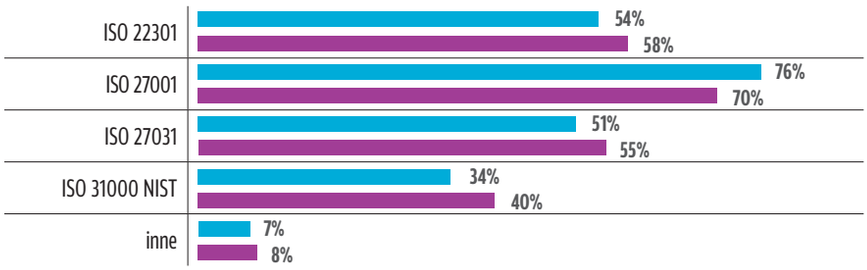
Najczęściej implementowane standardy to ISO 27001 (72% wskazań), ISO 22301 (56%), ISO 27031 (53%) oraz ISO 31000 NIST (37%).

74% dużych przedsiębiorstw i korporacji wdrożyło i certyfikowało co najmniej jeden międzynarodowy standard (framework) w obszarze zapewnienia ciągłości działania i bezpieczeństwa informacji IT

MIĘDZYNARODOWE STANDARDY (FRAMEWORKI) W OBSZARZE ZAPEWNIENIA CIĄGŁOŚCI DZIAŁANIA I BEZPIECZEŃSTWA INFORMACJI IT WDROŻONE I CERTYFIKOWANE W FIRMIE (WIELOKROTNY WYBÓR)



Przedsiębiorstwa, które nie wdrożyły żadnego z wymienionych standardów



Przedsiębiorstwa, które nie wdrożyły żadnego z wymienionych standardów

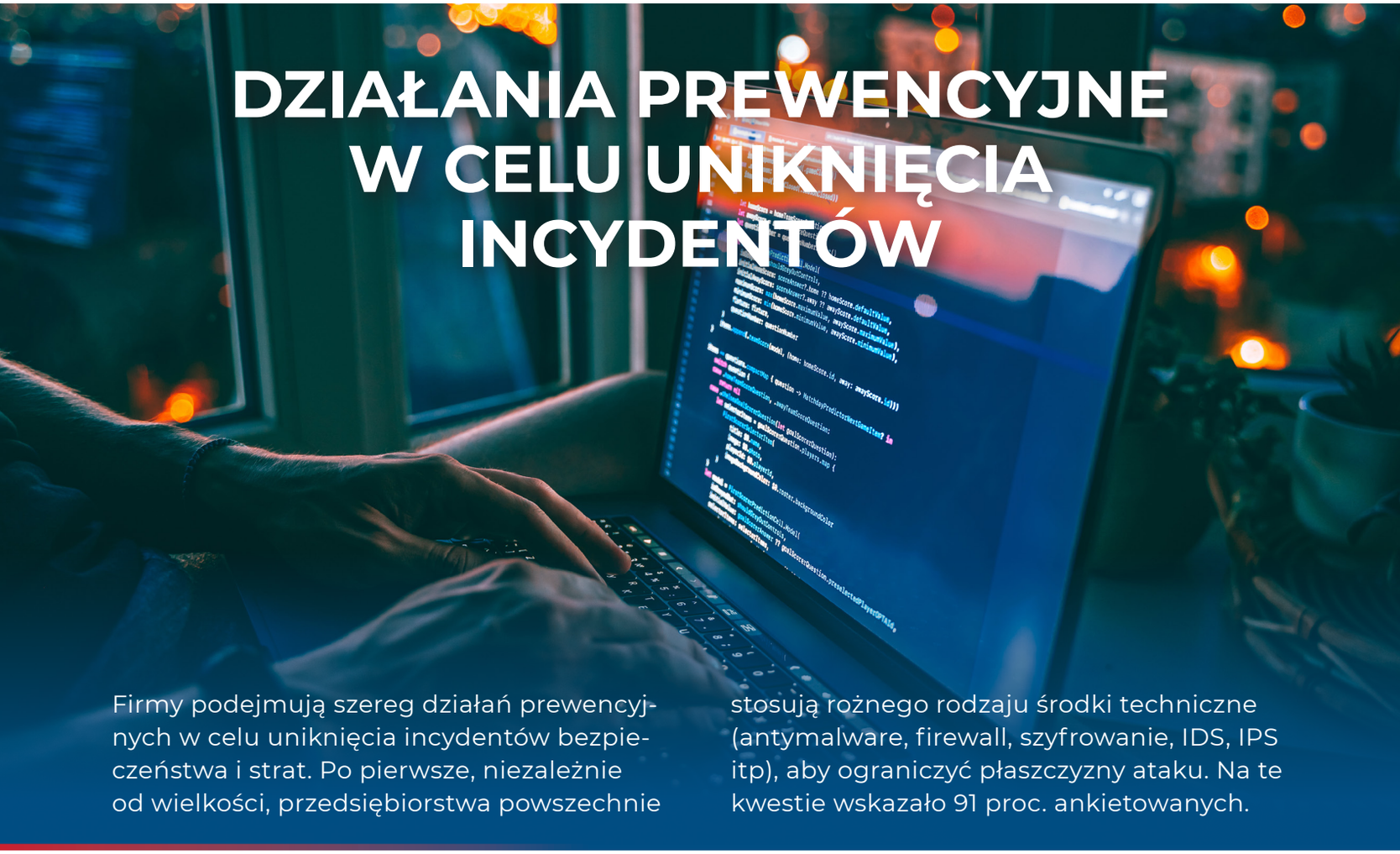
Średnie firmy Duże przedsiębiorstwa i korporacje

Marcin Kowalczyk,
dyrektor Departamentu
Bezpieczeństwa i Usług IT, PBSG

Ogromna popularność wdrażania i certyfikacji standardów odzwierciedla obecny trend, który jest wynikiem wzrostu świadomości w zakresie zapewnienia bezpieczeństwa, większego zaufania do systemów zarządzania oraz aktualnych oczekiwań partnerów biznesowych. Stosowanie właściwych frameworków i ich certyfikacja gwarantują wysoki poziom bezpieczeństwa oraz pozwalają organizacjom na skupienie się na głównym obszarze działalności. Stosowanie standardów ułatwia ocenę stopnia zapewnienia bezpieczeństwa, a certyfikacja zwalnia kontrahentów od przeprowadzania dodatkowych audytów.

Nasze obserwacje potwierdzają, że zdecydowana większość podmiotów posiada wdrożone takie systemy, lecz nie wszystkie zdecydowały się na ich certyfikację. Trend ten jednak się zmienia i obserwujemy wzrost zainteresowania przygotowaniem do ścieżki certyfikacyjnej.

Popularność standardów z rodziny ISO 27000 utrzymuje się na wysokim poziomie już wiele lat, zaskakujący jest natomiast wysoki odsetek wdrożeń i certyfikacji wg normy ISO 22301. Obserwujemy na rynku, że doświadczenia związane z pandemią przekonały organizacje do konieczności posiadania skutecznego systemu zapewnienia ciągłości działania. W sytuacjach kryzysowych i przy braku stabilności łańcucha dostaw szczególnie docenia się współpracę z dostawcami i partnerami, którzy są odpowiednio przygotowani na wypadek wystąpienia nieprzewidzianych zdarzeń.



DZIAŁANIA PREWENCYJNE W CELU UNIKNIĘCIA INCYDENTÓW

Firmy podejmują szereg działań prewencyjnych w celu uniknięcia incydentów bezpieczeństwa i strat. Po pierwsze, niezależnie od wielkości, przedsiębiorstwa powszechnie stosują rożnego rodzaju środki techniczne (antymalware, firewall, szyfrowanie, IDS, IPS itp), aby ograniczyć płaszczyzny ataku. Na te kwestie wskazało 91 proc. ankietowanych.

Grzegorz Michałek,
współzałożyciel i prezes zarządu,
Arcabit/mks_vir

Jako producent oprogramowania ochronnego ze szczególną uwagą śledzimy pozycję i rolę software'owych narzędzi zabezpieczających w szeroko pojętych systemach zabezpieczających systemy i dane. W naszej ocenie, popartej bieżącymi relacjami z klientami, wbrew pojawiającym się w mediach branżowych spekulacjom, znaczenie oprogramowania ochronnego będzie rosło, akcentując swoją aktywność w kolejnych obszarach, które znacznie wykraczają poza klasyczne wykrywanie szkodliwego oprogramowania.

Analizując i przewidując kierunki, w których podążają cyberprzestępcy, kładziemy szczególny nacisk na analizę, blokowanie i raportowanie nowych szkodliwych aktywności pracujących w systemach i sieciach procesów, uwzględniając również potencjalnie niebezpieczne działania samych użytkowników. Potwierdzeniem zasadności takiej strategii jest np. praktycznie stuprocentowa skuteczność w blokowaniu szkodliwych wiadomości e-mail zarówno jako nośników szkodliwego oprogramowania, jak i różnorodnych prób wyłudzania danych i środków finansowych.

