**Mały i średni biznes przygotowany na cyberataki tak samo, jak duże firmy**

*Raport Cisco obala mity dotyczące bezpieczeństwa cyfrowego małych i średnich firm*

**Sektor MŚP w wielu wypadkach stanowi trzon gospodarki. Tylko w Polsce, w 2019 roku było na tym rynku prawie 2,1 miliona podmiotów, zatrudniających blisko 10 milionów pracowników[[1]](#footnote-1). Małe i średnie przedsiębiorstwa na całym świecie stoją w obliczu bezprecedensowych wyzwań, zwłaszcza mając na uwadze zmiany, których doświadczają teraz i które wprowadzają nowy porządek ich funkcjonowania. W warunkach masowego przejścia na model pracy zdalnej, cyberbezpieczeństwo stało ważniejsze niż kiedykolwiek. Mały i średni biznes musi niejednokrotnie udowadniać, że jest odpowiednio zabezpieczony i przygotowany do pracy w świecie cyfrowym. Cisco publikuje raport „[Big Security in a Small Business World](https://www.cisco.com/c/en/us/products/security/smb-report-2020.html?CCID=cc000160&DTID=oblgcdc000651&OID=rptsc021237" \t "_blank)”, który prezentuje, w jaki sposób małe i średnie organizacje wykorzystują cyberbezpieczeństwo do rozwoju swojej działalności.**

**Warszawa, 14 maja 2020 r.** – W badaniu Cisco wzięło udział 500 przedstawicieli małych i średnich firm z całego świata. Raport pokazuje nie tylko to, jak poważnie traktują one kwestię bezpieczeństwa w cyfrowych czasach, ale również prezentuje innowacyjne i przedsiębiorcze podejście, które przynosi realne korzyści.

Na łamach raportu eksperci Cisco analizują i obalają najpopularniejsze mity, które krążą wokół kwestii bezpieczeństwa cybernetycznego małych i średnich przedsiębiorstw i tego jak firmy z tego sektora wykorzystują swoje zasoby w tym zakresie.

**Mit: osoby na kierowniczych stanowiskach w MŚP nie traktują poważnie bezpieczeństwa i prywatności danych**

Odpowiedzi uczestników badania odpowiadających w firmach za kwestie IT potwierdzają, że to twierdzenie jest dalekie od prawdy, przytaczając trzy główne argumenty: poufność danych, edukacja oraz poparcie zarządu.

90% osób podejmujących decyzje w kwestiach IT w małych i średnich przedsiębiorstwach przyznaje, że znają programy ochrony danych osobowych, które są realizowane w ich organizacjach. Co ciekawe, w przypadku dużych firm, ten odsetek jest wyższy jedynie o jeden procent.

To samo dotyczy kwestii świadomości w zakresie cyberbezpieczeństwa. Sektor MŚP nie pozostaje w tyle za dużymi firmami jeżeli myślimy o poziomie wiedzy dotyczącej cyberryzyk. Prowadzenie obowiązkowych, regularnych działań edukacyjnych na tym polu potwierdza 84% respondentów badania Cisco. Takiej samej odpowiedzi udzieliło tylko 4% więcej reprezentantów większych firm. 87% kadry kierowniczej w małych i średnich przedsiębiorstwach zgadza się z faktem, że bezpieczeństwo ma wysoki priorytet w ich organizacji. Na tym polu pozostają oni jedynie odrobinę w tyle za dużymi organizacjami (90%).

„Często słyszymy od naszych klientów, i sami się z tym zgadzamy, że kwestia bezpieczeństwa musi przenikać całe przedsiębiorstwa, aby firmy mogły mieć jakikolwiek realny wpływ na jego poziom, a wsparcie ze strony kadry kierowniczej ma dla tej kwestii kluczowe znaczenie. Jest to tak samo prawdziwe stwierdzenie dla małego i średniego przedsiębiorstwa, jak i dla większej organizacji. Warto zaznaczyć, że w większości przypadków, łatwiej jest to osiągnąć w mniejszym, bardziej zwinnym środowisku” – mówi Mateusz Pastewski, Menedżer ds. Sprzedaży Rozwiązań Cyberbezpieczeństwa Cisco Polska.

Bazując na wynikach badania Cisco, można stwierdzić, że małe i średnie przedsiębiorstwa mogą pochwalić się wysoką kulturą organizacyjną skupioną wokół bezpieczeństwa i prywatności danych. Ponad dwie trzecie respondentów ze wszystkich branży, którzy wzięli udział w badaniu stwierdziło, że kierownictwo w ich organizacjach nadało bezpieczeństwu wysoki priorytet.

**Mit: małe i średnie przedsiębiorstwa borykają się z innymi zagrożeniami niż większe firmy**

Eksperci Cisco porównali rodzaje cyberataków, których doświadczały firmy z sektora MŚP oraz duże przedsiębiorstwa w ciągu ostatniego roku. Sprawdzili również jakie czasy przestojów spowodowanych atakami zanotowały przedsiębiorstwa.

W ubiegłym roku 24% małych i średnich przedsiębiorstw musiało stawić czoła przestojom trwającym ponad osiem godzin z powodu najpoważniejszego naruszenia bezpieczeństwa, w stosunku do 31% większych organizacji. Co ciekawe, aż 75% firm z sektora MŚP doświadczyło przestojów krótszych niż 8 godzin (68% w przypadku większych firm).

