2022

Raport ESET ws. opinii sektora MŚP o cyberbezpieczeństwie

CYBER-RYZYKO SKŁANIAJĄCE MŚP KU ROZWIĄZANIOM KLASY ENTERPRISE

Digital Security

Progress. Protected.

SKALOWANIE BEZPIECZEŃSTWA:

Czy MŚP postawią na wykrywanie zagrożeń i reagowanie na nie, aby pójść dalej w rozwoju swojego bezpieczeństwa?

Michal Jankech
Wiceprezes ESET ds. segmentu
Małych i Średnich Przedsiębiorstw

"

Problemy w interesach chodzą trójkami, a nawet czwórkami. Niczym trójkąt bermudzki, Cerber lub czterej jeźdźcy apokalipsy. Jak zwał, tak zwał. Jeśli zarządzacie bezpieczeństwem cyfrowym w małym lub średnim przedsiębiorstwie, wiecie, że problemy z nim mają trzy oblicza: braki w personelu, braki w dojrzałości pracowników działu bezpieczeństwa, braki w wiedzy o odpowiedzialności za bezpieczeństwo oraz znajomości technologii. Problemy te wynikają z budżetu i zasobów. Czym jest problem numer cztery? Uwarunkowania prowadzenia działalności podyktowane czynnikami społecznymi, politycznymi i gospodarczymi.

SKALOWANIE BEZPIECZEŃSTWA:

Przed pandemią COVID-19 sektory takie jak technologiczny, detaliczny, telekomunikacyjny, a nawet bezpieczeństwa IT radziły sobie dobrze, rozwijając się wręcz w przewidywalny sposób. W tle tego rozwoju miała miejsce transformacja cyfrowa. Ugruntowały się nowe formy handlu, łączności, usług i produktów, lecz niemal nic nie wskazywało pełni skali i możliwości cyfryzacji. COVID-19 zresetował transformację cyfrową. Rozpoczęła się presja na wzrost wydajności i usprawnienie procesów – całe rzesze pracowników starały się pracować zdalnie poprzez platformy do współpracy w chmurze, od Zoom po MS Teams. W ten sposób cyfryzacja zyskała drugie życie.

Budżety na IT topniały i puchły, i tak zmienił się sposób, w jaki pracujemy, handlujemy i robimy zakupy. Jednocześnie zaczęto na poważnie interesować się bezpieczeństwem elektronicznym, przez co małe i średnie przedsiębiorstwa (MŚP) zwróciły uwagę na bezpieczeństwo biura w chmurze oraz bardziej zaawansowane rozwiązania do wykrywania zagrożeń i reagowania na nie. Lata 2020-2022 dały ku temu silną motywację. Przypomnijmy sobie o atakach Kaseya, na Microsoft Exchange, czy Emotet, a także wielu atakach webowych, które pogłębiły obawy przed ransomware.

SKALOWANIE BEZPIECZEŃSTWA:

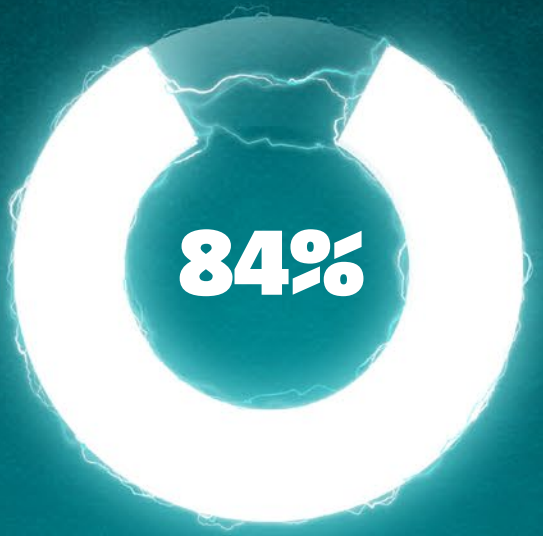
Współcześnie problem jest bardziej skomplikowany i nie dotyczy wyłącznie braków kadrowych na rynku, braków w podaży mikroprocesorów, czy fali „Wielkiej Rezygnacji" – oczy świata zwrócone są ku wojnie na Ukrainie, która według korespondentów w Europie jest kolejną przyczyną cyberataków. Media donoszą o zagrożeniach zakłócenia działalności gospodarczej równie często, co o celach politycznych państw.

