Najlepsze praktyki obsługi incydentu naruszenia cyberbezpieczeństwa związanego z atakiem ransomware w podmiocie publicznym. Poradnik

Wersja 1.0.2
Kwiecień 2021

Przedmowa

Niniejsze opracowanie oparto na następujących praktykach i standardach: Zbiór dobrych praktyk zarządzania incydentem ENISA (Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji), 10 grudnia 2020 r.; Poradnik obsługi incydentu bezpieczeństwa komputerowego SP 800-61 Rev. 2, NIST (Narodowy Instytut Standaryzacji i Technologii), sierpień 2012; RFC 2196 Site Security Handbook, IETF (Internet Engineering Task Force), wrzesień 1997; ISO/IEC 20000, ISO/IEC 27035; Poradnik obsługi incydentu ransomware, CISA (Cybersecurity and Infrastructure Security Agency), wrzesień 2020.

Zasady postępowania zawarte w powyższych dokumentach zostały uzupełnione o doświadczenia autorów, w tym o szczególny kontekst infrastruktury wybranych podmiotów publicznych i wpływ, jaki ataki ransomware mogą mieć na funkcjonowanie tych podmiotów.

Zebraliśmy nasze obserwacje w zakresie obsługi incydentów naruszenia cyberbezpieczeństwa i zabezpieczania danych po stronie instytucji dotkniętej incydentem. Publikujemy poradnik z nadzieją, że będzie wsparciem dla podmiotów publicznych w obsłudze incydentów, pozwoli na uniknięcie najczęściej popełnianych błędów oraz pomoże w przywracaniu ciągłości działania po incydencie. Podawane w tekście przykłady konkretnych skutków takiego ataku dotyczą obszaru zadań wybranych podmiotów publicznych, jednak w praktyce są one ściśle uzależnione od specyfiki działalności ofiary.

Autorzy

Ania, Jakub Dysarz, Renata Klimek, Maciej Kotowicz, Tomasz Kułakowski, Radosław Machała, Witold Sobolewski, Grzegorz Tworek.

Opracowanie językowe – Katarzyna Sajdak

Spis treści

Wstęp

Dotychczasowe obserwacje w obsłudze incydentów bezpieczeństwa w podmiotach publicznych, niezależnie od szczebla, rodzaju podmiotu oraz wpływu incydentu na funkcjonowanie podmiotu publicznego, realizowanie zadań czy życie i zdrowie ludzi, prowadzą do konstatacji, że podmioty publiczne w obsłudze incydentów potrzebują pomocy wyspecjalizowanych zespołów.

Na poziomie krajowym funkcjonuje zespół CSIRT NASK, jednak należy podkreślić, że **jego zadaniem nie jest obsługa indywidualnych incydentów** w podmiotach w jego właściwości. CSIRT NASK monitoruje zagrożenia cyberbezpieczeństwa i incydentów, wspiera wymianę informacji i reaguje na zgłoszone incydenty wspierając zaatakowane podmioty np. analizą złośliwego oprogramowania. Jednak w przypadku indywidualnych incydentów podmioty publiczne zmuszone są korzystać z pomocy podmiotów komercyjnych, bądź z własnych zasobów. **Trzeba jednak pamiętać, że niezależnie od udzielonej (lub nieudzielonej) pomocy przez podmioty zewnętrzne, ciężar odpowiedzialności za reakcję na incydent spoczywa na podmiocie publicznym i to podmiot publiczny ma obowiązek przywrócić ciągłość swojego działania tak, aby mógł realizować swoje zadania.**

Przerwanie ciągłości działania podmiotu publicznego zazwyczaj oznacza, że zadania publiczne będą realizowane o obniżonej jakości lub nastąpi całkowite ich przerwanie. Skutki incydentu mogą być bardzo poważne i obejmować negatywne konsekwencje prawne, finansowe i wizerunkowe. Zaatakowane instytucje często mierzą się z problemem terminowego realizowania zadań zleconych, takich jak np. wypłata świadczeń 500+, oraz – coraz częściej – wyciekiem danych.

Ustawa o krajowym systemie cyberbezpieczeństwa z 2018 r. nakłada na podmioty publiczne zadania z zakresu zarządzania incydentem naruszenia cyberbezpieczeństwa. Poza zgłoszeniem incydentu w ciągu 24 godzin od stwierdzenia naruszenia, podmioty publiczne mają również obowiązek obsługi incydentu we współpracy z właściwym zespołem CSIRT, którym dla większości podmiotów jest zespół CSIRT NASK (zespół CERT Polska)[1].

[1] Pozostałe zespoły CSIRT to CSIRT GOV (wspierający obsługę incydentów w centralnej administracji rządowej oraz w infrastrukturze krytycznej) i CSIRT MON (wspierający obsługę incydentów podmiotów wojskowych).

Obsługa incydentu

Zgodnie z definicją ustawową, obsługa incydentu obejmuje czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu. Poniżej przedstawione zostały najlepsze praktyki, wypracowane w trakcie reagowania na incydenty w podmiotach publicznych, związane z działaniem oprogramowania typu ransomware (szyfrującego dane i wymuszającego okup).