Po drugie – firmy monitorują i zarządzają całością zasobów IT. 86 proc. firm sklasyfikowanych przez nas jako duże i 76 proc. średniej wielkości organizacji ma dedykowanego administratora IT. Przeciętnie 59 proc. przedsiębiorstw przeprowadza testy bezpieczeństwa swoich systemów – penetracyjne, audytowe (np. ISO 27001), socjotechniczne czy red teaming.

67% firm zdefiniowało procedury reagowania na incydenty. A gdy te wystąpią, będą potrafiły zidentyfikować źródło, usunąć zagrożenie oraz wyciągnąć wnioski. 58 proc. podmiotów każdorazowo przeprowadza ocenę działań po zakończeniu operacji reagowania na poważne incydenty.

Właściwa ochrona systemów informatycznych wymaga wyposażenia pracowników w szereg umiejętności miękkich z zakresu cyberbezpieczeństwa. W tym celu 51 proc. firm prowadzi cykliczne szkolenia pracowników technicznych oraz nietechnicznych. 60 proc. deklaruje, że regularnie podnosi kwalifikację personelu technicznego w zakresie wykrywania incydentów bezpieczeństwa.

Miłosz Cisowski,
Product Owner
Vector Synergy/CDeX

Szacuje się, że co 39 sekund występuje nowy atak, a 64% firm na świecie doświadczyło przynajmniej jednej jego formy w ubiegłym roku. Co więcej, średni koszt wyniósł 3,86 mln dolarów, a globalne koszty cyberprzestępczości wciąż rosną.

Niezależnie od swojej wielkości i branży, firmy są narażone na cyberataki, których celem może być kradzież danych (własnych, klientów), szpiegostwo korporacyjne czy wymuszenie okupu. Utrata przychodów i reputacji, przestoje, koszty odzyskania danych oraz konsekwencje prawne często są bolesne.

Zapobieganie incydentom jest bezpieczniejszą i tańszą opcją niż reagowanie, gdy jest już za późno. Widzimy wzorzec, w którym 70% ekspertów uważa prewencję ataków za najważniejszą, natomiast skupia się na niej tylko 24% firm. Z uwagi na to, że jest ona trudna, większość budżetu w branży cyberbezpieczeństwa wydawana jest na detekcję.

Cyberpoligon to rozwiązanie, które wspiera proaktywną strategię bezpieczeństwa. Dzięki możliwości symulacji ataków i ruchu sieciowego, odwzorowania własnej infrastruktury oraz wykorzystania bazy scenariuszy treningowych skupia się na prewencji. Możliwe są testowanie i ocena pod kątem istniejących podatności w zamkniętym i kontrolowanym środowisku środków technicznych (firewall, antymalware itp.), rekrutacja dobrych specjalistów i podnoszenie w praktyczny sposób ich kompetencji, weryfikacja oraz wypracowywanie planów i procedur reagowania na incydenty.

Prewencja nie jest trudna, jeśli podejdziemy do niej w holistyczny sposób.

Przezorny zawsze ubezpieczony. Działy IT muszą być przygotowane na każdą ewentualność, ale pewien odsetek firm decyduje się na wykupienie polisy ubezpieczeniowej na wypadek wystąpienia niepożądanych sytuacji. 22 proc. ankietowanych przedsiębiorstw wykupiło ubezpieczenie na wypadek ataku lub wycieku danych. 15 proc. wymaga od zewnętrznych kontraktorów policy OC w zakresie cyberbezpieczeństwa.

Tomasz Gaj,
CEO, Findia

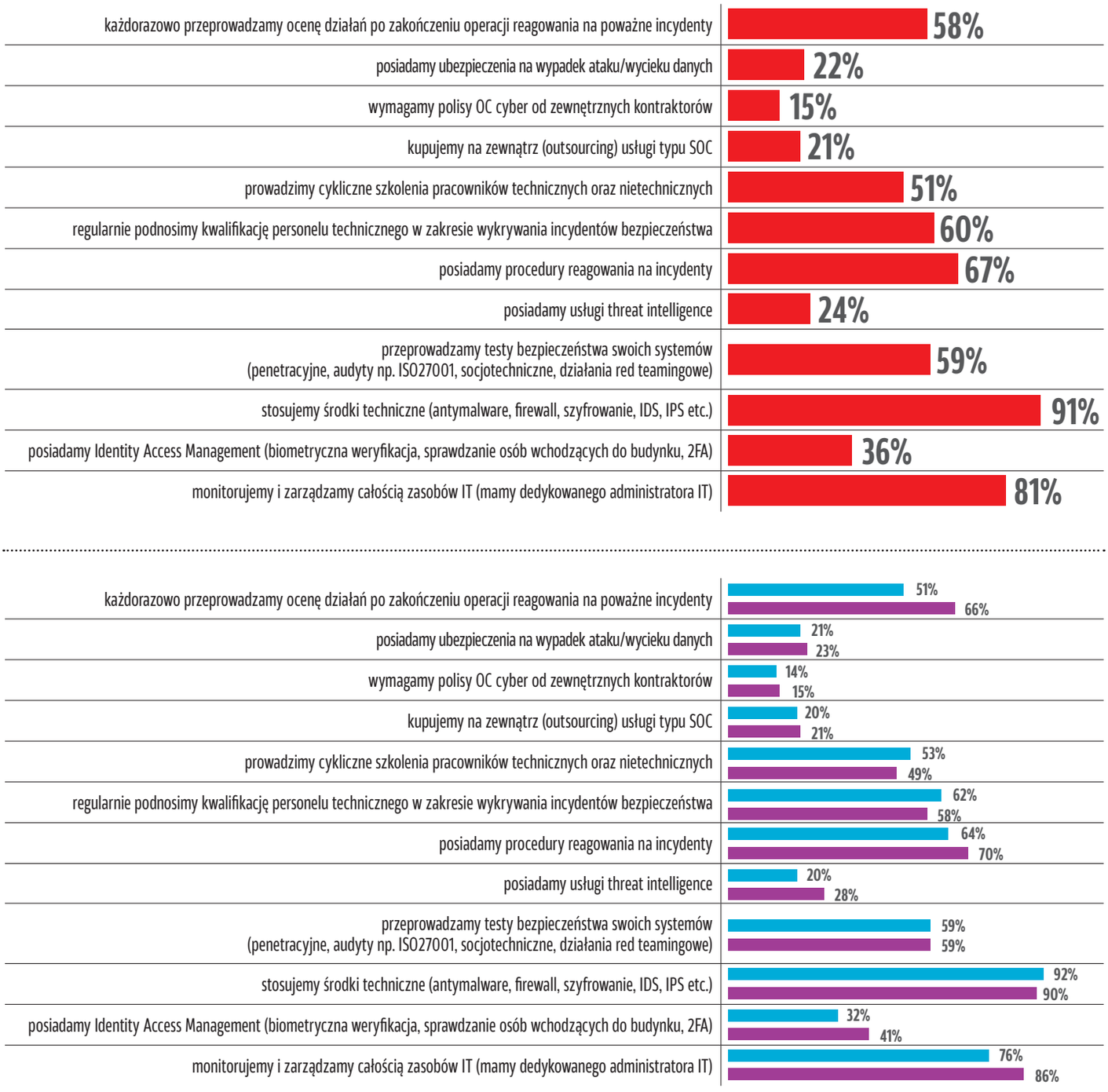
findia
• INSURANCE •

Pandemia oraz rosnąca liczba ataków typu ransomware spowodowały, że ubezpieczyciele coraz ostrożniej oferują ubezpieczenia cyber dla podmiotów gospodarczych. Równolegle zwiększane są wymagania, jakie spełnić musi dana firma, aby takie ubezpieczenie wykupić.

Ubezpieczyciele przedstawiają firmom rekomendacje wskazujące, jakie obszary bezpieczeństwa cybernetycznego muszą być poprawione w organizacji, aby mogła ona otrzymać polisę cyber. Można się spodziewać, że ze względu na straty finansowe ubezpieczycieli ten trend w najbliższym czasie będzie kontynuowany, co wymusi większe nakłady na bezpieczeństwo cybernetyczne w organizacjach.

Obszary, na które ubezpieczyciele w szczególności zwracają uwagę, to: regularnie testowane plany ciągłości działania, a także plany reakcji na incydenty cyber, regularnie przeprowadzane testy penetracyjne oraz sprawnie wdrażane rekomendacje krytyczne, bezpieczeństwo kopii zapasowych, zarządzanie uprawnieniami, wieloskładnikowe uwierzytelnianie MFA przy dostępie zdalnym do systemów i poczty elektronicznej.

JAKIE DZIAŁANIA PODEJMUJE PAŃSTWA FIRMA, ABY UNIKNĄĆ INCYDENTÓW BEZPIECZEŃSTWA I STRAT?



