**Ataki ransomware to numer 1 w tym roku. Jak firmy mogą się zabezpieczyć?**

* **Najczęściej przeprowadzanym atakiem na duże i średnie firmy są incydenty ransomware – wynika z danych „Acronis Mid-Year Cyberthreats Report 2023”.**
* **Wprowadzeniem do tych ataków są kampanie phishingowe – liczba fałszywych wiadomości w I poł. 2023 r. wzrosła aż o 464% w porównaniu z analogicznym okresem zeszłego roku.**
* **Kluczowy wpływ na minimalizację ryzyka ataku na firmową sieć IT mogą mieć stosowanie rozwiązań Endpoint Security (zwłaszcza EDR - Endpoint Detection and Response) oraz szkolenia pracowników.**

Ransomware króluje wśród cyberataków – wynika z raportu Acronis. na celowniku są przede wszystkim duże i średnie firmy, ale problem nie omija też administracji, służby zdrowia i innych instytucji publicznych . Cyberprzestępcy paraliżują za pomocą złośliwego oprogramowania systemy bezpieczeństwa i blokują dostęp do urządzeń czy danych. Udaje im się to, bo wcześniej uzyskali dostęp do sieci IT atakowanych firm.

*– Hakerzy zazwyczaj żądają okupu od ofiary za możliwość odblokowania dostępu do systemu. To standardowy element ich działania w ramach ataku ransomware. Jednak zanim uda im się wprowadzić złośliwe oprogramowanie do sieci IT zaatakowanej firmy lub instytucji, wcześniej muszą zdobyć do niej dostęp. Próby złamania systemów zabezpieczeń to rzecz trudna i ryzykowna, dlatego hakerzy często korzystają z innej metody, która okazuje się prostsza i w dodatku bardziej skuteczna. Mam na myśli phishing, czyli rozsyłanie fałszywych wiadomości z linkami. Ofiara po kliknięciu w link nieświadomie przekazuje dostęp do swojego urządzenia, a to już znacznie skraca drogę dostępu do firmowych systemów –* mówi Patrycja Tatara, ekspertka ds. cyberbezpieczeństwa w Sprint S.A.

W pierwszej połowie 2023 r. drastycznie wzrosła liczba fałszywych wiadomości. Specjaliści Acronis w swoim raporcie mówią o 464% w stosunku do I poł. 2022 r. Wśród nich 73% to klasyczne maile phishingowe, czyli wiadomości z fałszywymi linkami, umożliwiającymi hakerom dostęp do danych. Warto zauważyć, że rośnie rola sztucznej inteligencji w cyfrowej przestępczości.

*– AI zna języki programowania, zatem bywa wykorzystywana także do tworzenia linijek kodu w złośliwych aplikacjach. I tu, wracając do ataków ransomware, pojawia się kolejne zagrożenie – kradzież danych. Blokowanie dostępu do nich może również służyć jako zasłona dymna do pozyskania informacji z systemu, do którego ofiara tymczasowo utraciła dostęp –* dodaje Patrycja Tatara ze Sprint S.A.

Nielegalne zdobycie danych, według raportu Acronis, zajmuje drugie miejsce wśród najczęściej przeprowadzanych cyberataków. Zarówno sama blokada dostępu do danych, jak i ich kradzież, mogą oznaczać dla firmy kłopoty finansowe. Na skutek działań hakerów może dojść do czasowego spowolnienia lub zaniechania procesów – np. produkcji lub świadczenia usług. Przywrócenie wszystkiego do normy może oznaczać wysokie koszty.

**Jak działa Endpoint Security?**

W jaki sposób można zminimalizować ryzyko ataków ransomware i phinshingowych? Najpierw warto zadbać o odpowiedniej jakości oprogramowanie na stacjach końcowych użytkowników. W ochronie przed tego typu atakami najlepiej korzystać z rozwiązań typu EDR - Endpoint Detection and Response. Zadaniem tego systemu jest zabezpieczenie i monitorowanie poszczególnych urządzeń w sieci, czyli wszystkich komputerów i serwerów, a także smartfonów znajdujących się w organizacji. Istotną cechą tego zabezpieczenia jest uczenie maszynowe, które analizuje zachowania poszczególnych urządzeń/użytkowników, co pozwala na szybkie wykrycie anomalii, czyli prawdopodobnego ataku. Dzięki temu jeśli dojdzie do zainfekowania któregokolwiek z nich punktów systemu IT, zostaje on natychmiast odizolowany, żeby atak nie objął całej sieci firmowej oraz innych urządzeń.

**Także szkolenia pracowników zmniejszają ryzyko**

Pozytywny wpływ na poziomi bezpieczeństwa firmy ma również inwestycja w edukację pracowników.

*– Hakerzy często rozpoczynają atak od wysłania wiadomości do szeregowych pracowników firmy, ponieważ istnieje spora szansa, że to właśnie taka osoba kliknie w zainfekowany link. Świadomość cyberzagrożeń wśród zatrudnionych jest nadal nierówna i zazwyczaj mniejsza niż w przypadku specjalistów IT. Cyklicznie szkolenia umożliwiają podniesienie poziomu wiedzy i wykształcenie dobrych praktyk, które podniosą odporność pracowników na manipulacje hakerów. A  te bywają czasem o wiele bardziej złośliwe niż maile phishingowe. Dziś każdy korzysta z narzędzi informatycznych na co dzień, więc wszyscy jesteśmy niejako pracownikami działu IT –* mówi Patrycja Tatara ze Sprint S.A.

Źródło: Sprint S.A.