Wobec złożoności zagrożeń i ataków instytucja mierząca się z obsługą incydentu powinna rozważyć współpracę z innymi organizacjami. Obsługa incydentu często przekracza możliwości podmiotu publicznego, a współpracując z innymi podmiotami będzie w stanie działać w sposób niedostępny dla pojedynczej organizacji. Współpraca z podmiotami wyspecjalizowanymi – nie tylko z zespołami informatyki śledczej, ale również z integratorami i dostawcami sprzętu, oprogramowania, w tym oprogramowania dziedzinowego, pozwala zmniejszyć negatywny wpływ incydentu na funkcjonowanie podmiotu publicznego oraz skraca czas przywracania ciągłości działania zaatakowanej instytucji. Bardzo ważna, choć nieopisana w niniejszym dokumencie, jest koordynacja obsługi incydentu. Poprawna koordynacja zapewnia przede wszystkim prawidłowy obieg informacji i zmniejsza ryzyko popełnienia błędu w obsłudze incydentu oraz przy zabezpieczeniu danych. Jednym z najpoważniejszych błędów, jaki można popełnić już na początkowym etapie obsługi incydentu, jest zaangażowanie znacznej liczby osób, z których każda pracuje niezależnie, a nie współdziałają w ramach wielospecjalistycznego zespołu[2].

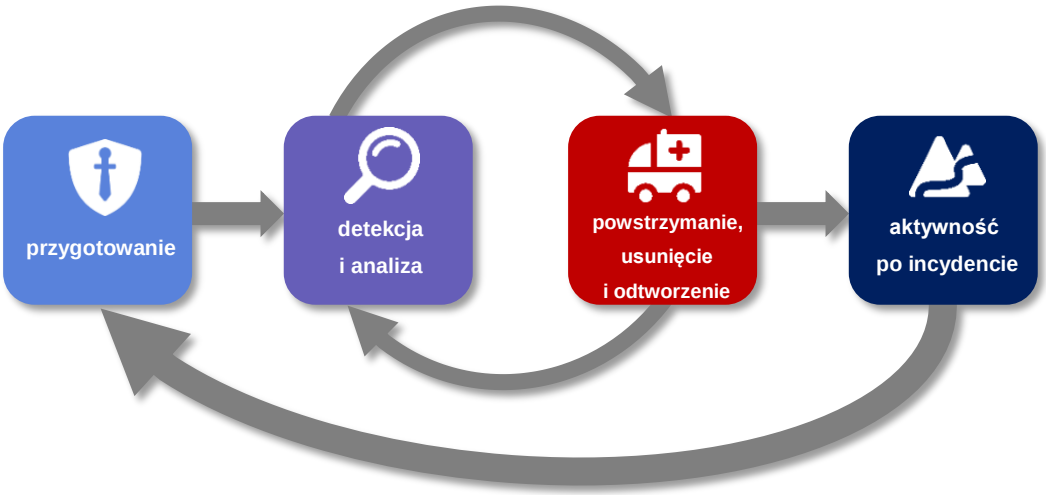
Incydenty związane z działaniem sprawców szyfrujących dane i żądających okupu są zazwyczaj bardziej rozległe i poważniejsze w skutkach, niż wynika to ze wstępnej oceny dokonywanej przez osoby odpowiedzialne za obszary technologii informacyjnej w podmiotach publicznych. Zaszyfrowanie danych jest ostatnią techniką wykorzystywaną przez sprawców, ale pierwszą, którą dostrzegają użytkownicy systemów. Nie widzą oni wielu wcześniejszych kroków, takich jak np. uzyskanie dostępu do systemów i ich eksfiltracja – wykradzenie poświadczeń, wykradzenie (wyciek) danych[3].

Zgodnie z NIST SP 800-61r2, na proces obsługi incydentu składają się cztery główne etapy:

1) przygotowanie,
2) detekcja i analiza,
3) powstrzymanie, usunięcie i odtworzenie,
4) aktywność po incydencie.

[2] W RFC 2196 Site Security Handboook, 5.2.1, ujęte jest to w następujący sposób:- `A major mistake that can be made is to have a number of people who are each working independently, but are not working together. This will only add to the confusion of the event and will probably lead to wasted or ineffective effort.`

[3] Szerzej opisane jest to w artykule *Ransomware - zapiski z placu boju*, as, ks, ms, sekurak.pl, 27 marca 2021 r.



Obraz 1. Cykl obsługi incydentu (za: NIST SP 800-61r2)

Prewencja

Warto uwzględnić działania prewencyjne związane z wdrożeniem odpowiednich środków technicznych i organizacyjnych, ograniczających ryzyko wystąpienia naruszenia. Działania te mogą obejmować między innymi szkolenie użytkowników z zakresu prawidłowego korzystania z systemów informatycznych i identyfikowania zagrożeń (np. wyłapywanie podejrzanych wiadomości), ale nie powinny się do nich ograniczać.

Istotne jest wdrożenie przede wszystkim odpowiednich środków technicznych, które w obiektywny sposób zmniejszają ryzyko wystąpienia naruszenia i nie polegają wyłącznie na ocenie ludzkiego arbitra. Środki te związane są z poprawną konfiguracją systemów informatycznych – od urządzeń na brzegu sieci, środowiska serwerowego, przez stacje robocze, do konkretnych aplikacji dziedzinowych.

W przypadku incydentów związanych z działaniem złośliwego oprogramowania typu ransomware, ważne jest też ograniczenie możliwości wykorzystania przez atakujących najbardziej popularnych błędów konfiguracyjnych i podatności systemów. W literaturze nazywa się to „minimalizacją płaszczyzny ataku". Warto rozważyć:

- ograniczenie korzystania z RDP (*usługi pulpitu zdalnego*), ponieważ RDP *wystawiony na świat* jest jednym z najczęściej wykorzystywanych przez atakujących sposobów *wejścia* do instytucji – nawet jeśli dostęp został zabezpieczony hasłem, dane do logowania były łamane przez atakujących; dotyczy to również innych nieużywanych usług czy procesów – część z nich można usunąć (np. te odpowiedzialne za serwer NTP/czasu),
- ograniczenie uprawnień użytkownika zgodnie z zasadą najniższych przywilejów, ponieważ złośliwe oprogramowanie, w tym ransomware, w przypadku uruchomienia przez użytkownika bez praw administratora, spowoduje wielokrotnie mniejsze straty niż w przypadku uruchomienia

na wysokich uprawnieniach – nawet jeżeli złośliwe oprogramowanie doprowadzi do utraty części danych, to stosowane w infrastrukturze zabezpieczenia umożliwią ich szybkie odtworzenie, a ponadto niemożliwe będzie jego rozprzestrzenienie się na inne systemy,

