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 1
WYCIEK DANYCH

Wyciek danych to niezmiernie groźna infekcja; jak pokazaliśmy we wstępie, może ona zakończyć się wizerunkową i finansową klęską placówki.

JAKIE PODMIOTY SĄ WIĘC NAJBARDZIEJ ZAGROŻONE TĄ CHOROBĄ?

Takie, które:

- nie przestrzegają zasad cyberbezpieczeństwa
- nie posiadają formalnych procedur postępowania z oprogramowaniem i danymi
- nie skanują regularnie systemów w poszukiwaniu podatności na zakażenie
- nie prowadzą szkoleń personelu, pozwalających wyłapać wczesne oznaki infekcji systemu
- nie testują kompetencji pracowników w zakresie reakcji na cyberatak
- nie posiadają wewnętrznych procedur logowania do systemu (także określonych odpowiednich poziomów dostępności do danych dla personelu)

Jeśli spełniasz chociaż jeden z powyższych warunków, jesteś w grupie podwyższonego ryzyka.

DZIAŁANIA PROFILAKTYCZNE POLEGAJĄ NA:

- regularnych audytach bezpieczeństwa systemów i sieci informatycznych
- analizie logowań do systemu pod kątem potencjalnych prób ataku lub anomalii systemowych
- regularnych testach bezpieczeństwa systemów ochrony przed złośliwym oprogramowaniem
- testach socjotechnicznych pracowników (testowanie pracowników pod kątem pracy z danymi wrażliwymi)
- audycie dokumentacji
- szkoleniach pracowników

Atak na szpital w Kole to największy ujawniony incydent wycieku danych w polskiej ochronie zdrowia. W jego trakcie wyciekły m.in. dane wrażliwe aż 50 tysięcy pacjentów, 600 pracowników szpitala, kopie serwerów placówki, backupy komputerów pracowników i dokumenty księgowe szpitala.

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