Zarówno przedstawiciele sektora MŚP, jak i ich koledzy z większych przedsiębiorstw zgodnie przyznali, że najwięcej szkody (przestoje dłuższe niż 24 godziny) powodują ataki oparte o ransomware. Co ciekawe, w przypadku mniejszych organizacji dość nisko uplasowały się ataki typu DDoS (miejsce 9 na liście 10 najbardziej destrukcyjnych typów ataków), ale zajmują one wysokie (3 na 10) miejsce w przypadku organizacji zatrudniających ponad 10 000 pracowników. Z drugiej strony, małe organizacje częściej niż duże padają ofiarą phishingu.

Cyberprzestępcy, którzy dystrybuują złośliwe oprogramowanie typu „wiper” mają szczególny cel, jakim jest zniszczenie danych lub zakłócenie pracy systemów. Zarówno dla małych i średnich przedsiębiorstw, jak i dużych firm posiadających więcej niż 10.000 pracowników, złośliwe oprogramowanie tego typu powodowało w ostatnim roku przestoje w pracy trwające od 17 do 24 godzin.

Jednym z głównych problemów, z którymi borykały się firmy sektora MŚP było wykradanie danych dostępowych, co tylko w ciągu ostatniego roku powodowało średnio 17-24 godzinne przestoje.

„W odróżnieniu od złośliwego oprogramowania, którego celem jest wykradzenie lub zaszyfrowanie danych oraz żądanie okupu za ponownie uzyskanie dostępu do nich (ransomware), za atakami typu wiper nie zawsze stoi motywacja finansowa. Czasami chodzi o sparaliżowanie bieżącej działalności firmy. Dla przedsiębiorstw jest to często najgorszy rodzaj ataku, ponieważ szanse na odzyskanie danych są znacznie mniejsze” – podsumowuje Mateusz Pastewski z Cisco.

**Mit: mniejsze firmy nie testują swoich planów cyberbezpieczeństwa**

Mogłoby się wydawać, że mali i średni nie mają czasu i środków na testowanie swoich środowisk cyberbezpieczeństwa. Według danych z raportu Cisco, tylko jeden procent firm MŚP nigdy nie testuje swoich planów bezpieczeństwa cyfrowego, a 4% przyznaje, że robi to rzadko. 12% firm realizuje takie działania regularnie co dwa lata, natomiast ponad jedna trzecia (36%) wykonuje testy roczne. Największy odsetek, bo aż 45% firm potwierdza cykliczne testy co 6 miesięcy.

Raport pokazuje również, że im więcej dostawców, z których rozwiązań korzystali ankietowani w małych i średnich firmach, tym dłużej trwały przestoje spowodowane naruszeniami bezpieczeństwa. Czas ten wahał się od średnio czterech godzin w przypadku jednego dostawcy do średnio ponad 17 godzin w przypadku ponad 50 dostawców. Dane te istotnie pokazują, że trend konsolidacji dostawców technologii cyberbezpieczeństwa ma znaczenie i przekłada się na utrzymanie jego wysokiego poziomu.

**Wyzwanie: zabezpieczenie pracowników zdalnych**

Biorąc pod uwagę nową rzeczywistość, małe i średnie firmy potrzebują strategii zabezpieczającej pracowników i urządzenia znajdujące się poza ich siedzibą, a jednocześnie zapewniającej elastyczność i szybkość reakcji, z których firmy te są znane. Raport Cisco zawiera rekomendacje dotyczące pokonywania tych wyzwań w kontekście tego, co wiemy o bezpieczeństwie MŚP:

* Po pierwsze, opanuj podstawy – łatanie luk w zabezpieczeniach, szkolenie pracowników, wdrażanie strategii zerowego zaufania z uwierzytelnianiem wieloskładnikowym oraz zabezpieczanie sieci, punktów końcowych, chmury i aplikacji.
* Po drugie, zrównoważ bezpieczeństwo z użytecznością. Pracownicy nie powinni musieć czytać w myślach specjalistów od bezpieczeństwa. Mają własne zadania do wykonania. Udostępnij takie zabezpieczenia, aby były bezproblemowe w ich pracy.
* Po trzecie, współpracuj z dostawcami zabezpieczeń, którzy pomagają uprościć infrastrukturę bezpieczeństwa, zamiast ją komplikować. Z danych Cisco wynika, że istnieje korelacja pomiędzy krótszym czasem przestoju spowodowanym naruszeniami, a liczbą wykorzystywanych dostawców rozwiązań bezpieczeństwa – im jest ich mniej i im bardziej są strategiczni, tym przestoje są krótsze.

Cały raport jest dostępny na stronie [Big Security in a Small Business World](https://www.cisco.com/c/en/us/products/security/smb-report-2020.html?CCID=cc000160&DTID=oblgcdc000651&OID=rptsc021237).

.:|:.:|:.

**O Cisco:**

Cisco (NASDAQ: CSCO) to światowy lider technologiczny zapewniający działanie Internetu od 1984 r. Pracownicy, partnerzy i produkty Cisco pomagają społeczeństwom łączyć się w bezpieczny sposób i już dziś korzystać z cyfrowych możliwości jutra. Dowiedz się więcej na www.newsroom.cisco.com. Cisco i logo Cisco to zastrzeżone znaki towarowe należące do Cisco i/lub jego podmiotów zależnych w U.S. i innych krajach. Pełna lista znaków towarowych Cisco dostępna jest pod adresem: www.cisco.com/go/trademarks. Znaki towarowe firm trzecich są ich własnością. Użycie słowa partner nie oznacza stosunku partnerstwa pomiędzy Cisco i inną firmą.

1. PARP, Raport o stanie sektora małych i średnich przedsiębiorstw w Polsce. Warszaw, czerwiec 2019 [↑](#footnote-ref-1)