Cyfrowy bunkier – odpowiedź na zagrożenia XXI wieku

Cyfryzacja zmienia gospodarkę. Cyfrowa rewolucja sprawia, że firmy mogą funkcjonować efektywniej, reagować szybciej, lepiej kontrolować wszystkie procesy i skuteczniej korzystać z potencjału swoich pracowników. Kontrolowane cyfrowo łańcuchy dostaw pozwalają unikać przestojów i minimalizować stany magazynowe, a produkcja sterowana za pomocą technologii informatycznych jest wydajniejsza i umożliwia osiągnięcie najwyższej jakości. W tym raju czai się jednak niebezpieczeństwo.

Cyberprzestępczość towarzyszy rozwojowi technologii informatycznych jak cień, a jego oblicze zmienia się równie szybko, jak same technologie. Tak jak piractwo morskie narodziło się, kiedy na statkach zaczęły być przewożone cenne towary, tak samo ataki na komputery i sieci komputerowe, najpierw mające na celu wyłącznie wykazanie programistycznych zdolności hakerów, ewentualnie czystą, bezprzedmiotową destrukcję, powoli przerodziły się w konkretny, dochodowy biznes. Dziś cyberprzestępcy to już nie cyfrowi anarchiści czy spragnieni sławy młodociani programiści, ale starannie ukrywający swoją tożsamość zawodowcy,

DELL Technologies

Amica for living

którzy mają jeden, bardzo konkretny cel: zarobić pieniądze. Jednym z najskuteczniejszych narzędzi, jakie do tego stosują jest ransomware.

Ransomware: co to jest i jak działa?

Ransomware to w wolnym tłumaczeniu „oprogramowanie biorące okup", a jego koncepcja jest bardzo prosta: z jego pomocą cyberprzestępcy biorą na zakładnika całą firmę i jeśli nie dostaną kwoty, której żądają, mogą zupełnie nic nie robiąc spowodować w niej ogromne straty, a w najgorszym przypadku nawet doprowadzić do jej upadku. Jak to możliwe?

W przypadku, gdy zainfekowana wiadomość szyfrująca dane zostanie otworzona przez pracownika firmy lub nastąpiło to w inny sposób, całe przedsiębiorstwo jest sparaliżowane - stoi produkcja, logistyka, księgowość. Każda godzina przestoju to konkretne, wymierne straty, których skala lawinowo rośnie wraz upływem czasu. Samodzielne odszyfrowanie danych niestety nie wchodzi w grę, powszechnie dostępne asymetryczne algorytmy szyfrujące są zbyt mocne, żeby można je było złamać w rozsądnym czasie. Z kolei nawet gdyby zdecydować się na zakup nowych komputerów i serwerów, to firma bez swoich danych i archiwów nie będzie w stanie funkcjonować. Pozostaje więc zapłacenie przestępcom i wiara w ich „uczciwość" - doprawdy przerażająca myśl.

Wyzwania

ryzyko cyberataku
z użyciem ransomware

wielkość firmy, która jest
jednym z czynników
zwiększających ryzyko ataku

To może spotkać każdego

Niestety takie wydarzenia mają miejsce bardzo często, a ofiarą ransomware padają zarówno niewielkie firmy, jak i jednostki samorządowe, instytucje finansowe, a także wielkie, światowe korporacje.

27 czerwca 2016 roku oprogramowanie ransomware znane jako „Petya" zablokowało wszystkie komputery z Windows w firmie będącej globalnym potentatem farmaceutycznym. Zainfekowane zostały maszyny we wszystkich oddziałach firmy. Zatrzymała się produkcja w 17 fabrykach, stanęły windy w biurach, przestały działać telefony i systemy bezpieczeństwa a nawet skomputeryzowane ekspresy do kawy. Firma znalazła się na skraju katastrofy, tracąc miliony euro.

Rok później, wiosną 2017 roku ofiarą oprogramowania szyfrującego padła jedna z największych na świecie firm zajmujących się transportem morskim. W ciągu zaledwie jednego dnia infekcja rozprzestrzeniła się na wszystkie filie duńskiego giganta, unieruchamiając obsługiwane przez firmę terminale przeładunkowe i centra logistyczne i zmuszając pozbawionych łączności pracowników do komunikacji za pomocą prywatnych telefonów komórkowych.

W obu przypadkach bezpośrednie straty sięgnęły setek milionów dolarów, a straty wizerunkowe i długoterminowe, choć trudno do dokładnego wycenienia, były kolosalne. Czy można zrobić coś, żeby uniknąć ataku ransomware?

Krótka odpowiedź brzmi: nie. Żaden system nie jest idealnie szczelny, żadne zabezpieczenia - doskonałe. Wszystko, czego potrzeba to jeden błąd jednego z setek pracowników, albo jedna niezałatana w porę dziura w którymś z dziesiątek programów działających na którymś z tysięcy komputerów. Można - i należy - podjąć wysiłki zmierzające do zminimalizowania ryzyka udanego ataku, ale nigdy nie uda się osiągnąć całkowitej odporności. Trzeba zabezpieczyć się w inny sposób.