– segmentacja i restrykcje sieci, ponieważ często zdarza się, że w instytucjach funkcjonuje jedna płaska sieć, bez VLAN (sieci wydzielonej logicznie w ramach większej sieci fizycznej), a nawet jeśli istnieje taki podział, to brakuje uruchomienia funkcji pozwalających na ograniczanie i ewentualną analizę zdarzeń pomiędzy poszczególnymi podsieciami logicznymi. W obszarach DC warto rozważyć mikrosegmentację sieci z wykorzystaniem usług. Warto też zweryfikować strukturę aplikacji, która, by podnieść bezpieczeństwo, powinna zostać zbudowana w architekturze trójwarstwowej (prezentacja, logika biznesowa, baza danych), a pomiędzy poszczególnymi warstwami warto zastosować mechanizmy weryfikujące ruch (np. z wykorzystaniem zapór ogniowych, oprogramowania analitycznego lub sond IPS, IDS).
– ograniczenie praw dostępu do kopii zapasowych, ponieważ złośliwe oprogramowanie często automatycznie uszkadza np. VSS (ang. Volume Shadow Copy Service) i szyfruje kopie zapasowe – jeśli zostanie wykonane z poziomu użytkownika, który nie ma uprawnień do dokonywania tego typu zmian, ograniczone zostanie ryzyko uszkodzenia tych kopii. Skutecznym rozwiązaniem może być zastosowanie VTL (ang. Virtual Tape Library), które pozwoli zasymulować pracę bibliotek taśmowych, jednocześnie pozbywając się problemu w postaci długiego RTO (ang. Recovery Time Objective), czasu przywracania procesów biznesowych; zasada działania ma polegać na zapisywaniu archiwum na taśmach, którymi w rzeczywistości mogą być szybkie dyski macierzowe, a podłączenie systemu odbywa się z wykorzystaniem FC (ang. Fiber Connector) lub iSCSI, co utrudnia lub nawet uniemożliwia złośliwemu oprogramowaniu zaszyfrowanie takich zasobów.

W przypadku ograniczania skutków ataku ransomware w wyniku nieuprawnionego działania w ramach prewencji ograniczany jest również dostęp do plików i systemów, warto więc poddać rewizji procedury kopii zapasowych i regularnie testować, czy wykonane kopie pozwalają w praktyce na odtworzenie zabezpieczanych w ten sposób danych i systemów w zadowalającym czasie i w sposób, który spowoduje utratę danych nie większą niż dla danej instytucji akceptowalna (np. utrata dokumentów wprowadzonych ostatniego dnia, bo te dane można w stosunkowo krótkim czasie i niskim nakładem środków odtworzyć). **W wypadku infiltracji środowiska DC (ang. Data Center), środowiska serwerowego, należy brać pod uwagę okres, w jakim mogła ona nastąpić, a fakt, że posiadamy niezaszyfrowaną kopię środowiska wcale nie oznacza, że w tym zabezpieczonym kopią środowisku nie występuje ukryte złośliwe oprogramowanie, które może się po odtworzeniu uaktywnić.**

Pozostałe środki prewencji ransomware obejmują działania ograniczające związane z pozyskiwaniem przez atakujących nieuprawnionego dostępu do danych (wyciekami danych), uzyskiwaniem dostępów do innych systemów i sieci, zarówno poprzez wykradanie poświadczeń, jak i w wyniku braku środków

ograniczających lub ich niepoprawnej konfiguracji (np. segmentacja sieci, ale bez restrykcji, kto może się do danej sieci przyłączyć lub bez zapory ogniowej pomiędzy segmentami).

Przygotowanie do obsługi incydentu

W ramach przygotowania do obsługi incydentu instytucja powinna stworzyć i testować procedurę reagowania na naruszenia cyberbezpieczeństwa. Procedura powinna określać, jak należy postępować w przypadku naruszenia — nawet jeśli nie posiada ona własnego zespołu reagowania. Osoby wewnątrz organizacji powinny wiedzieć, jak należy postępować w przypadku wystąpienia incydentu w zależności od i z uwzględnieniem roli, jaką pełnią w instytucji. Pozwala to już od momentu powzięcia podejrzenia, że do naruszenia doszło, postępować metodycznie z wiedzą, komu i w jaki sposób należy to zgłosić. Przed wystąpieniem incydentu należy również określić zakres kompetencji poszczególnych osób w zakresie podejmowania decyzji oraz komunikacji wewnątrz i na zewnątrz organizacji, w tym do mediów, organów ścigania oraz innych podmiotów, które należy powiadomić (np. w związku z naruszeniem ochrony danych osobowych).

Jednym z obowiązków wynikającym z ustawy o krajowym systemie cyberbezpieczeństwa jest wskazanie do właściwego zespołu CSIRT osoby do kontaktu dla podmiotów krajowego systemu cyberbezpieczeństwa. Podmioty publiczne powinny wypełnić ten obowiązek przed wystąpieniem incydentu. Dla większości podmiotów publicznych właściwym CSIRT jest CSIRT NASK[4].

