Ransomware – jakie informacje CISO (Chief Information Security Officer) powinien przekazać prezesowi, zarządowi.

Spis treści

Wstęp

Działalność każdej organizacji związana jest z szacowaniem, monitorowaniem i zarządzaniem, w tym zarządzaniem cyber-ryzykiem. W momencie, kiedy identyfikujemy ryzyko i wiemy jaki czynnik je wywołuje, możemy podjąć odpowiednie kroki w celu ochrony organizacji. Kluczowa w tym wszystkim jest wiedza na temat tego co nam zagraża i jakie mogą być tego skutki, jeżeli odpowiednio nie zareagujemy. Co powinniśmy wiedzieć o atakach tzw. „ransomware"? Co powinni wiedzieć członkowie zarządu, CEO, Prezes? Aby wiedzieć co zrobić i jak zarządzać organizacją w obliczu cyberzagrożeń należy poznać „przeciwnika".

Ransomware

To jedno z najbardziej „popularnych" obecnie zagrożeń dla systemów informacyjnych. „Ransomware" to oprogramowanie szkodliwe, najczęściej występujące wspólnie z innymi programami w postaci „konia trojańskiego" lub RAT (Remote Access Trojan), którego głównym celem jest:
- zainfekowanie stacji roboczej, systemu IT, całej sieci IT;
- zablokowanie dostępu do danych, informacji, urządzeń z użyciem algorytmów szyfrujących tzw. szyfrowania;
- „wymuszenie" okupu za odblokowanie dostępu. (odzyskanie kontroli lub uzyskanie informacji zdarza się bardzo rzadko, jak wynika z analizy statystyk około 70 % zaszyfrowanych informacji nigdy nie jest odzyskiwana")1.

- **Od czego to się zaczęło**
  Obecne bardzo złożone i zaawansowane w swoim działaniu oprogramowanie „ransomware", ma swoje początki pod koniec lat 80 ubiegłego wieku. Oprogramowanie było rozsyłane na dyskietkach do uczestników konferencji WHO na temat zagrożeń wirusem HIV i AIDS, blokowało dostęp do komputera i plików a okup należało wpłacić na konto w banku.

- **Rozwój na przestrzeni ostatnich lat**
  Rozwój Internetu oraz dostęp do tego medium całkowicie zmienił oprogramowanie, sposób działania cyberprzestępców oraz skalę działania. Początkowe ataki były oparte na oprogramowaniu typu „Locker" – blokujących dostęp do systemu z wyświetleniem ekranu informującego o przejęciu komputera np. przez policję i żądaniem opłaty za odstąpienie od działań prawnych. „Cryptoloker" – szyfrujący wybrane pliki uniemożliwiając dostęp do zawartych w nich danych oraz żądanie okupu. Opłaty były mało wygórowane rządu 50$ do 150$, płatność mogła być dokonana w różnych systemach np. „premium sms" i kodach np. „Ukash" anonimizujących – bezpiecznych dla atakującego.

- **Jak dzisiaj działa typowa korporacja „Ransomware"**
  Sytuacja całkowicie uległa zmianie, w momencie, kiedy cyberprzestępcy zauważali jak niewiele firm czy też osób prywatnych dba o swoje bezpieczeństwo – nie robiąc kopii swoich informacji. Dawało to przewagę i pewność, że osoba zaatakowana zapłaci okup. Dodatkowo pojawia się Bitcoin – kryptowaluta, dająca praktycznie pełną anonimowość w obrocie i wymianie a przez to bardzo szybko stała się „walutą cyberprzestępców". Początkowe skuteczne ataki na osoby prywatne, przenoszą się coraz bardziej na firmy, co skutkuje dynamicznym rozwojem ataków z wykorzystaniem „ransomware". Cyberprzestępcy z okupu inwestowali w rozwój swoich działań – system korporacyjny stał się powszechnie wykorzystywanym w tej działalności przestępczej. W latach 2000 popularne stają się systemy RaaS (Rasnomware as a Service) oferujące w sieci

1 https://pl.malwarebytes.com/ransomware/ - dostęp: 14.06.2023 r.