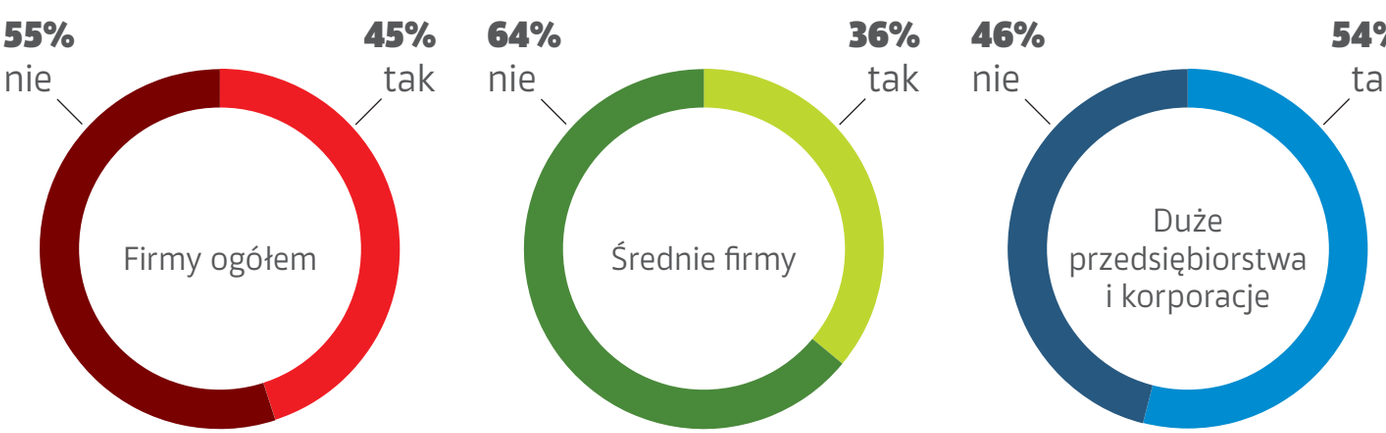
91% firm stosuje rożnego rodzaju środki techniczne, aby uniknąć incydentów bezpieczeństwa i strat

IDENTYFIKACJA AKTAULNYCH ZAGROŻEŃ I ZASZŁYCH NARUSZEŃ

W 45 proc. ankietowanych firmach funkcjonuje proces proaktywnego wykrywania zagrożeń w obszarze cyberbezpieczeństwa z ang. threat intelligence / hunting. W grupie dużych przedsiębiorstw i korporacji odsetek ten sięga nawet 54 proc.

Wiele zauważonych incydentów wymaga dalszej analizy w celu ustalenia źródeł pochodzenia ataku, podstawy naruszenia i jego skutków. Nic dziwnego, że aż 17 proc. firm korzystało kiedyś z usług informatyki śledczej (ang. digital forensic). W gronie dużych – już co czwarta (25%).

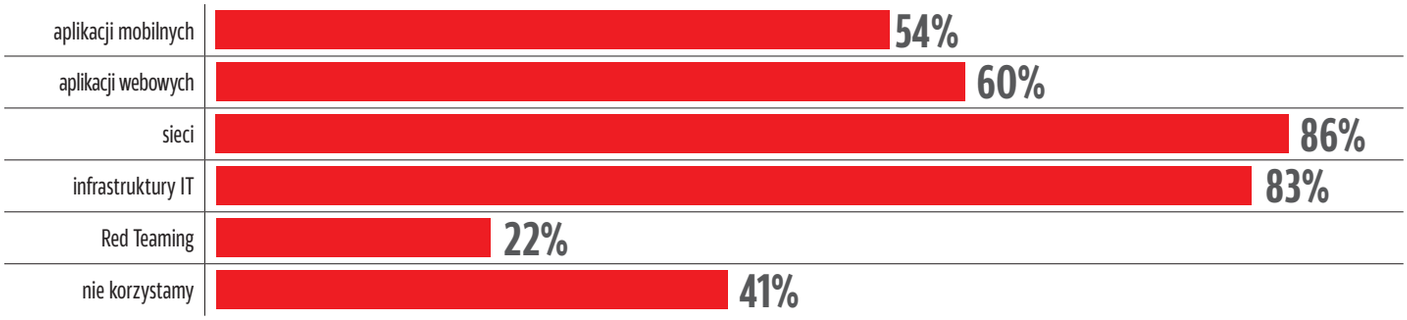
CZY W FIRMIE FUNKCJONUJE PROCES PROAKTYWNEGO WYKRYWANIA ZAGROŻEŃ W OBSZARZE CYBERBEZPIECZEŃSTWA Z ANG. THREAT INTELLIGENCE / HUNTING?

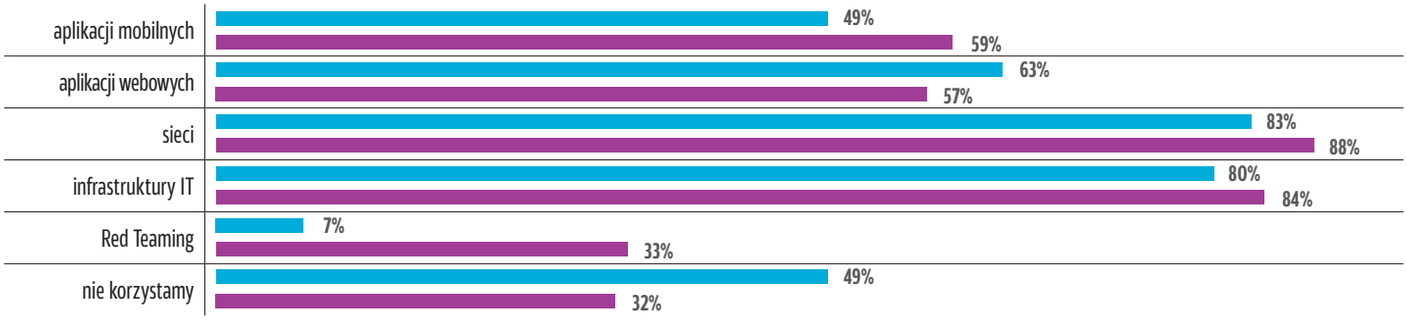


59 proc. firm korzysta z usług testów bezpieczeństwa (testów penetracyjnych). Po takie usługi częściej sięgają duże przedsiębiorstwa i korporacje (68%) niż ich mniejsi konkurenci (51%). Prowadzone audyty dotyczą bezpieczeństwa sieci (86%) oraz infrastruktury IT (83%). W miarę potrzeb firmy równie chętnie sięgają po testy aplikacji webowych (60%) oraz mobilnych (54%).

Nieco mniej firm zamawia usługi typu Red Teaming polegające na wynajęciu badaczy, których zadaniem jest wcielenie się w rolę hakerów i podjęcie próby wykrycia podatności na różnych płaszczyznach bezpieczeństwa informatycznego – od sieci po socjotechnikę. Z usług Red Teaming korzysta mniej niż co czwarta firma (22%) przy czym w grupie największych organizacji odsetek ten rośnie do 33 proc.

CZY KORZYSTAJĄ PAŃSTWO Z USŁUG TESTÓW BEZPIECZEŃSTWA (TESTÓW PENETRACYJNYCH)?





Dr inż. Michał Suchocki,
Product Director, CyCommSec

CyCommSec

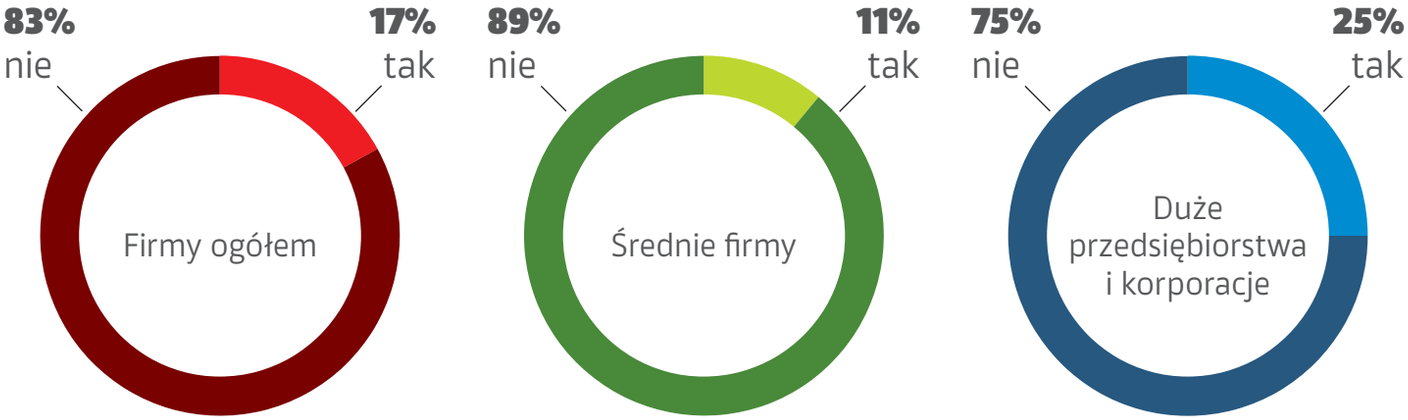
Wyniki przeprowadzonego sondażu są zadowalające. Patrząc z perspektywy ostatnich pięciu lat, można zauważyć, że polskie przedsiębiorstwa odrabiają lekcję z cyberbezpieczeństwa.