Zdając sobie sprawę z zagrożenia, działamy proaktywnie - mówi **Jerzy Zieliński, Dyrektor IT w Grupie Amica SA** - *prowadząc dziesiątki działań służących minimalizacji zagrożenia, jakie stwarza ransomware. Intensywnie szkolimy i edukujemy pracowników w tym, jak rozpoznawać najczęstsze wektory ataku, jakim są maile phishingowe, także prowadząc wewnętrzne testy, mające sprawdzić ich reakcję. Mamy też kopie zapasowe krytycznej infrastruktury i danych. Ale ryzyko wciąż istnieje.*

Bunkier, most zwodzony i zaklęcie zamieniające dane w kamień - dzięki nim dane są bezpieczne

Grupa Amica to wiodący europejski producent sprzętu gospodarstwa domowego z ponad 70-letnim doświadczeniem. W ofercie posiada

pełną gamę inteligentnych urządzeń dużego i małego AGD, wyróżniających się użytecznymi rozwiązaniami, najnowszą technologią i nowoczesnym designem. W portfelu grupy znajdują się marki: Amica (Europa Środkowa i Zachodnia), Hansa (Europa Wschodnia), Gram (Skandynawia), CDA (Wielka Brytania) oraz Fagor (Hiszpania). Amica dostarcza sprzęt AGD do klientów na blisko 70 rynkach sprzedając ponad 5 milionów urządzeń rocznie. Przy tej skali działalności i wysokim stopniu cyfryzacji prawdopodobieństwo wystąpienia zagrożenia udanym atakiem za pomocą oprogramowania ransomware stało się znaczące, a jego potencjalne skutki wpływałyby na wiele ryzyk operacyjnych. W konsekwencji nic więc dziwnego, że firma zdecydowała się podjąć kroki zmierzające do obniżenia prawdopodobieństwa wystąpienia zagrożenia *ransomware*. Inicjatywa cyfrowy bunkier znalazła się w *Programie bezpieczeństwa cyfrowego* i została zaakceptowana do realizacji w ramach planu rozwoju.

Zarządzanie ryzykiem jest częścią systemu zarządzania Grupą Kapitałową Amica i stanowi podstawę trwałej ochrony i budowy jej wartości. Dotyczy zarówno zagrożeń dla działalności, przynoszących wyłącznie negatywne skutki i potencjalny spadek jej wartości, jak i ryzyk związanych z szansami rozwoju. Zarządzanie ryzykiem odbywa się na każdym poziomie zarządzania organizacją, ze szczególnym uwzględnieniem poziomu strategicznego. Ryzyko zagrożeń cybernetycznych w ramach naszej polityki zostało zakwalifikowane jako ryzyko strategiczne. W ramach wewnętrzych procesów zarządzania ryzykiem zidentyfikowano ponad 100 ryzyk operacyjnych, czyli sytuacji, w których firma może ponieść jakiegoś rodzaju szkody - tłumaczy **Jerzy Zieliński z Amica SA.** *Zagrożenie cybernetyczne jakim jest ransomware to zagorożenie, które bardzo mocno zwiększa prawdopodobieństwo wystąpienia dużej części z tych ryzyk, dlatego z punktu widzenia biznesowego skuteczne zabezpieczenie się przed takimi atakami jest bardzo istotne.*

Wdrożenie całej architektury rozwiązania realizowane było przez wewnętrzne służby z różnych obszarów począwszy od sekcji odpowiedzialnej m.in. za zarządzanie systemami kopii bezpieczeństwa – czyli sekcji infrastruktry krytycznej IT, po sekcje systemów IT, jak również sekcję bezpieczeństwa IT. Całość projektu realizowana była we współpracy z wykwalifikowanymi inżynierami Dell Technologies. Należy zwrócić uwagę, że projekt to duża rozbudowa aktualnego środowiska kopii bezpieczeństwa o kolejny obszar. Wykorzystując swoje doświadczenie, eksperci dostawcy zaproponowali najskuteczniejsze istniejące rozwiązanie, określane jako cyfrowy bunkier.

Koncepcja cyfrowego bunkra bazuje na założeniu, że jedynym sposobem, na jaki firma może być odporna na niszczycielski atak typu ransomware, jest umożliwienie jej szybkiego i pełnego przywrócenia pełnej sprawności, jeśli takie wydarzenie kiedyś nastąpi. Oznacza to, że firma musi dysponować niezainfekowaną kopią wszystkich krytycznych danych - kopią, która będzie jednocześnie skutecznie zabezpieczona i jak najbardziej aktualna.

Cyfrowy bunkier to wspólne określenie na rozwiązanie, które obejmuje infrastrukturę, cały zestaw sprzętu, oprogramowania i pewien niezwykle istotny dodatkowy składnik, o którym będzie mowa później. Zaczynając od samych podstaw, lokalizacja cyfrowego bunkra powinna być znana możliwie wąskiemu gronu pracowników, a fizyczna lokalizacja serwerów, które będą zawierały kopię zapasową danych firmy musi być odpowiednio zabezpieczona przed niepowołanym dostępem.