„DarkNet" dostęp do gotowych programów „ransomware", udzielających wsparcia i informacji na temat tego jak atakować i wymuszać okup. „Zyski" z takiej działalności były podzielone pomiędzy dwie strony.2 Przełomem w działalności cyberprzestępców były ataki z użyciem „ransomware" o nazwie kodowej – „Notpetya" i „Wannacry"3. Infekcje tymi programami objęły setki tysięcy komputerów i systemów w wielu krajach na całym świecie. Szkody wywołane atakiem oraz nakłady związane z przywróceniem działalności organizacji liczone są w miliardach dolarów. World Economic Forum klasyfikuje „ransomware" jako poważny problem na skalę światową. Obecnie systemy ataków z wykorzystaniem „ransomware" są bardzo złożone. Atakujący wykorzystują różne techniki w tym socjotechnikę, podatności „O-day" oraz nieuczciwych pracowników, którzy np. po opuszczeniu organizacji przekazują swoje dane dostępowe do systemów byłego pracodawcy.
W obecnym ataku możemy wyróżnić 4 fazy4:

1. atak i zablokowanie, szyfrowanie dostępu do komputerów, sieci firmy z żądaniem okupu,
2. dodatkowe żądanie okupu z groźbą nieodwracalnego zniszczenia danych i informacji (obecnie około 70% firm nigdy nie odzyska swoich danych),
3. wymuszenie płatności pod „groźbą" upublicznienia informacji firmowych w tym np. tajemnic handlowych lub „szantaż" sprzedaży informacji pochodzących z organizacji,
4. dodatkowy atak DDoS (Distributed Denial of Service - atak odmowy), na serwisy internetowe organizacji, mające wpłynąć na szybkość wnoszonej płatności.

Celem atakującego jest w większości przypadku wymuszenie okupu i osiągniecie zysku. Zysk, który pozwala na rozwój ataków „ransomware". Dlatego podstawowym zaleceniem dla „ofiary" ataku jest – nie płacić okupu. Znane są przypadki, gdzie atakujący powrócił do organizacji, która zapłaciła okup, gdyż wiedział jakie ma słabości w „systemie obrony" i wiedział, że ponownie firma zapłaci za odzyskanie danych. W przypadku ataku, lepiej zwrócić się do specjalistycznych firm o pomoc.

Czy można się przed tym „obronić"?

- Codzienna „cyberkultura".
Nie zapominaj kto jest najważniejszy w twojej organizacji i kto może Ci pomóc w uniknięciu poważnych problemów związanych z „ransomware". Twoja „pierwsza linia obrony" to pracownicy. Jeżeli właściwie zdefiniujesz, przekażesz zasady postępowania z systemami, sprzętem i oprogramowaniem oraz ich użyciem unikniesz poważnych kłopotów. Mało tego, jeżeli pracownicy będą mieli pełną świadomość zagrożeń i będą znali system oraz procedury powiadamiania o zagrożeniach, bardzo szybko dowiesz się, kiedy nadciąga kryzys. Pamiętaj przy tym, aby ustanowić system nagród za pozytywne podejście i informowanie o zidentyfikowanych sytuacjach zagrożeń. Unikaj kar i wyciągania negatywnych konsekwencji tak długo jak to możliwe.

- Szkolenie, uczenie się na systemach symulujących.
Nic tak pozytywnie nie wpływa na właściwe reakcje pracowników, użytkowników jak wiedza co oraz jak mają zrobić. Dotyczy to również zachowania w sytuacji zagrożeń pochodzących z cyberprzestrzeni, sieci Internet. „Ransomware" nie jest tutaj wyjątkiem. Uczmy i weryfikujmy wiedzę oraz zachowania

2 https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/ - dostęp: 14.06.2023 r.
3 https://www.phishlabs.com/blog/wannacry-notpetya-ransomware-evolved-in-2017/ - dostęp: 10.06.2023 r.
4 https://unit42.paloaltonetworks.com/multi-extortion-rise-ransomware-report/ - dostęp: 10.06.2023 r.

naszych użytkowników. Wiemy doskonale, że jednym z wektorów, sposobów ataku naszej organizacji może być socjotechnika - wywieranie wpływu na osobę. Dodając do tego „główne medium" ataku, czyli pocztę elektroniczną, e-mail to tzw. atak „phishingowy" czy też „spear- phishingowy", wiemy już od czego zacząć naszą akcję uczenia rozpoznawania i identyfikowania ataków. Wprowadzajmy regularne testy (np. raz na kwartał) tzw. „testy phishingowe" w celu uczenia i doskonalenia reakcji pracowników. Lepiej szkolić niż płacić okup.

