NASK

CyberBHP

Jak chronić swoją firmę przed ransomware

Ransomware to jedno z najpoważniejszych cyfrowych niebezpieczeństw, na które w szczególności narażone są firmy i organizacje. Na czym polega to zagrożenie i jak się przed nim zabezpieczyć?

Cyberbezpieczeństwo w mikro-, małych i średnich przedsiębiorstwach (MŚP)

Ransomware

To złośliwe oprogramowanie, które powoduje blokadę urządzenia lub zaszyfrowanie znajdujących się w nim plików. Następnie przestępcy żądają pieniędzy w zamian za zlikwidowanie blokady, odszyfrowanie danych lub za obietnicę nieupubliczniania wykradzionych informacji.

730 000 zł

to szacowana średnia wysokość okupu po ataku ransomware w Polsce w 2021 roku.

77%

tyle polskich firm zetknęło się w 2021 roku z atakiem typu ransomware.

938

tyle razy w ciągu każdego tygodnia atakowane były polskie firmy w połowie 2022 roku.

Źródła: Sophos, Check Point Research

Jakie są oznaki infekcji?

- Komunikaty z żądaniem płatności w celu odblokowania plików lub całego urządzenia
- Brak możliwości zalogowania się do urządzenia
- Brak dostępu do plików lub zasobów sieciowych

NASK

W jaki sposób ransomware może trafić do Twojej firmy?

Zainfekowane wiadomości e-mail, niebezpieczne linki i załączniki

Słabe hasło do publicznie dostępnych usług
i brak wieloskładnikowego uwierzytelniania

Nieaktualizowane systemy operacyjne i aplikacje

Niebezpieczne i fałszywe strony WWW,
fałszywe reklamy na legalnych stronach

Zainfekowane urządzenie, np. dysk zewnętrzny, pendrive

Jak postępować w przypadku ataku?

Nie wyłączaj komputera, ale natychmiast odłącz go
od internetu (wyciągnij kabel sieciowy lub wyłącz Wi-Fi).

Od razu powiadom o incydencie przełożonego
oraz swój dział IT lub bezpieczeństwa.

Zgłoś sprawę do właściwego zespołu CSIRT i na policję.
Im więcej szczegółów podasz, tym skuteczniej
będą ścigani sprawcy ataku.

NIGDY NIE PŁAĆ OKUPU! Nie ma gwarancji, że Twoje pliki zostaną przywrócone albo że wpłata zapobiegnie publikacji skradzionych danych lub ich sprzedaży. Jeśli zapłacisz, sfinansujesz nielegalną działalność, a także jak pokazują statystyki – prawdopodobnie staniesz się obiektem kolejnych ataków.

NASK

Jak się chronić?

Twórz na bieżąco kopie zapasowe danych i zapisuj je na zewnętrznych dyskach bądź przechowuj w chmurze.

Aktualizuj oprogramowanie – szczególnie to, które obsługuje usługi dostępne z poziomu internetu, oraz aplikacje, z których korzystasz, np. przeglądarki, programy biurowe, pocztowe itp.

Używaj aktualnej wersji oprogramowania antywirusowego.

Nie klikaj w podejrzane linki lub załączniki, niezależnie od tego, czy znajdują się na stronie internetowej, czy w treści e-maila, SMS-a.

Zanim otworzysz plik dołączony do wiadomości zwróć szczególną uwagę na jego rozszerzenie. Te najbardziej podejrzane to: .com, .scr, .js, .jse, .rtf, .iso, .img, .htm, .html, .xlsx, .xlsm, .xls. Pamiętaj też, że złośliwy plik może być spakowany w archiwum, np. .zip/.rar/.iso.

Upewnij się, czy link zamieszczony w treści wiadomości prowadzi do znanej i zaufanej strony. Najedź kursorem na link (nie klikaj) i sprawdź u dołu przeglądarki lub programu pocztowego, jaki adres się wyświetla.

NASK

Finansowane ze środków Kancelarii Prezesa Rady Ministrów.
Publikacja wyraża jedynie poglądy autorów i nie może być utożsamiana z oficjalnym stanowiskiem Kancelarii Prezesa Rady Ministrów.