O ile wszystkie firmy muszą liczyć się z powyższymi problemami i mnogością innych zagrożeń dla bezpieczeństwa, MŚP muszą zająć się nimi z „gorszej pozycji". Można twierdzić, że takiej elastyczności i przedsiębiorczego ducha trzeba oczekiwać od małych i średnich firm, lecz niestabilność gospodarcza po pandemii wzmogła zapotrzebowanie na cyberbezpieczeństwo, które ma rozwiązywać konkretne problemy i być skalowalne.

Tegoroczne badanie w sektorze MŚP służy ustaleniu opinii firm o cyberbezpieczeństwie w ujęciu kadr, dojrzałości technicznej i obciążenia finansowego. Zobaczmy, jak wspomniane wydarzenia i zagadnienia bezpieczeństwa odmieniły opinię o bezpieczeństwie cyfrowym małych i średnich przedsiębiorstw.

MŚP SĄ FUNDAMENTEM ŚWIATOWEJ GOSPODARKI

wszystkich firm w Europie i Ameryce Płn. to Małe i Średnie Przedsiębiorstwa



MŚP uważa, że **rozwój technologii** umożliwia ich rozwój

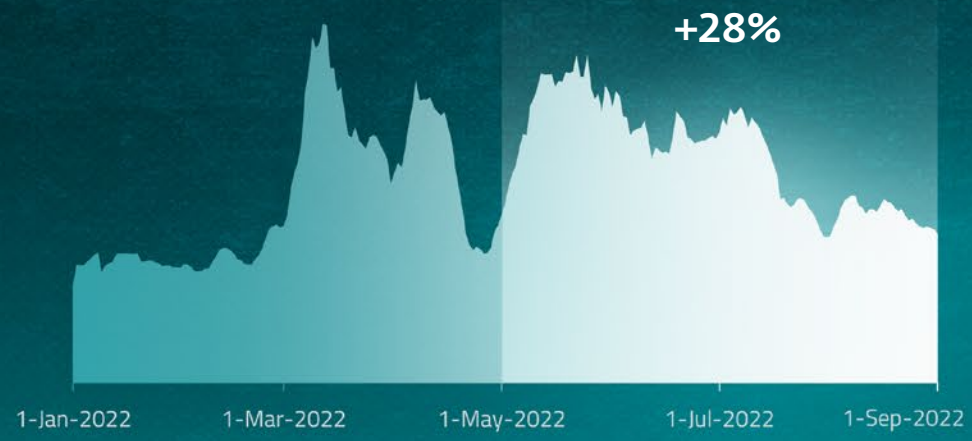
MŚP MAJĄ PROBLEMY Z OCHRONĄ SWOJEJ DZIAŁALNOŚCI – TAK WYNIKĄ Z OSTATNICH RAPORTÓW ESET WS. ZAGROŻEŃ

20% wzrost liczby wykrytych zagrożeń

MŚP jest przekonanych, że **wojna cybernetyczna** jest faktycznym zagrożeniem dla wszystkich

MŚP WIDZĄ WZROST LICZBY ZAGROŻEŃ ATAKAMI WEBOWYMI I E-MAILOWYMI

Część najgłośniejszych ataków malware została zrealizowana poprzez sieć web i e-mail. MŚP mogą określić priorytet przyszłych inwestycji w bezpieczeństwo, chroniących narzędzia i aplikacje do współpracy.