Dodatkowo, aby mieć możliwość poddania obiektywnej weryfikacji zgłoszenia, warto określić katalog zgłoszeń (zagrożeń) i informacji, które są potrzebne do ich weryfikacji, np. dzienników zdarzeń systemowych czy logów z urządzeń sieciowych, aby określić niezbędny oraz prawnie dopuszczalny zakres i czas ich retencji.

Procedurę reagowania na incydenty naruszenia cyberbezpieczeństwa można powiązać z procedurami związanymi z ochroną danych osobowych i zarządzaniem ciągłością działania, ponieważ obszary te są nierozerwalnie związane z incydentami i ich obsługą.

Jeśli instytucja zamierza obsługiwać incydenty, w tym usuwać ich skutki, bez udziału podmiotów zewnętrznych, wykorzystując własne zasoby na jednym lub wielu etapach przedstawionych w dalszej części niniejszego poradnika, powinna wcześniej rozpoznać te zasoby. Jeśli instytucja zamierza korzystać z podmiotów zewnętrznych, również warto je zidentyfikować i ustalić, czy i w jakim zakresie może oczekiwać wsparcia oraz na jakich warunkach. **Często zdarza się, że podmioty publiczne oczekują od zespołu CSIRT NASK kompleksowego obsłużenia incydentu, podczas gdy CSIRT**

[4] Rekomendacje zespołu CSIRT NASK w zakresie zgłaszania osób kontaktowych

NASK nie świadczy takich usług[5]. Ciężar obsługi incydentu zawsze leży po stronie właściciela danego systemu.

Detekcja i analiza

W przypadku odnotowania przez użytkownika lub administratora anomalii należy zidentyfikować, czy problem naprawdę istnieje oraz czy jest incydentem. Wiele nietypowych oznak działania systemów informatycznych można racjonalnie wyjaśnić i nie są one związane z wystąpieniem naruszenia cyberbezpieczeństwa, ale mogą dotyczyć np. awarii sprzętu lub błędów oprogramowania.

Incydenty związane z działaniem oprogramowania ransomware najczęściej wykrywane są przez użytkowników systemów informatycznych, rzadziej przez administratorów. Detekcja następuje zazwyczaj na ostatnim etapie ataku, którym jest zaszyfrowanie danych przez złośliwe oprogramowanie i użytkownik nie może uzyskać dostępu np. do bazy danych systemu księgowego. Ten etap jest poprzedzony wieloma innymi czynnościami, które już zostały wykonane przez atakujących, i które prawdopodobnie mogłyby zostać zidentyfikowane, gdyby tylko systemy informatyczne były na bieżąco odpowiednio monitorowane.

Detekcję potencjalnego naruszenia, jeszcze zanim dojdzie do zaszyfrowania danych, można oprzeć o monitoring zachowań wskazujących na przygotowania do przeprowadzenia ataku mogącego skutkować naruszeniami cyberbezpieczeństwa. W przypadku ataków ransomware zanim dojdzie do zaszyfrowania danych obserwujemy przede wszystkim nieudane próby logowania do RDP, nietypowy ruch w sieci (np. z/do krajów, z którymi połączeń nie można racjonalnie wyjaśnić, oraz transfer danych, którego nie można uzasadnić), wykorzystanie narzędzi takich jak mimikatz, CobaltStrike.

Po potwierdzeniu, że doszło do incydentu, należy go wstępnie przeanalizować, aby określić jego zakres, wpływ i możliwość przywrócenia możliwości realizowania zadań przez instytucję nim dotkniętą. Pozwoli to sklasyfikować incydent i nadać priorytet jego obsłudze.

W przypadku incydentów, w tym ataków ransomware, aby nadać priorytet obsługi i odtworzenia, należy określić przede wszystkim:

Wpływ incydentu na funkcjonowanie instytucji:

- jakie systemy zostały dotknięte naruszeniem (np. systemy, za pomocą których realizowane są zadania zlecone w zakresie wypłaty świadczeń z programu Rodzina 500+),
- czy incydent skutkuje znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności

[5] Opis usług świadczonych przez zespół CSIRT NASK (CERT Polska)

obywatelskich lub życia i zdrowia ludzi (np. brak możliwości świadczenia usług dla pacjentów w ciężkim stanie z powodu koronawirusa przez szpital jednoimienny lub świadczenie usług o obniżonej jakości bez możliwości skorzystania z pełnej funkcjonalności systemów medycznych, które również mogą być objęte incydentem),

- czy zadanie, które było realizowane przez system, może zostać wykonane w terminie (np. do incydentu doszło 7 dni przed terminem wypłaty świadczeń i paczki przelewów do banku nie mogą być sporządzone w alternatywny sposób, nawet przy zaangażowaniu większej liczby pracowników do wprowadzenia danych niezbędnych do wykonania przelewu, a konieczność zweryfikowania uprawnień do pobierania świadczeń przez każdego świadczeniobiorcę przekracza możliwości instytucji odpowiedzialnej za wypłatę świadczeń),
- czy zadanie może zostać wykonane w inny sposób (np. czy można sporządzić listę świadczeniobiorców inaczej niż systemu, do którego nie ma dostępu),
- czy zadanie będzie realizowane z uszczerbkiem dla klientów (np. świadczenia zostaną wypłacone w terminie, ale później, niż miało to miejsce zazwyczaj, więc świadczeniobiorcy, dla których świadczenie 500+ jest jedynym stałym przychodem, przez kilka dni nie będą mieli środków na zaspokojenie bieżących potrzeb swojej rodziny),
- czy incydent spowoduje znaczną stratę finansową (np. nieterminowa wypłata świadczeń 500+, będzie związana z zapłatą odsetek za opóźnienie),
- czy realizacja zadania w obniżonej jakości będzie miała wpływ na wizerunek instytucji (np. opóźniona wypłata świadczeń 500+ przed Wielkanocą).