- Przygotowanie planów: utrzymania ciągłości działania (BCP) i przywracania po incydencie (DRP), budowa odporności organizacji

Przygotowanie pracowników, czyli „pierwszej" linii obrony to warunek podstawowy do osiągnięcia odporności organizacji. Kolejny etap, bez którego trudno funkcjonować to plany ciągłości działalności, procesów kluczowych i odtwarzanie po incydencie. Nawet najlepiej zorganizowana organizacja nie osiągnie 100 % poziomu bezpieczeństwa. Atakujący, jeżeli będzie „zmotywowany" znajdzie sposób, system, współpracującą z nami organizację (z tzw. „łańcucha dostaw") na przeniknięcie do wnętrza firmy i przeprowadzi ostateczny atak. Wtedy musimy uruchomić procedury związane z zachowaniem ciągłości działania systemów informacyjnych i biznesowych a także odtwarzać organizację po cyberataku. Mając już te elementy możemy planować, budować program cyberbezpieczeństwa dla całej organizacji, którego celem jest reagowanie na zmiany zachodzące w organizacji oraz w cyberprzestrzeni.

„Huston", mamy problem – czyli co zrobić w przypadku ataku

- Działania SOC, CSIRT/CERT.

Jak w każdej działalności, świetnie zorganizowanej i przygotowanej na większość scenariuszy negatywnych, może nam się zdarzyć i zmierzyć z cyberatakiem typu „ransomware". Ważne w tym momencie jest szybkie przekazanie informacji pozwalającej na identyfikację zdarzenia i podjęcie właściwych działań zgodnie z procedurami, „playbookami", „runbookami". Komunikacja jest tutaj kluczowa. SOC (Security Operations Center) jest odpowiedzialny za monitorowanie i detekcję niechcianych zdarzeń w tym przeciwdziałania wystąpienia incydentom. W większości znanych przypadków ataków z wykorzystaniem znanych programów szkodliwych w tym „ransomware", SOC jest w stanie odpowiednio wcześniej zareagować i zablokować niechciane działania. Zdarzają się jednak przypadki wykorzystania podatności w tym „0-day", które są trudne do wykrycia i zidentyfikowania, pozwalają atakującemu na infiltrację naszej organizacji i przejęcie kontroli nad systemem (-ami). Wtedy mamy problem, który należy zaadresować do kolejnej grupy ekspertów – CSIRT/CERT (Computer Security Information Response Team / Computer Emergency Response Team). Zespoły te zajmują się bardziej złożonymi kwestiami (inżynieria wsteczna, informatyka śledczą, Cybert Threat Hunting, Cyber Threat Intelligence) i incydentami, wymagającymi nie tylko pracy w ramach organizacji, ale czasami podejmują współpracę z innymi zespołami CSIRT/CERT lub centrami cyberbezpieczeństwa i wymiany informacji - ISAC.

- Przekaż komunikat wewnątrz organizacji.

Jeżeli wiesz, że dzieje się źle i jest to atak z użyciem „ransomware" przekaż tak szybko jak to możliwe komunikat wewnętrzny do wszystkich pracowników opisując symptomy ataku, czego nie robić a o czym należy szybko poinformować zespół SOC/CERT.

- Przygotuj komunikat na zewnątrz do swoich biznes-partnerów, klientów.

Jeżeli masz informacje dot. skali ataku, zakresu, wiesz, że mogło dojść do przejęcia lub próby przejęcia kontroli nad systemami firm z którymi współpracujesz, podejmij natychmiastowe działania związane z przekazaniem informacji o tym co się dzieje. Pełna współpraca i wymiana informacji są tutaj podstawą działania.

