**Jak zmienił się krajobraz cyberzagrożeń podczas pandemii?**

**W minionym roku cyberprzestępcy wykazywali się wyjątkową aktywnością. Miało to oczywiście w dużym stopniu związek z masowym przejściem pracowników biurowych na tryb pracy zdalnej. Atakujący często wykorzystywali gorzej zabezpieczonych użytkowników i ich urządzenia do prowadzenia szeroko zakrojonych kampanii cyberprzestępczych. Zdaniem ekspertów Cisco, w 2021 r. trudno oczekiwać, że prób ataków będzie mniej. Wzrośnie również skala cyberincydentów o bardziej złożonym charakterze.**

[W najnowszym raporcie Cisco](https://www.cisco.com/c/dam/en/us/products/collateral/security/threats-year-report.pdf) możemy przeczytać o tym w jakich obszarach cyberprzestępcy byli szczególnie aktywni w 2020 r.:

**Ataki na zdalne pulpity**

Pandemia sprawiła, że znacznie wzrosła popularność zdalnych pulpitów (RDP – Remote Desktop Protocol), czyli technologii, która pozwala na dostęp do komputera (np. biurowego) ze zdalnej lokalizacji. Bez wątpienia stanowi to wygodne rozwiązanie w sytuacji masowego przejścia na pracę zdalną, ale jednocześnie wzbudza wiele obaw w kontekście cyberbezpieczeństwa.

Obawy te dotyczą kradzieży danych uwierzytelniających, ataków typu man-in-the-middle (cyberatak, w którym atakujący umieszcza się na linii komunikacji między dwiema stronami) czy zdalnego wykonania kodu (luka w zabezpieczeniach, którą atakujący może wykorzystać do uruchomienia własnego kodu na komputerze lub serwerze). Każde rozwiązanie RDP, jeśli zostanie przejęte, umożliwia atakującemu dostęp do cyfrowych zasobów organizacji.

Wg ekspertów Cisco, firmy korzystające z wirtualnych pulpitów powinny wdrożyć specjalne środki bezpieczeństwa:

* Unikać podłączania zdalnych pulpitów bezpośrednio do sieci. Zamiast tego można zapewnić pracownikom dostęp do wszystkich niezbędnych zasobów za pomocą usługi VPN.
* Wdrożyć system uwierzytelniania wielopoziomowego – dodatkową warstwę bezpieczeństwa, umożliwiającą potwierdzenie tożsamości użytkowników.
* Blokować użytkowników, którzy podjęli wiele nieudanych prób logowania.

**Ransomware i „podwójne wymuszenie”**

W minionym roku ataki typu ransomware przybrały nowe formy. Przykładowo, pojawiły się liczniki odliczające czas, który ma użytkownik na wpłacenie okupu. Eksperci Cisco zajmujący się cyberbezpieczeństwem zaobserwowali, że coraz częściej zaatakowani użytkownicy otrzymują groźby nie tyle zaszyfrowania, co trwałego usunięcia danych.

Zmieniła się również skala ransomware, a ataki na poszczególne urządzenia często są jedynie narzędziem, która pozwala uzyskać dostęp do sieci organizacji. Gdy to już nastąpi, atak ransomware jest uruchamiany dopiero po tym, gdy atakujący wejdą w posiadanie danych firmy, w tym własności intelektualnej czy poufnych informacji handlowych. Często mamy wówczas wg ekspertów Cisco do czynienia ze zjawiskiem „podwójnego wymuszenia” – z jednej strony atakujący przejmują dane, które mogą wykorzystać i dalej monetyzować, z drugiej wymuszają okup za ich odszyfrowanie czy niewykasowanie, co ma na celu maksymalizację szkód ofiar i zysków atakujących.

Kwitnie również czarny rynek, na którym sprzedawane są np. dostępy do sieci firmowych. Nieuczciwi użytkownicy mogą zatem lepiej przygotować się do ataku i w jednym momencie rozesłać złośliwe oprogramowanie do większej liczby organizacji.

Co może zrobić biznes, żeby ustrzec się przed nowymi formami ransomware? Eksperci Cisco podkreślają, że najważniejsze jest kompleksowe podejście do kwestii cyberbezpieczeństwa, na które składa się zapobieganie, lokalizowanie zagrożeń i odpowiadanie na nie. Ekosystem cyberbezpieczeństwa powinien obejmować m.in.:

* Bezpieczeństwo poczty e-mail
* Zarządzanie aktualizacjami i łatkami
* Monitoring systemów i sieci
* Segmentację sieci
* Backup i przywracanie systemu po awarii
* Polityki i procedury
* Szkolenia

**Wykradane hasła i “credential dumping”**

Kradzież danych do logowania stanowi drugą najczęstszą aktywność cyberprzestępców podczas włamań do firmowych systemów bezpieczeństwa. Posługując się wykradzionym loginem i hasłem, mogą oni pozostać niezauważeni w sieci danej organizacji. Podobnie jak w przypadku ransomware, również kradzież danych do logowania służy za punkt wyjścia do dalszych ataków i wykradania kolejnych danych do logowania. Zjawisko to nazywa się „credential dumping”. Cyberprzestępcy nie poprzestają na uzyskaniu dostępu do jednego urządzenia. Często z jego poziomu chcą wejść w posiadanie haseł do innych elementów firmowej infrastruktury IT, przeszukując różne obszary systemów, gdzie tego typu informacje są przechowywane. Jak się zabezpieczyć przed tym procederem? Eksperci Cisco radzą, aby:

* Monitorować dostęp do baz danych LSASS (Local Security Authority Subsystem Service) i SAM (Storage Area Management).
* Monitorować logi w celu wyszukiwania nieplanowych, podejrzanych aktywności w kontrolerach domen.
* Wyszukiwać nieoczekiwane i nieprzydzielone połączenia z adresów IP do kontrolerów domen.

Więcej o tym jak działali cyberprzestępcy w roku 2020 można przeczytać w najnowszym raporcie Cisco: [Defending Against Critical Threats: A 12 month roundup](https://www.cisco.com/c/dam/en/us/products/collateral/security/threats-year-report.pdf).

.:|:.:|:.

**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.