Prawie połowa ankietowanych twierdzi, że wdrożyła proces proaktywnego wykrywania zagrożeń. Wypadamy znacznie lepiej w porównaniu z francuskimi przedsiębiorcami, gdzie tylko 33% przedsiębiorstw próbuje polować na zagrożenia; jednak Japonia (75%) czy Wielka Brytania (ponad 90%) biją nas na głowę. Oczywiście wyniki należy jeszcze rozpatrzeć pod względem efektywności wdrożonego programu bądź rozwiązania, np. czy dostarcza odpowiednich dowodów, aby zapobiec ponownemu atakowi lub infekcji.

Prawie 60% firm wykonuje testy bezpieczeństwa. Podejrzewamy, że procent ten jeszcze wzrośnie ze względu na zwiększoną liczbę ataków na polskie przedsiębiorstwa, co wynika głównie z sytuacji związanej z COVID-19 (praca zdalna) oraz z faktu, że Polska się bogaci. Testy penetracyjne umożliwiają wykrycie luk i ich remediacje przy stosunkowo niskim koszcie w porównaniu z defensywą. Niestety, z naszych obserwacji wynika, że nadal większość firm wykonuje takie testy czy audyty tylko raz w roku, a nie w modelu cyklicznym.

Nadal mamy niski odsetek firm wykonujących tzw. Red Teaming. Patrząc na rodzaje ataków i błędów, jakie popełniały polskie przedsiębiorstwa w 2020 r., odsetek wykonanych kampanii socjotechnicznych powinien znacznie wzrosnąć, chociażby z tego względu, że Polacy często otwierali pliki .exe otrzymane mailowo, stając się jednocześnie ofiarami phishingu.

CZY KORZYSTALI PAŃSTWO KIEDYŚ Z USŁUG DIGITAL FORENSICS (INFORMATYKA ŚLEDCZA)?



Joanna Miazga,
Senior Sales Manager, STM Cyber

Prezentowane wyniki to wyraźny sygnał zarówno dla firm branży ICT, jak i tych, które chcą uniknąć konsekwencji finansowych i wizerunkowych, będących skutkiem naruszeń bezpieczeństwa. Dostrzegamy potrzebę dojrzałego budowania strategii zarządzania bezpieczeństwem. Strategia ta skutkować powinna zwiększeniem świadomości organizacji oraz użytkownika, który przetwarza wrażliwe dane organizacji.

W Polsce aż 40% badanych firm nie wykonuje profesjonalnych testów penetracyjnych. Jest to spowodowane:

- *ograniczoną świadomością i wdrożeniem, uznanych standardów bezpieczeństwa;*
- *niedostateczną inwentaryzacją zasobów IT, prowadzącą do błędów w analizie ryzyka;*
- *niedostateczną alokacją w budżecie klienta funduszy na projekty z obszaru cybersecurity;*
- *brakiem informacji o potencjalnych ryzykach i incydentach bezpieczeństwa w mediach spoza branży ICT.*

Holistyczne podejście do strategii bezpieczeństwa wymaga uwzględnienia w niej realizacji usług red team, które najlepiej oddają sytuacje realnego ataku.

Usługa ta umożliwia ocenę zdolności organizacji do wykrywania potencjalnych naruszeń oraz skuteczność reagowania w przypadku identyfikacji incydentu bezpieczeństwa.

Badane są zarówno zabezpieczenia techniczne, jak i skuteczność wdrożonych procedur.

W 45% przedsiębiorstw funkcjonuje proces proaktywnego wykrywania zagrożeń w obszarze cyberbezpieczeństwa

25% dużych firm korzystało w przeszłości z usług informatyki śledczej

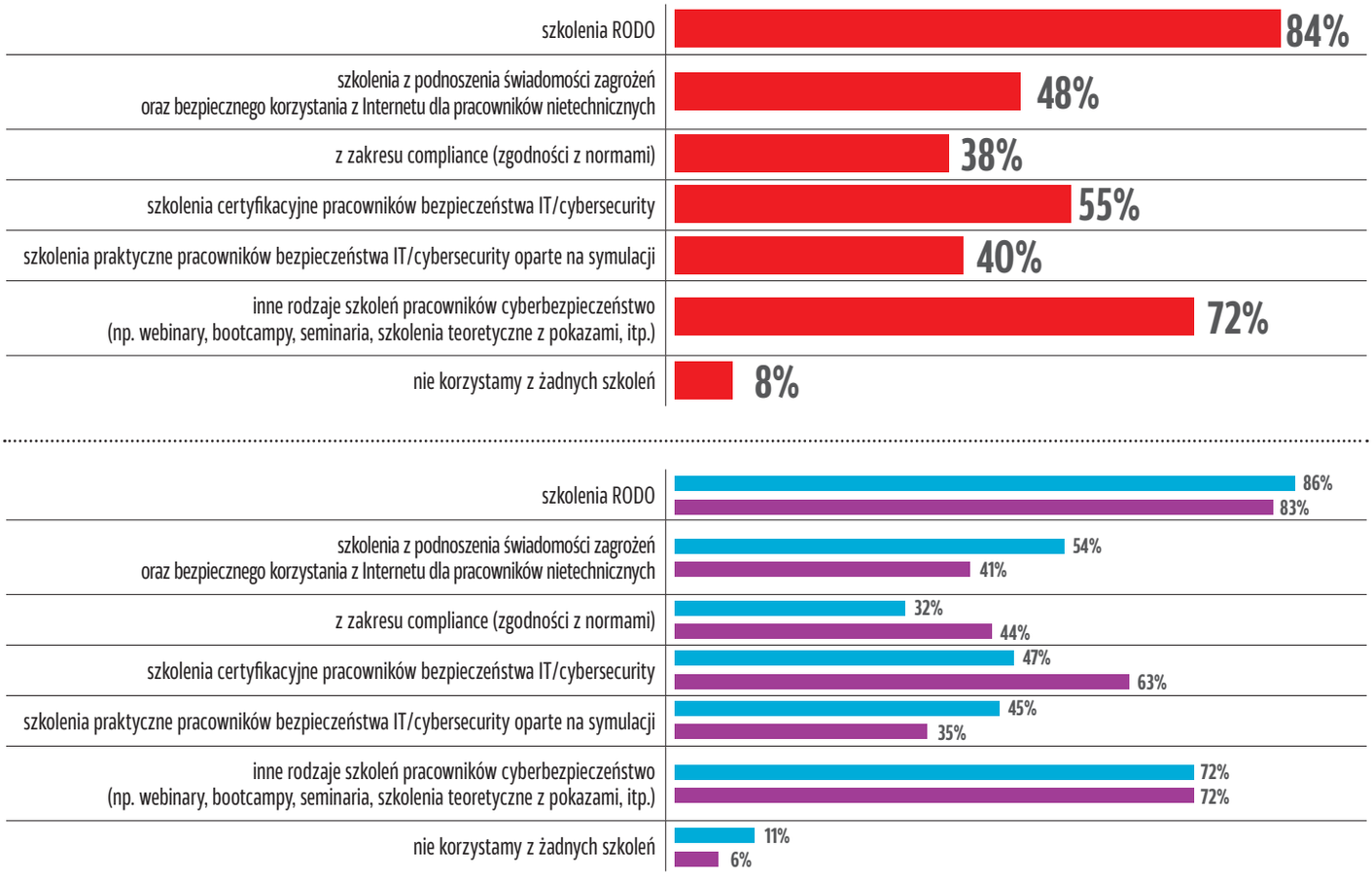
59% organizacji prowadzi testy penetracyjne

SZKOLENIA PERSONELU W OBSZARZE CYBERBEZPIECZEŃSTWA

Wejście w życie regulacji RODO wymusiło na firmach konieczność przeszkolenia personelu. Szkolenia z zakresu ochrony danych osobowych prowadzi 84 proc. ankietowanych przedsiębiorstw.

Firmy chętnie sięgają również po szkolenia certyfikacyjne (55%) oraz szkolenia praktyczne oparte na symulacji (40%) pracowników bezpieczeństwa IT i cybersecurity. Szkolenia z zakresu zgodności z normami (compliance) prowadzi zaś 38 proc. organizacji. Co warte odnotowania, co druga firma inwestuje w rozwój personelu nietechnicznego, organizując szkolenia z podnoszenia świadomości zagrożeń oraz bezpiecznego korzystania z Internetu.

RODZAJE SZKOLEŃ W OBSZARZE CYBERBEZPIECZEŃSTWA I BEZPIECZEŃSTWA INFORMACJI Z KTÓRYCH KORZYSTA FIRMA I JEJ PRACOWNICY



Poza tradycyjnymi formami szkoleń firmy niezwykle chętnie (72%) sięgają po inne rodzaje dokształcania pracowników w zakresie cyberbezpieczeństwa takie jak webinary, bootcampy, seminaria czy szkolenia teoretyczne z pokazami.