- Przygotuj komunikat dla mediów, raport dla CERT poziomu krajowego (o ile jest taki wymóg lub chcesz podzielić się wiedzą i doświadczeniami ze swojego przypadku)
Jeżeli twoja organizacja jest Operatorem Usługi Kluczowej tzw. OUK (uznanym przez organ właściwy w ramach obowiązującej ustawy o Krajowym Systemie Cyberbezpieczeństwa) w pewnych zdefiniowanych przez ustawę przypadkach, wystąpienia incydentu tzw. poważnego w tym z użyciem „ransomware" musisz powiadomić w ciągu 24 godzin właściwy CERT poziomu krajowego (jeden z następujących: CSIRT NASK, CSIRT MON, CSIRT GOV). Jeżeli twoja firma nie jest OUK, ale świadczysz usługi dla firm, osób fizycznych i twój komunikat pozytywnie może wpłynąć na bezpieczeństwo tych z którymi współpracujesz, chcesz być transparenty w obszarze zachowania wspólnych standardów bezpieczeństwa („*cyberbezpieczeństwo to nasza wspólna sprawa*") przekaż informację do zainteresowanych, opublikuj na własnych stronach internetowych informację, przekaż komunikat za pośrednictwem mediów społecznościowych. Dzięki takiemu postępowaniu uda Ci się uchronić innych przed atakiem „ransomware".

Płacić czy nie płacić okupu?

W momencie, kiedy widzimy na ekranie swojego „zablokowanego" komputera ekran z żądaniem okupu, za odblokowanie dostępu do danych i informacji, nie ma wątpliwości, że staliśmy się celem ataku. W takich przypadkach zawsze zadajemy sobie pytanie i co teraz? Firmy, organizacje, które oceniły ryzyko zagrożenia atakiem z wykorzystaniem ransomware i podjęcia odpowiednie kroki prewencyjne może przystąpić do działań odtworzeniowych z jednoczesnym utrzymaniem kluczowych procesów. BCP i DRP. W obszarze cyberbezpieczeństwa przeprowadzenie pełnej analiz przypadku wraz z wnioskami i rekomendacjami na przyszłość dla organizacji jest kluczowa. Uczmy się na incydentach, aby nie wydarzyły się kolejny raz w przyszłości. Ale co w przypadku, kiedy nie mamy planów działania w sytuacjach kryzysowych, nie mamy, jak odtworzyć nawet podstawowych informacji niezbędnych do funkcjonowania organizacji? Powstaje pytanie, płacić czy nie płacić okupu? Organa ścigania, służby federalne m.in. w USA jasno wskazują na fakt, iż płacenie okupu jest swoistego rodzaju sponsorowaniem działalności przestępczej i nie należy płacić okupu5.

Czy zarząd i CEO może być wsparciem w zapobieganiu atakom „Ransomware"?

Odpowiedź wydaje się oczywista – TAK. Dla dojrzałych organizacji, posiadających właściwie zaprojektowany i zarządzany program cyberbezpieczeństwa, polityki cyberbezpieczeństwa, plany ciągłości działania jest to element niezbędny do właściwego funkcjonowania. Wszyscy, bez wyjątku, w organizacji odpowiadamy za cyberbezpieczeństwo. Szczególna role ma tutaj zarząd i prezes, dyrektor generalny, który powinien być przykładem właściwego sposobu traktowania cyberbezpieczeństwa i nadawania tonu całej organizacji. Nie powinniśmy więc usłyszeć od zarządu stwierdzenia: ja tego nie potrzebuję, muszę mieć dostęp do wszystkiego, muszę mieć dostęp do poczty prywatnej, program AV – tylko mi przeszkadza i spowalnia komputer. Właściwe komunikowanie zagrożeń i ryzyk dla biznesu to główne zadanie zarządzających na każdym poziomie. Doceniać należy pozytywne reakcje pracowników, stwarzać warunki do pozyskiwania wiedzy i umiejętności pozwalających na ochronę organizacji przed cyberatakami w tym tymi „najskuteczniejszymi" – socjotechnicznym.

5 https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware - dostęp: 14.06.2023 r.