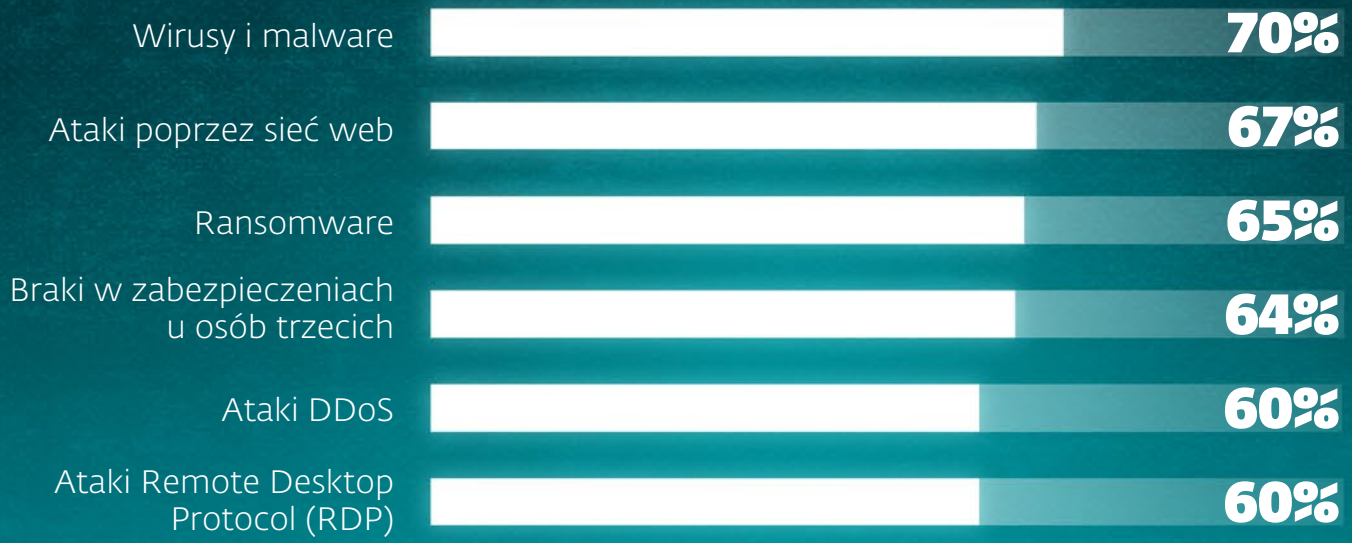
28% wzrost liczby ataków przez sieć web

66% wzrost liczby formularzy przesyłanych e-mailem celem kradzieży loginów do Outlooka

OPINIA MŚP O CYBERBEZPIECZEŃSTWIE

Firmy są świadome wielu rodzajów ryzyka i zagrożeń na polu cyberbezpieczeństwa, lecz nie wierzą, że są w stanie poradzić sobie ze wszystkimi. Największe obawy budzi kwestia narażenia pracowników na ataki malware, zwłaszcza poprzez sieć web; na drugim miejscu są ataki ransomware i braki w zabezpieczeniach u osób trzecich.

Największe obawy wobec cyberbezpieczeństwa na kolejny rok



OPINIA MŚP O CYBERBEZPIECZEŃSTWIE

Co jest przyczyną tych obaw? Zaskakującą informacją może być to, że MŚP widzą główną przyczynę w braku wiedzy ich pracowników o cyberbezpieczeństwie. Czynnik ten wyprzedza nawet skutki uboczne wojny na Ukrainie, czy ciągłą pracę zdalną po pandemii COVID-19. Oba te powody przyczyniły się do większych nakładów na cyberbezpieczeństwo w wielu firmach MŚP – czy oznacza to, że „zajęto się już cyberbezpieczeństwem" i jest ono problemem mniejszym, niż wiedza o cyberbezpieczeństwie?

5 największych czynników wzmagających ryzyko cyberataków wg opinii MŚP:

43%

Braki w wiedzy pracowników o cyberbezpieczeństwie

37%

Ataki rządowe z powodu wojny na Ukrainie

34%

Słabe strony w ekosystemie kontrahentów i dostawców

32%

Dalsza praca hybrydowa lub zdalna

31%

Korzystanie z RDP

Podane wartości były pierwszym wskazaniem respondentów, którzy mieli możliwość wyboru 3 opcji.