Kajetan Korzycki,
Cybersecurity Engineer,
IDENTT

Środki organizacyjne i techniczne nie są wystarczające, aby zapewnić bezpieczeństwo informacji współczesnych firm. Zdecydowana większość incydentów jest spowodowana nieumyślnym działaniem pracowników, dlatego podnoszenie świadomości zagrożeń oraz poznawanie sposobów bronienia się przed nimi są niezwykle istotne.

Wyniki raportu wskazują, że znaczna większość firm inwestuje w szkolenia dotyczące zagadnień związanych z cyberbezpieczeństwem – jedynie 8% wskazało, że nie wykonuje ich wcale.

Cieszy fakt, że znacząca większość firm, niezależnie od jej rozmiarów, decyduje się na przeprowadzanie szkoleń z zakresu RODO oraz bierze udział w różnego rodzaju konferencjach, warsztatach czy szczególnie popularnych obecnie webinarach z obszaru cyberbezpieczeństwa. Jednocześnie szkolenia, które zawierają element symulacji, przez co pozwalają lepiej zweryfikować rzeczywisty stan świadomości pracowników, przeprowadza już tylko 40% ankietowanych firm.

Szkolenia są także najczęściej wybieraną inwestycją w cyberbezpieczeństwo. Średnia ocen ważności szkoleń plasuje je jednak poniżej wielu innych środków technicznych czy organizacyjnych. Możliwe więc, że ich popularność wynika raczej z dostępności i wymagań prawnych, aniżeli wysokiej priorytetyzacji tego obszaru. Realny wpływ szkoleń personelu na bezpieczeństwo przedsiębiorstwa jest uzależniony od ich odpowiedniego przygotowania, zaadresowania w nich bieżących zagrożeń oraz dostosowania do konkretnej grupy odbiorców czy charakteru organizacji.

84% firm szkoli pracowników z zakresu ochrony danych osobowych

55% przedsiębiorstw prowadzi szkolenia certyfikacyjne

40% firm chętnie sięga po szkolenia praktyczne oparte na symulacji

BEZPIECZEŃSTWO PRACY ZDALNEJ

Pandemia COVID-19 doprowadziła do wzrostu znaczenia pracy zdalnej. 76 proc. firm stosuje połączenia VPN, aby zapewnić pracownikom bezpieczny dostęp do zasobów sieci wewnętrznej, centrów danych i chmury. 87 proc. organizacji wyposażyło urządzenia osobiste pracowników w oprogramowanie antywirusowe i zaporę sieciową (firewall). Połowa firm (50%) monitoruje stacje robocze użytkowników pracujących zdalnie.

Poza zabezpieczeniem punktów końcowych firmy wzmocniły mechanizmy ochrony wewnątrz sieci. Co druga ankietowana organizacja (48%) ma narzędzia zarządzania siecią, które dają administratorom wgląd w stan zabezpieczeń urządzeń łączących się z zasobami firmy zdalnie.

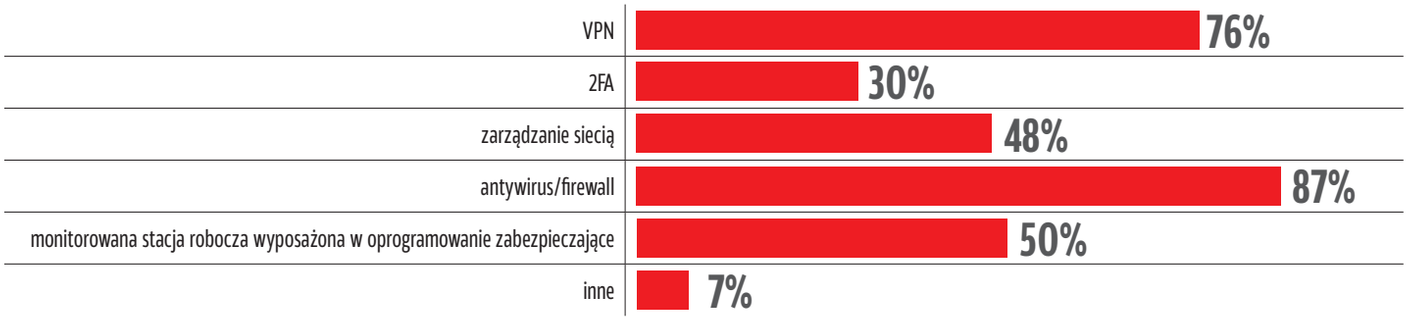
Dziwić może natomiast nadal niska adopcja rozwiązań z zakresu uwierzytelniania dwuskładnikowego (2FA). Tego typu mechanizmy wdrożyło 30 proc. ogółem i 37 proc. dużych firm. Zdawać się może, że wraz z rosnącą liczbą wdrażanych rozwiązań chmurowych, rola wieloskładnikowego uwierzytelniania w dostępie do zasobów będzie sukcesywnie rosnąć.

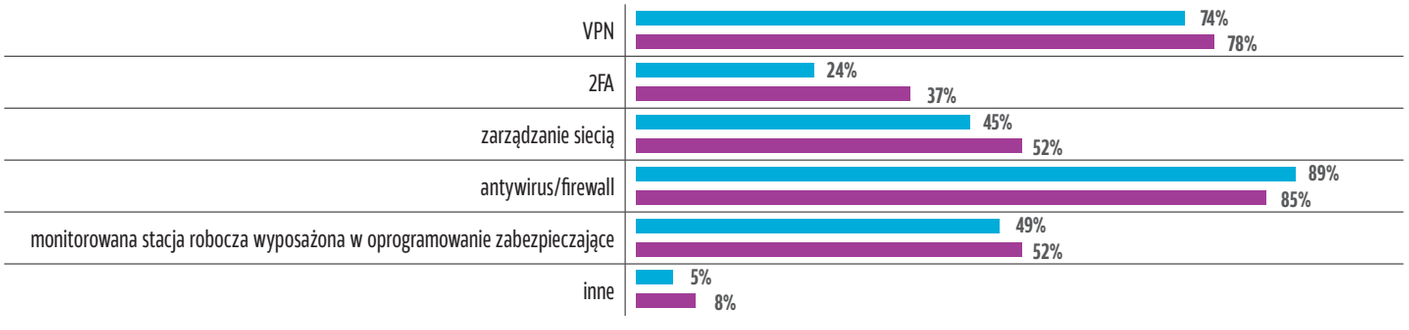
Bartosz Leoszewski,
CEO Famoc

Praca zdalna zwiększyła wykorzystanie urządzeń mobilnych, a pojęcie work-life balance nabrało dodatkowego wymiaru. W efekcie firmy zamiast zabezpieczać jedno biuro, muszą zarządzić niekiedy tysiącami biur mobilnych. Wiele z nich ponadto zezwala pracownikom na korzystanie ze służbowych urządzeń również do celów prywatnych. Dlatego kontrola i zabezpieczenie tych urządzeń jest obecnie kluczowym wyzwaniem dla działów bezpieczeństwa.

76% firm stosuje połączenia VPN, aby zapewnić pracownikom bezpieczny dostęp do zasobów sieci wewnętrznej, centrów danych i chmury

ZABEZPIECZENIA, KTÓRE POSIADAJĄ PRACOWNICY PODCZAS PRACY ZDALNEJ





PRYWATNA SIEĆ KOMÓRKOWA

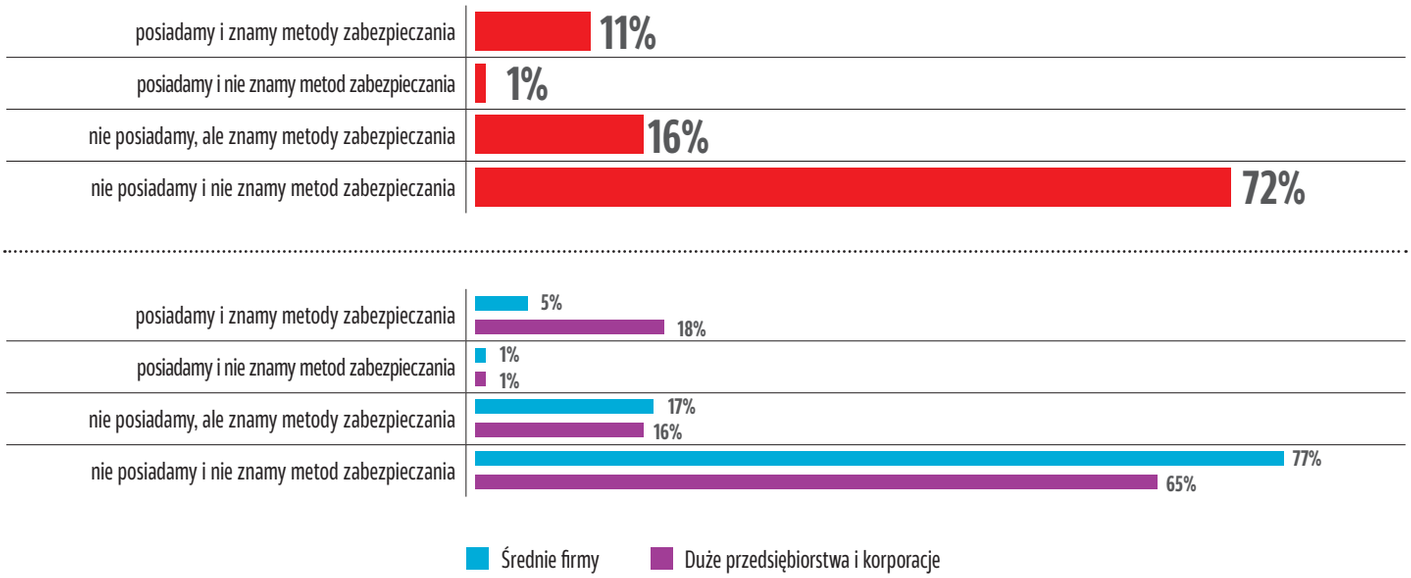
19 proc. dużych przedsiębiorstw i korporacji ma wdrożoną prywatną sieć telekomunikacyjną 4G/5G i zdecydowana większość z nich wie jak ją właściwie zabezpieczyć. Prywatna sieć komórkowa może zastąpić lokalną sieć Wi-Fi zapewniając wyższy poziom niezawodności oraz skuteczne pokrycie zasięgiem założonego obszaru. To także jeden z trendów definiujących jak mogą wyglądać fabryki projektowane zgodnie z ideą Przemysłu 4.0.

