SEQRED

# RANSOMWARE – ZAGROŻENIE DLA SEKTORA MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTW

Obecna sytuacja związana z pandemią stała się katalizatorem zmian w funkcjonowaniu wielu biznesów. Transformacja cyfrowa, praca zdalna oraz nowe kanały komunikacji z klientem przyniosły wiele możliwości, ale i zagrożeń związanych z funkcjonowaniem w świecie nowoczesnych technologii. Jednym z zagrożeń, mogącym mieć katastrofalne skutki, jest ransomware – złośliwe oprogramowanie, które może doprowadzić do utraty lub wycieku wrażliwych danych. Ataki ransomware nasiliły się w związku z digitalizacją rzeczywistości, w której się znaleźliśmy.

## CZYM JEST RANSOMWARE?

**Ransomware** to rodzaj złośliwego oprogramowania, które po zarażeniu komputera szyfruje lub blokuje dostęp do danych zawartych na dyskach, a następnie informuje ofiarę o możliwości ich odzyskania po zapłaceniu „okupu".

MALWARE › ZASZYFROWANIE DANYCH › ŻĄDANIE OKUPU

## METODY INFEKCJI

**E-mail** zawierający złośliwy plik, link lub załącznik wysyłany z wykorzystaniem metod phishingu

**Internet / link** – podszywanie się pod znany serwis lub wykorzystanie podatności w serwisie

**Pobranie lub transfer plików** z wbudowanym trojanem infekującym komputer ofiary

**Advanced Persistent Threat (APT)** – celowany atak, który może doprowadzić do infekcji ransomware (np. Ryuk)

## JAK SIĘ ZABEZPIECZYĆ?

**Regularnie wykonuj kopie zapasowe**
Przechowuj je w bezpiecznym miejscu.

**Bądź czujny!**
Nie klikaj w nieznane linki czy reklamy i nie wchodź na podejrzane strony internetowe.

**Uważaj na e-maile**
Nie otwieraj podejrzanych załączników oraz nie klikaj w umieszczone w treści e-maila linki. Sprawdzaj nadawców oraz adresatów e-maili.

**Ogranicz dostęp**
Nie korzystaj z konta administratora, jeżeli nie jest to konieczne – chronisz w ten sposób dane systemowe.

**Aktualizuj oprogramowanie**
Część ataków na cel bierze istniejące luki w oprogramowaniu (np. przeglądarkach).

**Segmentuj swoją sieć**
Infekcja jednego komputera nie pozwoli na rozprzestrzenienie ataku.

**Next-generation firewall (NGFW)**
Prawidłowo skonfigurowany NGFW może zatrzymać atak już w początkowej fazie.

**Włącz dwuskładnikowe uwierzytelnianie**
Nawet jeśli przestępcy przejmą Twoje hasła, to nie będą mogli zalogować się na Twoje konto.

**Zadbaj o szkolenia dla pracowników**
Naucz pracowników zwracać uwagę na możliwe metody ataków.

**Dbaj o prywatność**
Im mniej osoby trzecie mogą dowiedzieć się o Tobie i Twojej firmie, tym trudniej będzie przygotować dedykowany atak (phishing).

## SKUTKI ATAKU: CO JEST DO STRACENIA?

**Utrata poufnych danych** – zablokowanie dostępu do danych. Możliwe upublicznienie danych przez atakującego.

**Przerwanie ciągłości działania** – blokada danych może doprowadzić do zawieszenia funkcjonowania firmy.

**Utrata reputacji** – wyciek poufnych danych lub przerwanie ciągłości działania może obniżyć wiarygodność firmy i zaufania klientów.

**Konsekwencje prawne** – brak odpowiednich zabezpieczeń oraz wyciek poufnych danych może doprowadzić do procesów sądowych i odpowiedzialności karnej.

## PRZYKŁADY ATAKÓW

Firma **Visser Precision** projektująca oraz produkująca elementy dla Boeinga, Tesli, SpaceX, Honeywella i Joe Gibbs Racing padła ofiarą ransomware DoppelPaymer. Przestępcy ujawnili poufne dane firmy z powodu nieopłacenia okupu.

**EDP** – gigant energetyczny z Portugalii padł ofiarą ransomware Ragnar Locker. Przestępcy żądają 10 milionów dolarów w zamian za 10 terabajtów wykradzionych dokumentów.

Firma konsultingowa **Cognizant** pracująca między innymi dla Facebooka padła ofiarą ransomware Maze. Atak miał wpływ na funkcjonowanie części klientów.

**University of California San Francisco** – 1 czerwca 2020 Shool of Medicine UCSF utraciła dostęp do części serwerów na skutek ataku ransomware. Uczelnia zapłaciła 1,14 mln dolarów za odyskanie dostępu do danych badawczych.

## ZOSTAŁEM ZAATAKOWANY. CO ROBIĆ?

Niektóre ransomware zostały pokonane (np. Simplelocker, Hakbit) i istnieją metody odszyfrowywania zainfekowanych danych. Szczegółowe informacje znajdziesz na stronach:

**NoMoreRansom!**
polska strona wsparcia dla ofiar ransomware

**ID Ramsomware**
narzędzie do identyfikacji ransomware oraz zbiór instrukcji w jaki sposób można odzyskać dane

**Kaspersky NoRansom FAQ**
zbiór pytań i odpowiedzi przygotowany przez firmę Kaspersky

Skontaktuj się z prawnikiem w celu ochrony swojej firmy oraz kontrahentów. Jeżeli masz kopie zapasowe to przywróć dane w bezpieczny sposób. **Wyczyść zainfekowane dyski. Przywróć system. Przeskanuj dokładnie komputer, następnie wgraj dane.** Ponownie przeskanuj komputer w celu upewnienia się, że infekcja się nie powtórzyła.

**Zalecamy, żeby nie płacić okupu.** Nie utwierdzaj przestępców w przekonaniu, że ich metoda działa. Dodatkowo nie masz gwarancji, że uzyskasz klucz deszyfrujący.

**Jeśli nie masz kopii zapasowych, płatność może być jedyną opcją. Nie dopuść do takiej sytuacji!**

**Jak usunąć? Co zrobić?** | **Płacić czy nie płacić?**

www.seqred.pl, e-mail: biuro@seqred.pl, tel. +48 22 292 32 23