Wpływ incydentu na informacje:

- jakie atrybuty jakich zbiorów danych zostały naruszone – poufność, integralność, dostępność (np. naruszona została dostępność bazy danych systemu, ale dane beneficjentów nie wyciekły i numery rachunków bankowych beneficjentów nie zostały zmienione),
- jakie jest prawdopodobieństwo naruszenia pozostałych atrybutów (np. niskie prawdopodobieństwo naruszenia poufności, ponieważ nie stwierdzono objawów wycieku danych),
- jaki jest wpływ incydentu na funkcjonowanie innych organizacji (np. na serwerach urzędu gminy, utrzymywane były bazy danych ośrodka pomocy społecznej, co ma negatywny wpływ na funkcjonowanie tej instytucji).

W przypadku ransomware atakujący żądają zapłaty okupu za przywrócenie dostępu do danych (przekazanie narzędzia deszyfrującego). W niektórych przypadkach sprawcy żądają zapłaty okupu nie tylko za przekazanie narzędzi deszyfrujących, ale również za nieujawnianie danych wykradzionych z systemów informatycznych zaatakowanej instytucji[6]. **Warto podkreślić, że nie zawsze zapłata**

[6] W przypadku London Borough of Hackney, gminy zamieszkiwanej przez ok. 270 tys. mieszkańców, urząd odmówił zapłaty okupu i przywracał ciągłość działania, pomimo znacznych strat i kosztu, szacowanych na ok. 10 mln funtów brytyjskich. Ponieważ instytucja odmówiła zapłaty żądanego okupu, atakujący ujawnili wykradzione dane, które obejmowały dane osobowe, w tym dane wrażliwe, takie jak protokoły z wywiadów środowiskowych u osób objętych szczególnym rodzajem pomocy z uwagi na m.in. choroby psychiczne.

będzie się wiązała z odszyfrowaniem plików. Nie ma żadnej gwarancji, że przestępca będzie chciał – a czasami nawet mógł – odszyfrować pliki.

Możliwość odtworzenia po incydencie:

- czy instytucja ma (lub nie ma) możliwość odtworzenia zaatakowanych zasobów i procesów po incydencie we własnym zakresie (np. posiada kopie zapasowe i środowisko, na którym po stronie serwerowej może odtworzyć systemy dotknięte incydentem, oraz zatrudnia osoby, które mogą to technicznie zrealizować, jednak potrzebna jest pomoc dostawcy oprogramowania dziedzinowego do ponownego skonfigurowania i podłączenia stacji użytkowników, którzy pracują w tym systemie).

Należy pamiętać, że nie tylko ludzie, ale i systemy informatyczne nie są przystosowane do długotrwałego działania w trybie *kryzysowym*. Przedłużająca się praca w takim trybie może znacznie zwiększać ryzyko popełnienia błędów przez ludzi i maszyny oraz wystąpienia kolejnych naruszeń. Mogą być one nie tylko związane z naruszeniem ochrony danych osobowych, jak np. utrata poufności danych, ale również bardzo poważnych w skutkach błędów wpływających negatywnie na życie i zdrowie ludzkie (np. sprzęt medyczny zawsze pozwoli na wykonanie badania bez dostępu do systemu, z którego pobierane są zlecenia, i bez danych pacjenta, kiedy nie ma możliwości wprowadzenia danych pacjenta do systemu i wystawienia zlecenia na badanie, jednak sprzęt medyczny nie jest przystosowany do przechowywania danych, a długotrwałe wykonywanie badań bez zleceń z systemu zewnętrznego znacznie zwiększa ryzyko popełnienia błędu kwalifikowanego jako incydent medyczny).

Powiadomienie o incydencie

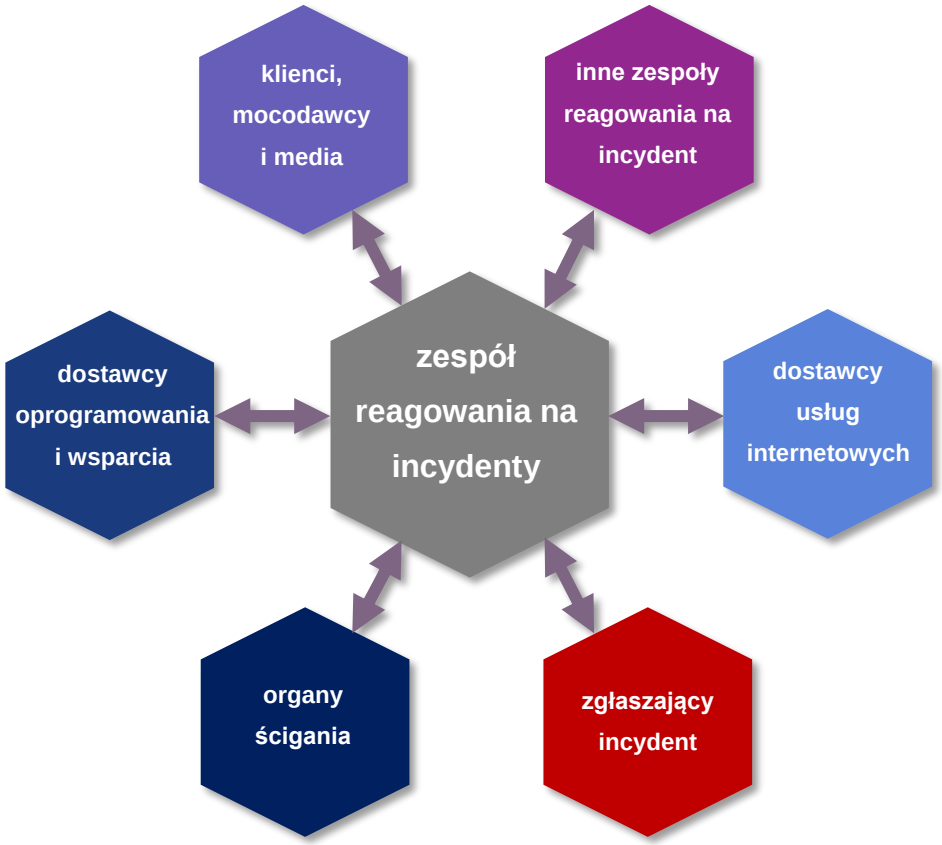
W zależności od wstępnej analizy charakteru naruszenia cyberbezpieczeństwa, instytucja ma możliwość, a często również obowiązek, powiadomienia określonych podmiotów o incydencie. Dokładne wymagania dotyczące zgłaszania incydentu zależą od rodzaju naruszenia i instytucji, jednak zwykle obejmują powiadomienie nie tylko kierownika jednostki, ale także:

- osoby odpowiedzialnej za ochronę danych osobowych, która ocenia ryzyko wystąpienia naruszenia danych osobowych, a na podstawie tej oceny właściwa osoba podejmuje dalsze działania przewidziane przepisami prawa,
- CSIRT NASK (w przypadku każdego incydentu cyberbezpieczeństwa),
- organów ścigania (w stosownych przypadkach).

W ramach komunikacji zewnętrznej do mediów, pomocne mogą być wskazówki z RFC 2196:

(1) Nie przekazuj szczegółów technicznych. Szczegółowe informacje o incydencie mogą dostarczyć informacji dla innych atakujących, którzy przeprowadzą atak w podobny sposób na inne organizacje, a nawet mogą niekorzystnie wpłynąć na możliwości pociągnięcia do odpowiedzialności osób odpowiedzialnych.

(2) Nie spekuluj w komunikatach prasowych. Spekulacje dotyczące sprawcy lub motywu najczęściej są omyłkowe i mogą zaburzyć obraz incydentu.
(3) Współpracuj z organami ścigania, aby mieć pewność, że dowody są chronione. Jeśli wszczęte jest śledztwo (dochodzenie), upewnij się, że nie ujawniasz dowodów.
(4) Nie udzielaj informacji, dopóki nie jesteś przygotowany. Nie pozwól, aby media pozyskały informacje, które nie są dla nich przeznaczone.
(5) Nie pozwól, aby uwaga mediów opóźniła obsługę incydentów. Pamiętaj, że prawidłowe zamknięcie incydentu ma najwyższy priorytet.



Obraz 2. Komunikacja ze stronami zewnętrznymi (za: NIST SP 800-61r2)

Dodatkowo należy również uwzględnić komunikację wewnętrzną, która jest szczególnie istotna w przypadku poważnych incydentów negatywnie wpływających na pracę całej instytucji. Pracownikom należy w miarę możliwości wyjaśnić, co się wydarzyło i jakie procedury awaryjne zostają uruchomione oraz precyzyjnie określić, co mogą, a czego nie powinni przekazywać dalej. Dotyczy to zarówno komunikacji na zewnątrz swoich działów (np. należy rozważyć, czy dział IT może mówić pracownikom wydziałów, że doszło do ataku ransomware, który sparaliżował cały urząd, ponieważ pracownik księgowości otworzył złośliwy dokument, który pobrał złośliwe oprogramowanie, które zaszyfrowało wszystkie serwery i stacje robocze), jak i na zewnątrz całej organizacji (np. czy pracownicy urzędu mogą przekazywać interesantom, że urząd padł ofiarą ataku hakerskiego, czy może jednak wystarczy

powiedzieć, że systemy są niedostępne, ponieważ informatycy poprawiają funkcjonowanie systemów informatycznych urzędu).

Zabezpieczenie dowodów

Dowody podczas obsługi incydentu powinny być gromadzone nie tylko na potrzeby ewentualnego postępowania przygotowawczego, ale również na potrzeby analizy incydentu. Określić należy dopuszczalny zakres i czas retencji określonego rodzaju dowodów. Zdarza się bowiem, że w trakcie obsługi incydentu pochopnie podejmowane są decyzje dotyczące strategii powstrzymania (np. wyłączenie wszystkich systemów i urządzeń powodującej nieodwracalną utratę materiału, na podstawie którego można byłoby ustalić przebieg ataku. Błędy zazwyczaj skutkują obniżeniem jakości materiału źródłowego, a nawet utratą dowodów.

W pierwszej kolejności powinno się zabezpieczyć dane najbardziej ulotne – z pamięci RAM, logi urządzeń sieciowych, następnie dane z zainfekowanych systemów oraz systemów z nimi połączonych. Dowody należy zabezpieczyć przed podjęciem kolejnych działań, w tym zwłaszcza przed usunięciem incydentu i jego skutków (np. przed usunięciem zidentyfikowanego złośliwego oprogramowania, przed wyczyszczeniem serwerów i stacji roboczych, przed dokonaniem zmian w konfiguracji sieci). Zabezpieczane dowody należy również opisać, w miarę możliwości określając np. rolę, jaką pełnił dany host i jak był połączony z innymi elementami sieci.

