5 INFEKCJI*
PRZEZ KTÓRE MOŻESZ ZBANKRUTOWAĆ

CO POWINIENEŚ WIEDZIEĆ O CYBERBEZPIECZEŃSTWIE

* na potrzeby publikacji przyjeto termin „infekcja" jako synonim ataku wirtualnego wirusa

ROMNY
CYBERBEZPIECZNI

WSTĘP

Tradycyjnie przyjmuje się, że na ataki cyberprzestępców są narażone sektory finansowy, energetyczny czy transportowy. Tymczasem zgodnie z przewidywaniami Europolu w 2017 r. pierwszoplanowym obiektem ataków będą wrażliwe dane medyczne pacjentów, przechowywane w słabo zabezpieczonych systemach. Blokada systemu informatycznego czy też wyciek danych o pacjentach mogą zdezorganizować pracę jednostki medycznej w takim stopniu, że nie będzie ona w stanie leczyć pacjentów, dopóki nie zapłaci wysokiego okupu cyberprzestępcom. Czy można uchronić się przed takim scenariuszem?

5 INFEKCJI, PRZEZ KTÓRE MOŻESZ ZBANKRUTOWAĆ

PONIŻEJ PRZEDSTAWIAMY KILKA WAŻNYCH INFORMACJI O TYM, CO NALEŻY WIEDZIEĆ, BY UCHRONIĆ SIĘ PRZED ATAKAMI CYBERPRZESTĘPCÓW.

Każdego dnia w pracy przywykamy do bakterii, wirusów i infekcji – w placówce medycznej to nie tylko codzienność, ale również źródło zarobków.

Czy znasz sytuacje, w których mogą one nie tylko nadwyrężyć Twój wizerunek, ale spowodować ogromne straty finansowe i doprowadzić Cię do upadłości? To cyberwirusy, cyberbakterie i cyberinfekcje – znacznie groźniejsze i jeszcze nierozpoznane, a na pewno dużo bardziej zaraźliwe.

W 2017 r. każdy, kto odwiedził serwer szpitala w Kole, mógł pobrać dane wszystkich pacjentów i pracowników placówki – od numerów PESEL, przez wyniki badań, dane z dokumentów tożsamości, po numery kont bankowych.

5 INFEKCJI, PRZEZ KTÓRE MOŻESZ ZBANKRUTOWAĆ

Taki atak to nie tylko olbrzymi cios wizerunkowy – to dochodzenie z prokuratury, pozwy o odszkodowanie i olbrzymie zagrożenie kradzieżą tożsamości. W pobranych dokumentach można było bowiem bez problemu znaleźć korespondencję pracowników i dane kont bankowych szpitala!

W 2018 r. w warszawskim ZOZ, który miał własny system rejestracji pacjentów i odbierania wyników badań, każdy z użytkowników mógł pobrać wyniki pozostałych klientów placówki.

Wraz z wynikami pacjenci pobierali też dane osobowe czy numery PESEL, a ani kierownik placówki, ani żaden z jego pracowników nie wiedział, jak łatwo można było zapobiec temu wyciekowi.

12 maja 2017 r. celem hakerów stały się szpitale należące do Narodowego Funduszu Zdrowia Wielkiej Brytanii. Komputery placówek zostały zablokowane, a lekarze poszukujący dokumentacji medycznej ujrzeli jedynie komunikat z żądaniem okupu.

Ten atak był jednym z wielu, podobne zdarzyły się również w Polsce. Szpitale w Wielkiej Brytanii odczuły go bardzo dotkliwie – wielu pacjentów musiało zostać przeniesionych do innych placówek, karetki były kierowane do innych szpitali, a część planowych zabiegów została odwołana.

Doświadczenie pokazuje, że placówki medyczne często stają się celem ataków cyberprzestępców, ponieważ gromadzone w nich dane osobowe to dla hakerów łakomy kąsek – kradzież tych danych nie tylko Ciebie narazi na ogromne straty finansowe i wizerunkowe, ale również dobra Twoich pacjentów.

Twoja placówka może być zagrożona nie tylko przez celowe działanie nieuczciwej konkurencji czy hakerów – wystarczy, że któryś z Twoich pacjentów był nieostrożny i logując się do systemu przypadkowo wprowadził do Twojego systemu złośliwego wirusa.