Wdrożenie sieci prywatnej wymaga jednak zmiany w sposobie zabezpieczania systemów informatycznych firmy. Co ciekawe, aż 16% ankietowanych zna metody i założenia zabezpieczania prywatnych sieci 4G/5G mimo, że w ich firmach nie wdrożono takich rozwiązań. Co warte odnotowania aż 8 proc. dużych przedsiębiorstw (i żadna średnia) zamierza w 2021 roku zainwestować środki właśnie w budowę prywatnej sieci 4G/5G.

19% dużych przedsiębiorstw i korporacji ma wdrożoną prywatną sieć telekomunikacyjną 4G/5G

Kolejne **16% ankietowanych** zna metody i założenia zabezpieczania prywatnych sieci 4G/5G mimo, że w ich firmach nie wdrożono takich rozwiązań

CZY POSIADAJĄ PAŃSTWO PRYWATNĄ SIEĆ TELEKOMUNIKACYJNĄ 4G/5G? CZY ZNAJĄ PAŃSTWO METODY ICH ZABEZPIECZANIA?



8% dużych przedsiębiorstw zamierza w 2021 roku zainwestować środki właśnie w budowę prywatnej sieci komórkowej

Sławomir Pietrzyk,
prezes IS-Wireless

Zapotrzebowanie na niezawodną łączność, która zapewnia niskie opóźnienia i której można zaufać w zakresie obsługi zadań o znaczeniu krytycznym, rośnie bardzo szybko. Coraz więcej przedsiębiorstw decyduje się na własne sieci 5G.

W badaniu 8% firm zadeklarowało, że zamierza to zrobić w tym roku. W najbliższych latach ten współczynnik będzie rósł – wg firmy badawczej Omdia w 2025 r. rynek prywatnych sieci telekomunikacyjnych będzie wart ponad 5 mld dol. Sprzyja temu kilka kwestii. Po pierwsze w wielu krajach państwowi regulatorzy rynku komunikacyjnego wydzielają część pasma na sieci prywatne. Tak jest np. w Niemczech czy Wielkiej Brytanii, gdzie za relatywnie niewielką opłatę można wykupić ograniczony geograficznie dostęp do pasma na własne potrzeby, co oznacza niezależność od operatorów ogólnokrajowych i niższe koszty instalacji. Liczymy, że i polski regulator zastosuje podobne rozwiązania w nadchodzącej aukcji. Po drugie, na rynek telekomunikacyjny wchodzą gracze, którzy potrafią zbudować sieci telekomunikacyjne w modelach otwartych (Open RAN), z pominięciem dotychczasowych monopolistów, co obniża koszt budowy sieci i pozwala ją dopasować do własnych potrzeb.

INWESTYCJE W CYBERBEZPIECZŃSTWO

Firmy zamierzają kontynuować kierunek obrany w celu realizacji strategii zapewnienia cyberbezpieczeństwa. 64 proc. z nich zamierza w bieżącym roku przeznaczyć środki na zakup rozwiązań antywirusowych i antyspyware. Kolejne 63 proc. na szkolenia pracowników. Co ciekawe, odsetek firm które deklarują tego typu inwestycje w cyberbezpieczeństwo jest wyraźnie wyższy wśród podmiotów średniej wielkości i wynosi odpowiednio 72 i 74 proc. Co więcej – przeciętnie 42 proc. organizacji zamierza wysłać w tym roku pracowników na konferencje branżowe.

Lista planowanych inwestycji zdaje się być długa i obejmuje ponadto narzędzia szyfrowania danych (51%), rozwiązania backupowe (49%), narzędzia ochrony poczty e-mail (tyle samo wskazań), sprzętowe zapory sieciowe (41%) oraz systemy ochrony w chmurze (33%).

Ankietowane przedsiębiorstwa zamierzają również wzmocnić zasoby kadrowe, sięgając także po usługi zewnętrznych dostawców. 21 proc. planuje zatrudnienie nowych pracowników zajmujących się cyberbezpieczeństwem. 19 proc. stawia w tym roku na outsorcing pracowników zajmujących się tym obszarem

bezpieczeństwa. Kolejne 39% zamierza wydać pieniądze na prowadzenie testów penetracyjnych i audytów. Środki te w dużej mierze również trafią do zewnętrznych dostawców.

Priorytetem firm ma być również bezpieczeństwo fizyczne. W 2021 roku mniej więcej co trzecia organizacja zamierza przeznaczyć środki na zakup fizycznych zabezpieczeń taki jak karty dostępowe, wagi (39%) czy zmodernizować lub rozszerzyć system alarmowy (25%) i monitoringu wizyjnego (34%).

Aleksander P. Czarnowski,
prezes AVET Information
and Network Security sp. z o.o.

AVETINS

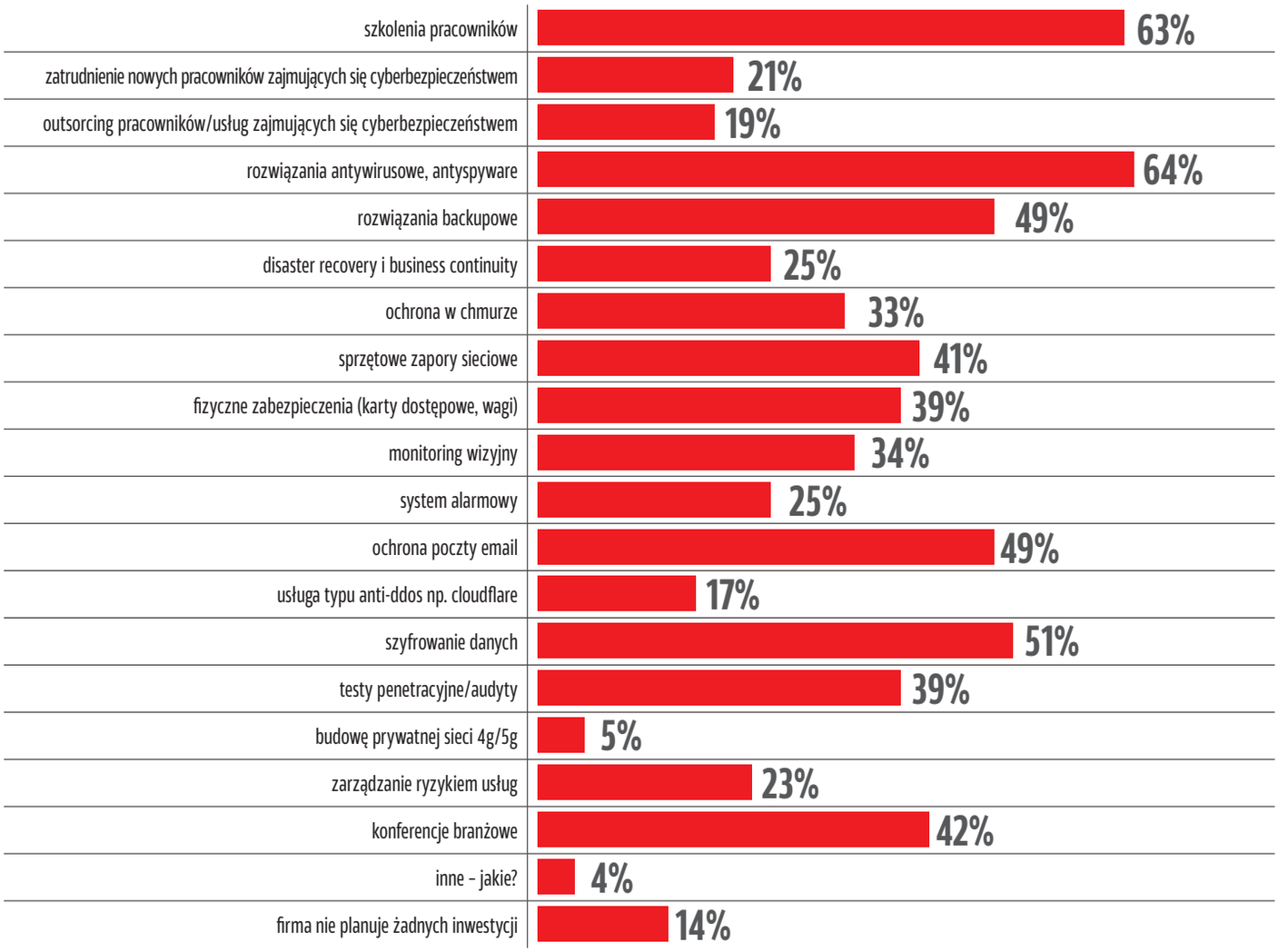
Każdy rzetelny raport na temat stanu cyberbezpieczeństwa w Polsce jest niezwykle istotny z kilku powodów. Po pierwsze, choć cyberbezpieczeństwo to problem globalny, to jednak celowe ataki są najgroźniejsze w skutkach i nie chodzi tylko o ryzyko utraty reputacji. Po drugie, lokalna charakterystyka, np. systemu podatkowego, powoduje, że jest tylko kwestią czasu, kiedy lokalni producenci oprogramowania zostaną zaatakowani jako ogniwo łańcucha dostaw. Świadomość ryzyka i konieczność zapewnienia właściwego poziomu bezpieczeństwa jest niezbędna. Lokalne oprogramowanie księgowe czy CRM jest idealnym celem np. dla ransomware. Drugim istotnym powodem jest fakt, że każdy raport to istotne narzędzie dla menedżerów, którzy muszą dzisiaj, w zmieniającym się dynamicznie świecie na skutek m.in. COVID-19, podejmować szybko trudne decyzje o daleko idących skutkach.