W przypadku złośliwego oprogramowania szyfrującego pliki należy pamiętać o tym, że oprogramowanie może działać uporczywie, to znaczy szyfrować nośniki podłączane do zainfekowanych stacji (np. pliki na pendrive oraz pliki backupu na zewnętrznych nośnikach), a także doszyfrowywać jeszcze nie zaszyfrowane pliki po ponownym uruchomieniu, często z zupełnie innymi kluczami szyfrującymi, niż przy poprzednim wykonaniu złośliwego oprogramowania. Oznacza to, że **jeśli szyfrowanie dopiero się rozpoczęło i stacja robocza została odcięta od zasilania, a następnie włączona przez funkcjonariusza organów ścigania, który chce dokonać oględzin i sprawdzić, czy pliki na pewno się zaszyfrowały – to należy założyć, że pliki, które wcześniej nie zostały zaszyfrowane, przy ponownym uruchomieniu na pewno zostaną zaszyfrowane. Już wyłączonych systemów nie należy podnosić, a jeśli konieczne jest przejrzenie zawartości dysku takiego komputera, najlepiej zrobić to w trybie wyłącznie odczytu (ang. read only, ro) jako zasobu podłączanego do innego, niezainfekowanego systemu (np. bootowanego z innego nośnika), a nie poprzez włączenie zainfekowanego komputera.**

W przypadku konieczności zabezpieczenia dowodów należy przyjąć założenie, że zatrzymanie na potrzeby postępowania, a nawet odłączanie i przenoszenie do laboratorium kryminalistycznego, fizycznych maszyn jest kontrproduktywne, niecelowe i negatywnie wpłynie na pracę instytucji dotkniętej incydentem, w tym zwłaszcza na odtwarzanie po incydencie i przywracanie ciągłości działania,

zwłaszcza w zakresie realizowania zadań publicznych. **Obecne możliwości techniczne informatyki śledczej dają możliwość zabezpieczenia dowodów na miejscu, bez uszczerbku dla wartości dowodowej i nie ma konieczności zatrzymywania serwerów i stacji roboczych.**

Powstrzymanie

Większość incydentów może zostać ograniczona, jeśli tylko zostaną w odpowiedni sposób powstrzymane. Wybór strategii powstrzymania zależy od rodzaju incydentu i od apetytu na ryzyko danej instytucji. W przypadków ataków ransomware zalecanym sposobem powstrzymania jest:

1) odcięcie dostępu do sieci zewnętrznej,
2) odcięcie dostępu do sieci wewnętrznej,
3) hibernacja wszystkich serwerów i stacji roboczych, a w przypadku środowisk wirtualnych, wykonanie migawek.

Wstępna analiza nie zawsze daje odpowiedź na to, czy i które hosty są dotknięte incydentem – czyli, czy i z których komputerów w instytucji można nadal korzystać, a jeśli tak, to w jakim zakresie (np. z dostępem do sieci, w tym sieci Internet, czy bez niego), ani czy korzystanie z tych urządzeń nie zaciera istotnych dowodów w sprawie incydentu. Instytucje powinny zatem określić:

- akceptowalne ryzyko korzystania z systemów, co do których nie ma pewności, że nie zostały objęte incydentem (np. nie ma pewności, że poświadczenia nie wyciekły, a atakujący mają lub mogą mieć dostęp do tych systemów, w tym mogą dokonywać dalszych uszkodzeń i naruszeń np. poufności danych przetwarzanych w systemach, a także usuwać dowody swoich działań),
- konieczność świadczenia usług (np. obsługi interesantów) pomimo ryzyka naruszenia poufności, integralności lub dostępności danych,
- czas i zasoby potrzebne do wdrożenia wybranej strategii (np. czy informatyk ma uprawnienia do odcięcia dostępu do sieci i może to zrobić z konsoli czy musi fizycznie wypiąć kable z portów przełącznika),
- skuteczność strategii (np. czy wyłączenie tylko zaszyfrowanych stacji roboczych zatrzyma szyfrowanie pozostałych),
- czas trwania (np. pracownicy pracują w ograniczonym zakresie lokalnie na swoich stacjach roboczych przez tydzień, a następnie ich stacje robocze są czyszczone, sprawdzane i podłączane do czystej strefy po stronie serwerowej).

I dopiero potem na tej podstawie podjąć decyzję o wyborze strategii powstrzymania incydentu.

Usunięcie

Usunięcie przyczyny incydentu skutkuje zazwyczaj również usunięciem wszelkich dowodów, które do tej pory nie zostały zabezpieczone. Obejmuje ono przede wszystkim usunięcie złośliwego oprogramowania i zainfekowanych plików oraz upewnienie się, że przywracane systemy nie są ani zainfekowane, ani podatne. Dotyczy to również sytuacji, w której systemy przywracane są z kopii zapasowych, które przed podłączeniem do odtwarzanej infrastruktury należy sprawdzić, załatać znane podatności i zmienić dane dostępowe, które mógł pozyskać atakujący, w tym do systemów dostępnych z zewnątrz, takich jak poczta elektroniczna, i systemów zewnętrznych, takich jak bankowość elektroniczna. Systemy, których nie można przeinstalować, należy uważnie przeaudytować.

Odtworzenie

Odtworzenie powinno odbywać się zgodnie z ustalonym harmonogramem prac naprawczych, z uwzględnieniem krytyczności zadań realizowanych przez instytucję. **Przywrócenie ciągłości działania dla większości podmiotów publicznych jest najważniejszym celem obsługi incydentu.** Nierzadko jest to proces bardziej czasochłonny od wszystkich poprzednich kroków, ponieważ wymaga przywrócenia danych i często związany jest ze zmianą dotychczasowej architektury systemów informatycznych w instytucji, aby ograniczyć ryzyka wystąpienia naruszenia w przyszłości.