Dobrą praktyką jest, żeby znajdowała się ona w innym miejscu, niż serwery produkcyjne. Chociaż w trzeciej dekadzie XXI stulecia znacznie większym niż katastrofy naturalne lub wywołane przez człowieka zagrożeniem dla danych są niezależne od lokalizacji ataki wirtualne, to jeśli atakujący będą wiedzieli, że firma jest zabezpieczona za pomocą cyfrowego bunkra, mogą podjąć próbę zniszczenia znajdującej się tam kopii zapasowej.

Jak jednak sprawić, żeby dane znajdujące się w bunkrze nie zostały zainfekowane? Twórcy

Rozwiązanie

Cyfrowy bunkier
oparty na systemach
Dell Data Domain

cyfrowego bunkra wyciągają wnioski z tego, co spotkało firmę Maersk i dlatego znajdujące się w nim dane są fizycznie odseparowane od jakichkolwiek innych komputerów czy sieci. To tak zwany „air gap", czyli przerwa między siecią firmową i internetem a serwerami kopii zapasowej.

Ta niezwykle skuteczna technika ma jednak pewną dość oczywistą wadę. Kopie zapasowe muszą być aktualizowane, najlepiej możliwie często - im częściej ma to miejsce, tym mniej straci firma w przypadku ataku. Jak przesyłać zmienione dane do bunkra, który jest odgrodzony od sieci firmowej „dziurą powietrzną"? Tu pojawia się coś w rodzaju zwodzonego mostu stosowanego w średniowiecznych zamkach. Podczas aktualizowania danych kopii most jest opuszczony, pozwalając danym przepływać, ale kiedy tylko przesyłanie się zakończy, natychmiast się podnosi, odcinając zamek od otoczenia. To jednak nie wszystko. Ponieważ wraz z nowymi aktualizacjami do bunkra mógłby trafić także i malware, wszystkie dane są zapisywane w trybie wyłącznie do odczytu - w razie, gdyby atak doszedł aż tu nie mogą więc zostać nadpisane i zaszyfrowane.

Ale żeby cyfrowy bunkier spełniał swoje zadanie, czyli umożliwiał firmie powrót do sprawnego funkcjonowania w każdej sytuacji utraty danych, potrzebne jest coś jeszcze.

Efekty

firma gotowa na ryzyko potencjalnego ataku

brak przestojów w przypadku cyberataku

Backup jest nie po to, żeby go robić, tylko żeby go przywracać

W jednym z centrów danych Amica SA powstał cyfrowy bunkier, składający się z systemów Dell Data Domain, replikujących dane z produkcyjnych urządzeń, oddzielony od całej reszty sieci ochronną przerwą air gap i skonfigurowany w taki sposób, żeby zapisane w bunkrze dane były zablokowane, bez możliwości ich usunięcia czy zmiany. Jednak wykonywanie i posiadanie zabezpieczonej w cyfrowym bunkrze kopii zapasowej nie jest celem samo w sobie. Chodzi przecież o to, żeby za pomocą tych danych móc zminimalizować skutki, jakie dla firmy może mieć atak ransomware - potrzebne jest więc sprawne i skuteczne reagowanie na takie wydarzenie.

Oprócz całej infrastruktury, sprzętu i oprogramowania, zapewniamy naszym partnerom niezbędne procedury, pozwalające na odtworzenie danych - opisuje kluczowy składnik cyfrowego bunkra **Paweł Chruściak, Data Protection Solutions Sales Representative z Dell Technologies** - *To zestawy jasnych instrukcji, które pozwalają pracownikom natychmiast podejmować właściwe działania, prowadząc ich krok po kroku przez kolejne etapy przywracania danych. To dzięki nim cyfrowy bunkier działa tak, jak powinien.*

Ważnym elementem jest też stała kontrola i testowanie tworzonych kopii. W tym celu w skład odizolowanego środowiska cyfrowego bunkra wchodzi także serwer pozwalający na odtwarzanie przechowywanych backupów - oczywiście znacznie mniej wydajny, niż maszyny produkcyjne, ale wystarczający do tego, żeby można było przećwiczyć wszystkie czynności a także skontrolować stan kopii.

Celem backupu nie jest jego wykonywanie, tylko skuteczne odtworzenie, dlatego nie poprzestajemy na składowaniu danych w bunkrze. Traktujemy je jako narzędzie, które pozwoli w razie zagrożenia przywrócić firmie pełną sprawność i szykujemy się na taką ewentualność - aby gdyby coś się zdarzyło, zadziałać szybko i skutecznie - mówi **Jerzy Zieliński z Amica SA.**

Jerzy Zieliński,
Dyrektor IT,
Grupa Kapitałowa Amica

Paweł Chruściak
Data Protection Sales Manager
Dell Technologies

pawel.chrusciak@dell.com