Rola i zadania CEO i zarządu w przypadku ataku

Zarząd, zarządzający oraz kierownictwo każdego szczebla w organizacji ma szczególna rolę w przypadku wystąpienia incydentu, ataku z wykorzystaniem „ransomware". Oprócz pełnej współpracy z zespołami reagowania SOC/CERT/CSIRT i realizacji ich poleceń, należy uruchomić w obszarach dotkniętych atakiem procedury BCP i DRP, o których wspominaliśmy. Komunikacja z pracownikami jest również elementem reagowania w sytuacji kryzysowej, w tym informowania co się stało i jak musimy sobie poradzić w trudnym okresie. Jakie realizować zadania, co robić i z kim się komunikować. Rola zarządu w takich sytuacjach jest znacząca w kwestiach wsparcia zespołów reagowania, informowania pracowników o podjętych działaniach oraz komunikowania na zewnątrz co się dzieje i jakie są podejmowane kolejne kroki. Kluczową rolą jest kierowanie organizacją w tak trudnym czasie. Kluczowe jest tutaj podjęcie decyzji, na bazie analizy sytuacji, o kwestii – płacić nie płacić. Bardzo ważne jest przygotowanie, nie tylko organizacji na takie sytuacje i scenariusze, ale zarządów. Jakie kroki należy podjąć w jakim czasie, jak przygotować procedury i jak je uruchamiać. Kto i za co odpowiedź oraz jakie ma uprawnienia. Ćwiczenie takich zachowań i reakcji, testowanie ich w symulowanych warunkach może dostarczyć bardzo cennych doświadczeń i wiedzy na temat funkcjonowania organizacji i zarządu. Rekomendujemy „obligatoryjne" szkolenie z udziałem zarządu przynajmniej raz w roku.

Gdzie szukać pomocy w sytuacjach kryzysowych?

Jeżeli zostałeś zaatakowany, wydaje ci się, że sytuacja wymknęła się spod kontroli. Nie masz już żadnego wyjścia? Sytuacja jest poważna, ale nie beznadziejna. Zawsze możesz sprawdzić, czy otrzymasz wsparcie od jednego z trzech CSIRT'ów poziomu krajowego (OUK – na pewno taką pomoc otrzyma i powinien o nią wnioskować). Zapytaj wśród firm z którymi współpracujesz czy nie spotkali się z podobnym przypadkiem. Sprawdź portale techniczne czy nie ma tam informacji o rodzaju „ransomware" jaki spowodował problem w twojej organizacji. Sprawdź strony internetowe organizacji zajmujących się bezpieczeństwem, cyberbezpieczeństwem czy nie oferują pomocy i rozwiązania przypadku takiego jak twój. Jeżeli wiesz jakie oprogramowanie zostało wykorzystane do ataku na twoja firmę poszukaj „dekryptora", aplikacji pozwalającej na odszyfrowanie twoich zasobów. Informacji możesz szukać m.in. na stronie Europolu – European Cybercrime Center – EC3, gdzie znajdziesz informacje i projekt „NoMoreRansom"6. Na stronach tego projektu (dostępnego również w języku polskim) znajdziesz "dekryptory" do wielu programów szkodliwych „ransomware". Znajdują się tam również informacje o prowadzonych aktualnie pracach nad "dekryptorami" do innych programów szyfrujących, więc być może warto, żeby się zastanowić ponownie nad pytaniem „płacić czy nie płacić"(?).

Podsumowanie

Cyberataki z wykorzystaniem oprogramowania „ransomware" będą utrzymywali się w obecnym wzrostowym trendzie. Główny cel atakującego, zysk, jest głównym motorem działalności przestępczej. Możemy być świadkami nowych technik, wektorów ataku, wykorzystania systemów tzw. uczących się czy też „sztucznej inteligencji" - „AI&ML" do wsparcia kampanii „ransomware". Mogą sprawdzić się przepowiednie firm zajmujących się cyberbezpieczeństwem o zmasowanych atakach na „łańcuch dostaw', słabiej zabezpieczone firmy i atakowanie z ich infrastruktury tych większych firm, które są właściwym celem. Zwiększyć się może zainteresowanie atakujących obszarem produkcyjnym, gdzie

6 https://www.nomoreransom.org/pl/index.html - dostęp: 14.06.2023 r.

zatrzymanie procesów technologicznych może być krytyczne dla organizacji z zakończeniem działalności biznesowej włącznie.

Pamiętajmy w takiej sytuacji o tym, żeby właściwie się przygotować na potencjalne zdarzenia i incydenty. Informujemy o zagrożeniach i przyjmujmy każdy komunikat o podejrzanym działaniu lub sytuacji. Reagujmy stosownie do zagrożenia. Angażujmy zarząd i kierującego organizacją dyrektora, prezesa, to nie tylko wspiera organizację to jego obowiązek prawny.

Przeciwdziałanie jest w tym zakresie zdecydowanie lepszym wyjściem niż reagowanie na incydent.