Odnosząc się do wyników raportu, widzimy kilka niepokojących sygnałów:

- *Niestety, fałszywe poczucie bezpieczeństwa nadal pokutuje w wielu organizacjach, niezbędne jest zatem stałe monitorowanie poziomu bezpieczeństwa organizacji i zabezpieczeń IT.*
- *Błędne poczucie, że automatyczne narzędzia zastąpią wiedzę ekspercką, jest ogromnie ryzykowne i w przyszłości prowadzić będzie do coraz większych strat organizacji.*
- *Chmura miała rozwiązać problem złożoności, tymczasem okazuje się, że sama staje się coraz bardziej złożona, a niestety, polskie prawo w tym nie pomaga skomplikowanymi regulacjami.*

Powyższe punkty sprawiają, że dzisiaj bardziej niż kiedykolwiek wcześniej potrzebny jest zaufany i doświadczony partner, który potrafi przeprowadzić organizację bezpiecznie nie tylko przez transformację cyfrową, ale także przez dynamicznie zmieniający się świat na skutek pandemii oraz czynników ekonomicznych i geopolitycznych.

NA CO ZWIĄZANEGO Z CYBERBEZPIECZEŃSTWEM FIRMY ZAMIERZAJĄ PRZEZNACZYĆ ŚRODKI W 2021 ROKU?

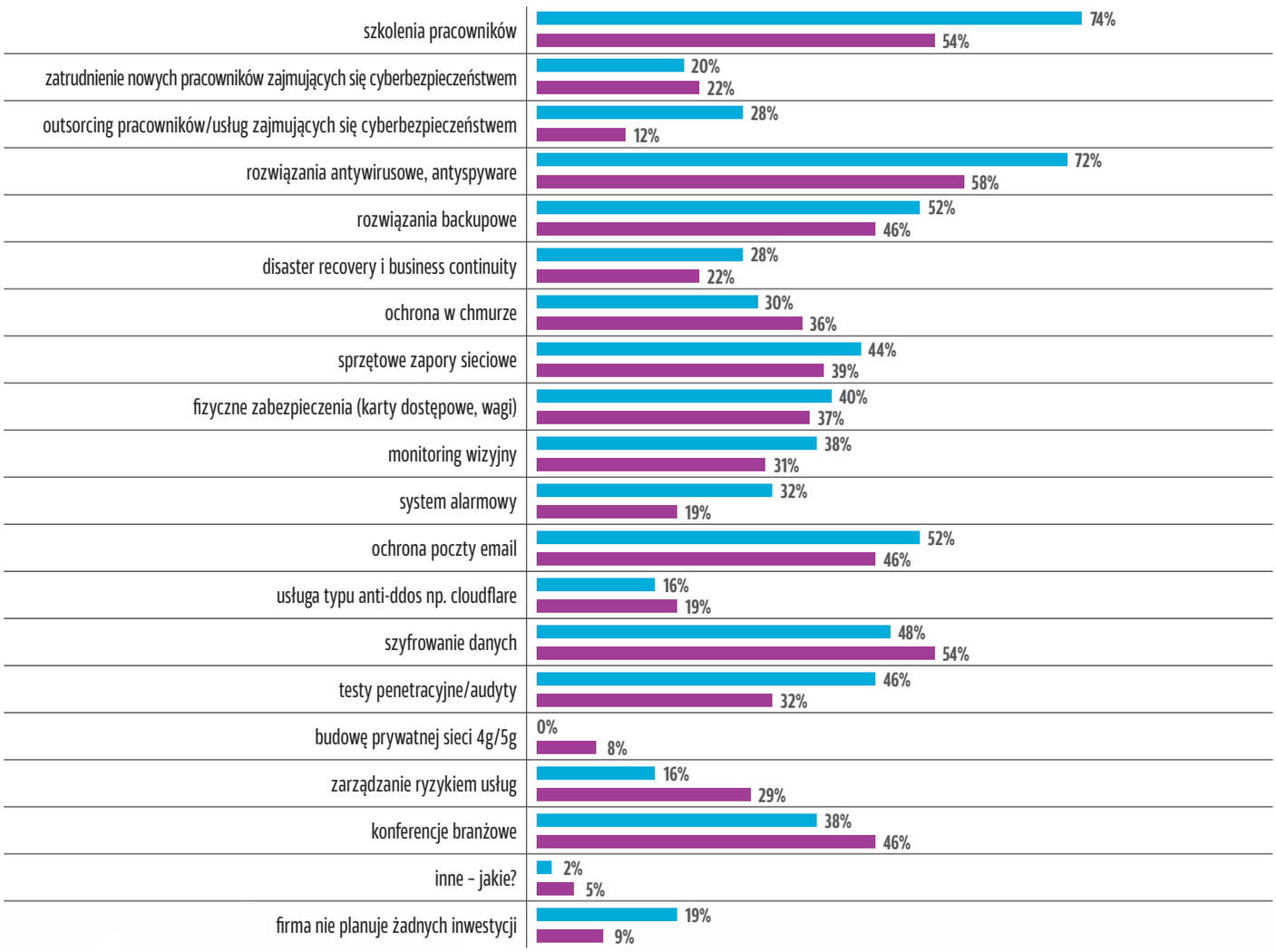


64% zamierza w bieżącym roku przeznaczyć środki na zakup rozwiązań antywirusowych i antyspyware

63% ma zagwarantowane środki na szkolenia pracowników

51% firm planuje zakup narzędzi szyfrowania danych,
49% rozwiązań backupu

NA CO ZWIĄZANEGO Z CYBERBEZPIECZEŃSTWEM FIRMY ZAMIERZAJĄ PRZEZNACZYĆ ŚRODKI W 2021 ROKU?



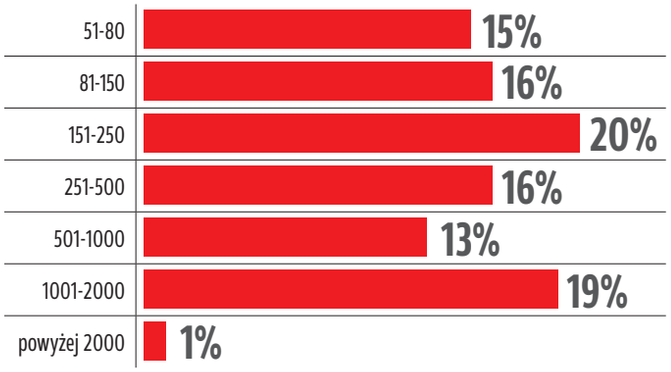
UCZESTNICY BADANIA

Badanie przeprowadzone zostało w czerwcu 2021 roku na grupie średnich i dużych przedsiębiorstw. 51% ankietowanych reprezentowało średniej wielkości firmy zatrudniające od 80 do 250 pracowników. 49% podmiotów, sklasyfikowanych przez nas jako duże, zatrudniało od 250 do ponad 2000 osób.