Dlatego koniecznie sprawdź, czy jesteś narażony na atak!

CO MOŻE ZAKAZIĆ TWÓJ SYSTEM?

W KOLEJNYCH CZĘŚCIACH BOOKLETU, OPIS POZOSTAŁYCH INFEKCJI

INFEKCJA 2
RANSOMWARE

Ransomware to infekcja złośliwa. Atakuje komputery, blokuje ich funkcje i zmusza użytkownika do zapłacenia haraczu w zamian za przywrócenie dostępu do komputera. Można się nią zarazić przez pobranie pliku, a nawet przez wiadomość tekstową!

Ciemną stroną skoku technologicznego jest zwiększone ryzyko utraty danych w wyniku działalności cyberprzestępców.

INFEKCJA 2: RANSOMWARE

Scenariusz ataków tego rodzaju najczęściej jest następujący: Do pracowników wysyłana jest seria maili z pozornie legalną treścią (np. zaproszenia na kongres naukowy, udział w projekcie badawczym itd.). Po otwarciu maila automatycznie instaluje się nielegalne oprogramowanie (tzw. malware), które skanuje zawartość sieci, blokuje dostęp do danych pacjentów i przesyła je w zaszyfrowanej formie do komputera, z którego pochodzi atak. Wobec utraty danych oraz blokady systemu placówka musi zawiesić działalność medyczną, a dyrekcja otrzymuje e-mail z żądaniem zapłaty w zamian za zwrot danych oraz odblokowanie systemu.

Podmiotami zagrożonymi złośliwym oprogramowaniem są placówki, które mają:

- publiczne serwery, np. do przechowywania dokumentacji medycznej, udostępniania wyników badań
- własną stronę internetową
- aplikacje dla pacjentów
- sieci lokalne, czyli np. komputery łączące się z siecią Wi-Fi, drukarkami, maszynami ksero etc.
- możliwość uruchamiania zewnętrznych nośników – płyt CD z wynikami badań, pamięci USB etc.

Niestety, żadna nowoczesna firma nie może się obyć bez powyższych udogodnień, dlatego Ransomware i złośliwe oprogramowanie są jedną z najczęstszych infekcji dotykających biznes, w tym placówki medyczne.

DZIAŁANIA PROFILAKTYCZNE POLEGAJĄ NA:

- regularnym szkoleniu pracowników z zasad bezpieczeństwa
- atakach socjotechnicznych
  (testowanie pracowników i systemów w zakresie reakcji na cyberatak)
- regularnym skanowaniu sieci w poszukiwaniu podatności i słabych punktów, które mogą umożliwić atak cyberprzestępcom

Atak na brytyjską służbę zdrowia w 2017 r. złośliwym oprogramowaniem był możliwy z wielu powodów:

- **z siecią służby zdrowia łączyło się wielu partnerów i dostawców,**
- **rozległa infrastruktura była trudna do kontrolowania,**
- **zewnętrzni użytkownicy nie dbali o bezpieczeństwo tak skrupulatnie, jak powinni,**
- **aktualizacja systemu i wszystkich jego części nie była dobrze przeprowadzona.**

Infekcja, kiedy tylko dostała się do systemu, mogła więc rozprzestrzenić się błyskawicznie.

Niezależnie od swojej wielkości Twoja placówka może stać się ofiarą cyberprzestępców – co więcej, wystarczy jeden nieostrożny pacjent, lekkomyślny dostawca, zmęczony pracownik rejestracji lub przerwa w działaniu internetu, przez którą Twój system antywirusowy nie zdąży się zaktualizować.

Jednak teraz, kiedy już wiesz, na czym polegają największe zagrożenia dla sieci komputerowej Twojej placówki, możesz im zapobiec!

SKONTAKTUJ SIĘ Z NAMI, A PRZEPROWADZIMY AUDYT TWOJEJ SIECI I JEJ ZABEZPIECZEŃ I POMOŻEMY CI UCHRONIĆ SIĘ PRZED KAŻDYM WIRTUALNYM WIRUSEM.

ROMNY
CYBERBEZPIECZNI

KATARZYNA REJENT
tel. 882 021 185
katarzyna.rejent@romny.pl

PAWEŁ ZADRĄG
882 021 187
pawel.zadrag@romny.pl

cyberbezpieczni.com