OPINIA MŚP O CYBERBEZPIECZEŃSTWIE

Firmy widzą, że jest wiele do zrobienia. Najważniejszymi ich problemami są dziś nadążanie za najnowszymi cyberzagrożeniami oraz technologią bezpieczeństwa, która ma zagrożenia te zwalczać. Problemy te można rozwiązać pieniędzmi, jednak ograniczenia budżetowe są barierą, która ogranicza taką możliwość.

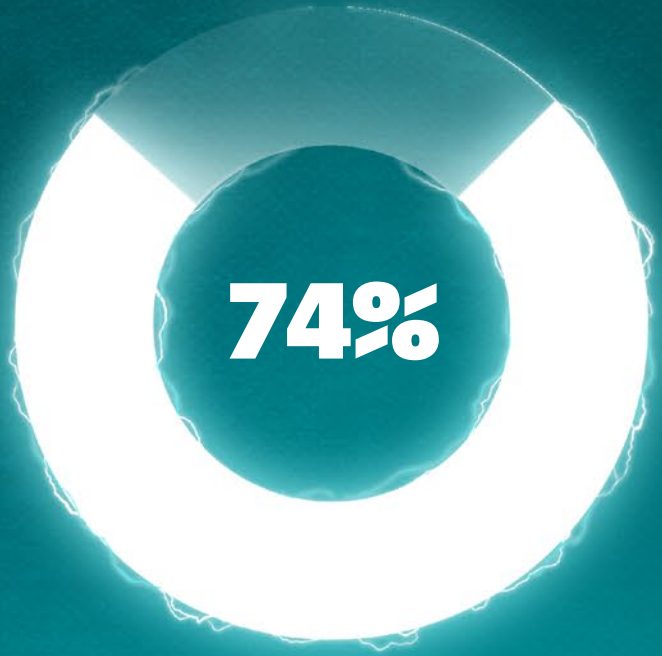
W jaki sposób firmy określą swoje budżety w obliczu niestabilności gospodarczej po pandemii oraz wojny w Europie? Pewnie znacie powiedzenie że „kto najgłośniej krzyczy, dostaje najwięcej".

Ograniczony budżet / brak inwestycji w cyberbezpieczeństwo należą do trójki największych problemów z cyberbezpieczeństwem w działach IT sektora MŚP

MŚP CZUJĄ SIĘ BARDZIEJ PODATNE NA ZAGROŻENIA NIŻ DUŻE PRZESIĘBIORSTWA...

Skoro ze wszystkich firm to właśnie MŚP zwykle sądzą, że to właśnie przez ich wielkość są podatniejsze na cyberataki niż duże firmy, to właśnie MŚP najlepiej dostrzegają problem cyberzagrożeń.

74% MŚP jest przekonanych, że ich wielkość czyni je podatniejszymi na cyberataki niż duże firmy.



MŚP CZUJĄ SIĘ BARDZIEJ PODATNE NA ZAGROŻENIA NIŻ DUŻE PRZESIĘBIORSTWA...

MŚP sądzą, że największe ryzyko dla nich stanowią incydenty skutkujące utratą danych lub znacznymi skutkami finansowymi. Taka ocena ryzyka wydaje się być dobrze uzasadniona. W ciągu ostatniego roku dwie trzecie MŚP spotkało się z zagrożeniem dla danych – w większości przypadków badanie takich zdarzeń zajęło nawet 3 miesiące, i kosztowało firmy sporo pieniędzy. Łączny koszt skutków ataku elektronicznego sięgnął średnio niemal 220 000 € na firmę – to są już duże pieniądze.

Największe obawy MŚP wobec skutków cyberataków dla ich działalności:

Podane wartości były pierwszym wskazaniem respondentów, którzy mieli możliwość wyboru 3 opcji.