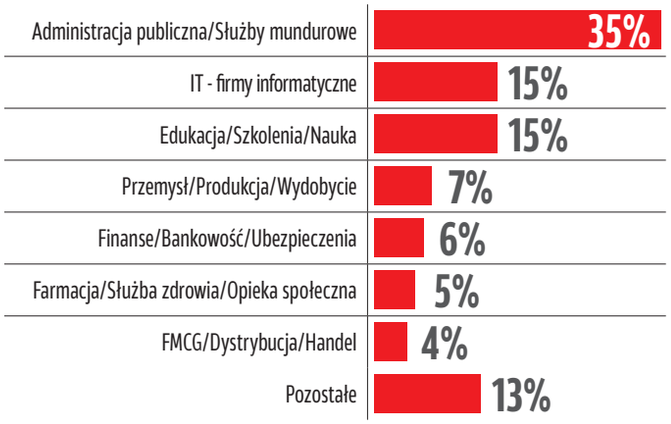
Badane podmioty wywodziły się z różnych gałęzi gospodarki. Najliczniej reprezentowane były organizacje administracji publicznej (35%), firmy informatyczne (15%) oraz sektora edukacyjnego (tyle samo wskazań). W badaniu udział wzięły również przedsiębiorstwa sektora przemysłowego, produkcji i wydobycia (7%), finansów i bankowości (6%), ochrony zdrowia (5%) oraz dóbr szybkozbywalnych, handlu i dystrybucji (4%).

O wypełnienie ankiet poprosiliśmy specjalistów (72%) oraz osoby zatrudnione na stanowiskach menedżerskich, w tym kierowników i dyrektorów działów (20%) oraz menedżerów wyższego szczebla (8%).

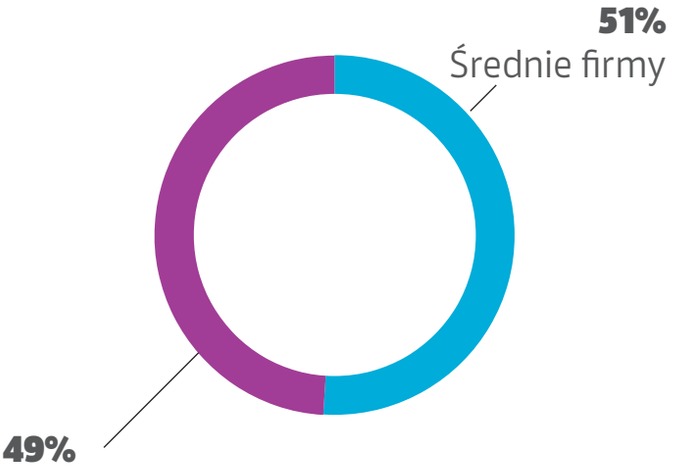
RESPONDENCI WG WIELKOŚCI PRZEDSIĘBIORSTWA



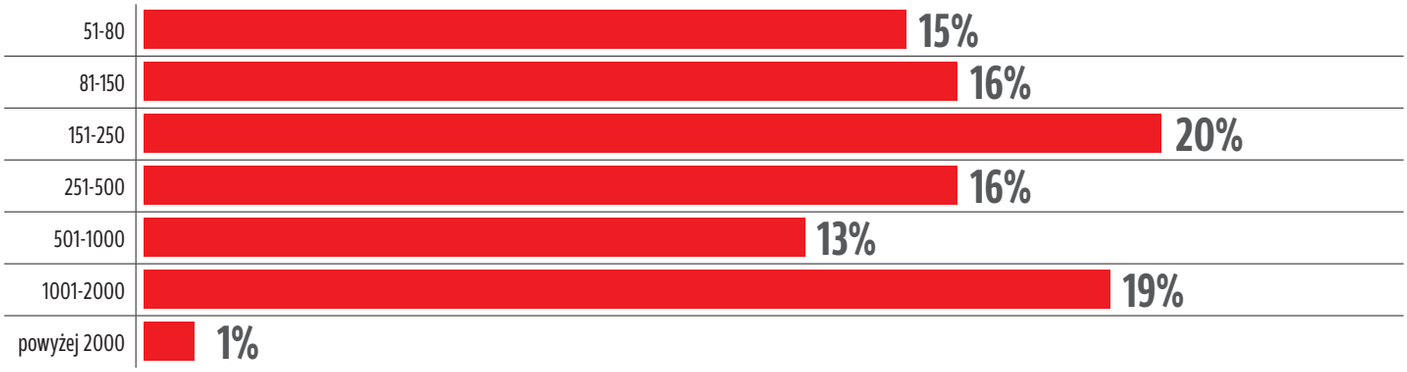
RESPONDENCI WG BRANŻY



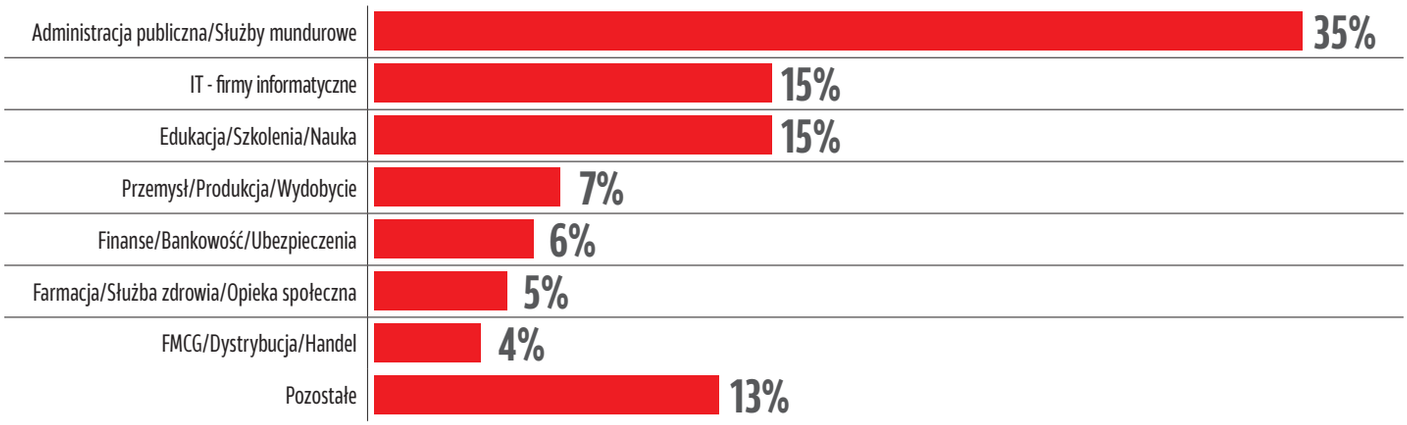
RESPONDENCI WG WIELKOŚCI PRZEDSIĘBIORSTWA



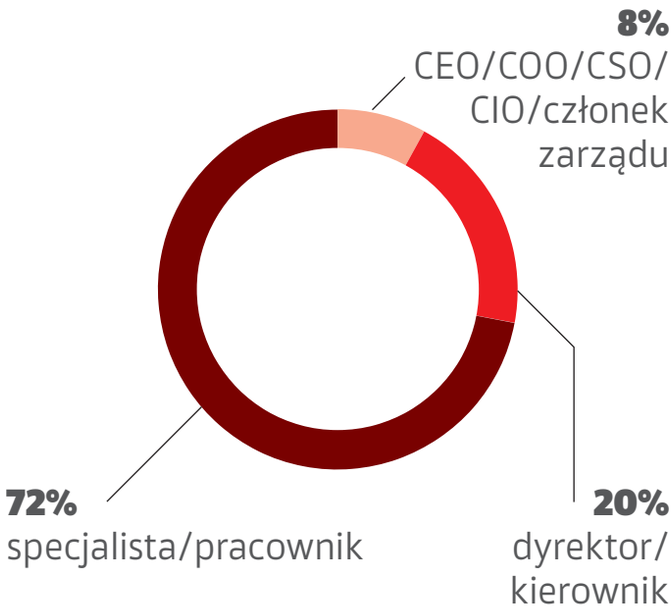
RESPONDENCI WG WIELKOŚCI PRZEDSIĘBIORSTWA



RESPONDENCI WG BRANŻY



RESPONDENCI WG STANOWISK



Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland reprezentuje ponad 45 innowacyjnych firm tworzących polski przemysł IT-security. Klaster wspiera rozbudowę i eksport krajowych usług oraz produktów, pomaga wypracowywać kluczowe polityki publiczne i regulacje, a także upowszechnia wiedzę branżową edukując rynek. #CybermadeInPoland to jedna z zaledwie dwóch instytucji w Europie Środkowo- Wschodniej, które otrzymały akredytację Europejskiej Organizacji Cyberbezpieczeństwa, umożliwiającą nadawanie znaku „Cybersecurity Made in Europe". Klaster reprezentuje także cały region środkowej Europy na platformie Global EPIC, zrzeszającej ponad trzydzieści ekosystemów cyberbezpieczeństwa z czterech kontynentów.

#CyberMadeInPoland

BADANIE COMPUTERWORLD

PARTNERZY RAPORTU