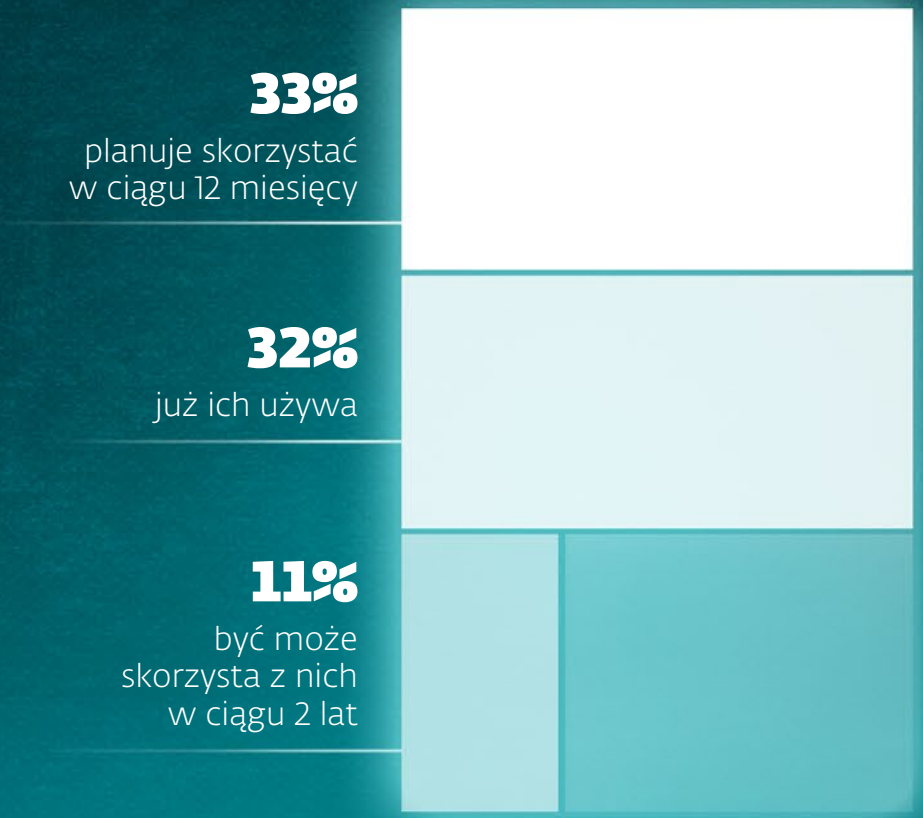
1% nie widzi żadnych problemów

ROSNĄCY APETYT?

Typową reakcją na powyższe incydenty są: nakłady na szkolenie pracowników IT, co nie powinno dziwić ze względu na niewielką wiedzę pracowników o cyberbezpieczeństwie, która dla MŚP jest źródłem największych obaw. Wiele firm przeprowadza również audyty i nabywa nowe narzędzia do cyberbezpieczeństwa.

Zdumiewający jest ogromny popyt na narzędzia do wykrywania zagrożeń i reagowania na nie. Zwykle korzystają z nich duże firmy, bo chcą dobrze wiedzieć, co dzieje się w ich sieciach i móc ustalić, co jest przyczyną incydentów związanych z cyberbezpieczeństwem. MŚP dysponując takimi możliwościami mogą bezpośrednio zająć się najnowszymi zagrożeniami, korzystając z innowacyjnych narzędzi klasy enterprise.

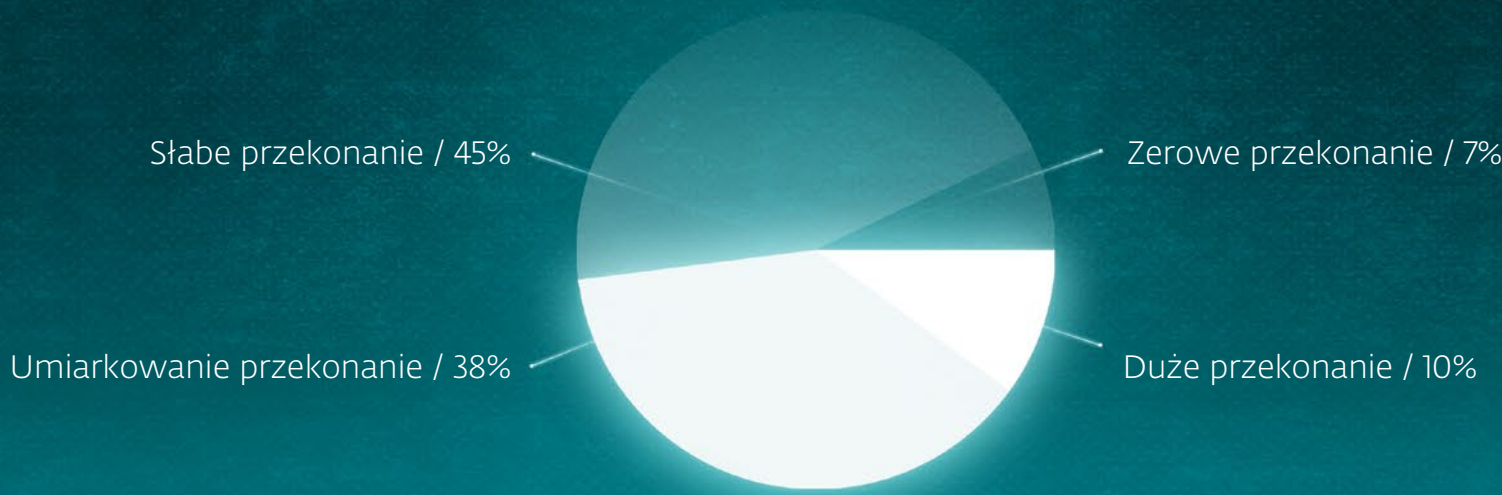
Wykorzystanie rozwiązań EDR / XDR / MDR



ROSNĄCY APETYT?

Nie powinno dziwić, iż mniej niż połowa firm jest średnio lub wysoce przekonana o swojej odporności na cyberataki. Odzwierciedla to ich obawy wobec wiedzy pracowników o cyberbezpieczeństwie, dostępie do niezależnych specjalistów i późnym reagowaniu na ataki.

Ogólne przekonanie o odporności na cyberataki w ciągu kolejnych 12 miesięcy jest słabe



Jedynie **48% firm** MŚP jest umiarkowanie lub dobrze przekonana o swojej odporności na cyberataki

ROSNĄCY APETYT?

Na pytanie o pewność wobec skuteczności własnych złożonych procesów bezpieczeństwa IT, np. badania zagrożeń, 71% MŚP jest ich wysoce pewna, zaś tylko 32% ankietowanych podało, że korzysta z produktów ‘endpoint’ do wykrywania zagrożeń i reagowania na nie. Taki kontrast świadczy albo o nadmiernej pewności lub konieczności poprawy wiedzy o tym, co daje przejście na rozwiązania do wykrywania zagrożeń i reagowania na nie.

MŚP mają największą pewność w następujących dziedzinach:

32%

Przekonanie o dobrej **wiedzy** pracowników IT na temat cyberbezpieczeństwa

30%

Prędkość rozpoznawania i izolowania zagrożeń oraz reagowania na nie

27%

Możliwości badania zagrożeń

ROSNĄCY APETYT?

Jest to zagadnienie podobne do problemu tego, co było pierwsze, jajko czy kura? MŚP widzą, że badanie zagrożeń jest przydatne i sądzą, że rozwiązania do wykrywania zagrożeń i reagowania na nie mogą się sprawdzić. Jednocześnie dość mały odsetek firm korzysta z takich narzędzi i ma znaczne braki w dojrzałości ich działów IT na polu bezpieczeństwa, a także w nakładach na cyberbezpieczeństwo – tym nie zajmuje się wiele małych i średnich firm.

Ocena wyników badania cyberbezpieczeństwa firm w 2022 r. wskazuje na brak skutecznej strategii cyberbezpieczeństwa, która zlikwiduje niedociągnięcia i zwiększy poziom odporności na cyberataki. Jeżeli problem ten rozwiązujemy stosując w przemyślany sposób, w odpowiedniej skali narzędzia endpoint do wykrywania zagrożeń i reagowania na nie, firmy mogą liczyć na większy spokój ducha i skupić się na podstawowych kompetencjach, rozwoju oraz innowacji. Mamy nadzieję, że raport ten skłoni do ważnych przemyśleń i pomoże ustalić, jak bardzo potrzebna jest taka przemiana na polu cyberbezpieczeństwa.

Digital Security
Progress. Protected.

kontakt: **handel@dagma.pl**