Odtworzenie po incydencie często przekracza możliwości instytucji, która padła ofiarą ataku i w tym zakresie niezbędne jest udzielenie wsparcia przez m.in. dostawców sprzętu, od których można wypożyczyć lub zakupić niezbędne urządzenia (np. serwery, ponieważ z tych, które znajdują się w instytucji, nie można się odtworzyć) i oprogramowania, zwłaszcza dziedzinowego, a także specjalistów z zakresu bezpieczeństwa. Pomogą oni m.in. w audycie infrastruktury, w tym serwerów i stacji roboczych, na których nie można z wielu względów przywrócić czystych kopii, ale organizacja musi z nich korzystać, aby realizować krytyczne zadania.

Odtworzenie może obejmować przywracanie systemów ze sprawdzonych i czystych kopii (tzw. złotych obrazów), migawek (w przypadku maszyn zwirtualizowanych), przeskanowanych plików użytkowników. Przywracane systemy należy utwardzić[7] – np. odpowiednio zmodyfikować reguły na urządzeniach sieciowych, wprowadzić segmentacje (np. na bazie VLAN i zapór ogniowych), zainstalować poprawki bezpieczeństwa, zmienić dane uwierzytelniające. Odtwarzając systemy, administratorzy oraz użytkownicy systemów potwierdzają ich poprawne funkcjonowanie.

W przypadku incydentów związanych z działaniem oprogramowania szyfrującego, bardzo rzadko zachodzi konieczność usunięcia wszystkich plików wszystkich użytkowników w danej instytucji – pliki,

[7] Brytyjskie NCSC (National Cyber Security Centre) podaje jako przykład ofiarę, która zapłaciła żądany wielomilionowy okup i uzyskała narzędzie deszyfrujące, jednak nie utwardziła swoich systemów. W rezultacie, ponownie padła ofiarą ataku ransomware.

w tym wiadomości poczty elektronicznej, można przywracać, jednak należy zachować należytą ostrożność. Powinno się zadbać nie tylko o przeskanowanie ich narzędziami wykrywającymi złośliwe oprogramowanie, ale również zbadać zgodność konfiguracji stacji użytkownika z dobrymi praktykami producenta systemu operacyjnego i innych systemów, z których użytkownik potrzebuje korzystać, ponieważ zaniedbania w tym obszarze niemal na pewno przełożą się na powodzenie ataków w przyszłości.

W przypadku zaszyfrowanych plików, gdy nie ma ich kopii zapasowych lub gdy zostały one uszkodzone, należy przede wszystkim zweryfikować, czy pliki zostały uszkodzone w całości czy tylko w części. Jeśli pliki zostały uszkodzone w całości, zazwyczaj nie ma możliwości przywrócenia ich bez wykorzystania narzędzia deszyfrującego – albo oferowanego przez sprawców, którego pozyskanie wiąże się z zapłatą żądanego okupu, albo stworzonego przez analityków złośliwego oprogramowania, którzy potrafią znaleźć słabości oprogramowania szyfrującego i stworzyć narzędzie deszyfrujące, co zdarza się niezwykle rzadko. Jeśli pliki zostały uszkodzone jedynie w części, zazwyczaj można je naprawiać i z pomocą dostawców oprogramowania dziedzinowego przywracać poprawne funkcjonowanie systemów, np. do wypłaty świadczeń 500+ czy systemów księgowych.

Decyzja o zapłacie okupu za uzyskanie narzędzia deszyfrującego, które, zgodnie z obietnicami atakujących, ma pozwolić na przywrócenie pełnej funkcjonalności zaszyfrowanych danych (i systemów), może wiązać się z negatywnymi konsekwencjami prawnymi dla ofiar i pośredników dokonujących zapłaty szantażującym w imieniu ofiar, ponieważ uiszczenie okupu może naruszać sankcje nałożone przez Unię Europejską na podmioty odpowiedzialne za cyberataki lub w te ataki zaangażowane. Przepisy unijne obejmują również zakaz udostępniania funduszy przez osoby i podmioty z Unii Europejskiej sankcjonowanym osobom i podmiotom.

Aktywność po incydencie

Po zakończeniu obsługi incydentu należy wyciągnąć wnioski z jego przebiegu i obsługi. Może to pomóc w identyfikacji luk, w tym niedoskonałości procedur, oraz dać impuls do zmiany, np. w wyniku oceny stosunku kosztów odtworzenia systemów po ataku do kosztów wprowadzenia mechanizmów prewencyjnych. W NIST SP 800-61r2 zawarte są listy zadań pomagające ocenić incydent oraz skorygować obsługę incydentu w przyszłości.

Lista zadań, które pozwalają ocenić incydent:

- przejrzenie dzienników, formularzy i raportów oraz innej dokumentacji pod względem zgodności z wcześniej ustalonymi zasadami i procedurami reagowania na incydenty,
- określenie, które prekursory i wskaźniki incydentu zostały zarejestrowane, aby określić jak skutecznie incydent został zarejestrowany i zidentyfikowany,
- ustalenie, czy incydent spowodował szkody, zanim został wykryty,

- ustalenie, czy zidentyfikowano rzeczywistą przyczynę incydentu,
- ustalenie wektora ataku, wykorzystanych luk w zabezpieczeniach oraz charakterystyki docelowych lub targetowanych systemów, sieci i aplikacji,
- ustalenie, czy incydent jest powtórzeniem poprzedniego incydentu,
- oszacowanie szkód pieniężnych wynikających z incydentu (np. koszt zatrzymania krytycznych procesów, na które incydent miał negatywny wpływ),
- określenie różnicy między wstępną a ostateczną oceną skutków incydentu,
- określenie jakie, jeśli w ogóle, środki mogłyby zapobiec incydentowi.

Lista pytań pomocnych przy skorygowaniu obsługi incydentu w przyszłości:

- jakie działania naprawcze mogą lub powinny zostać podjęte, aby zapobiec podobnym incydentom w przyszłości?
- na jakie prekursory lub wskaźniki należy zwrócić uwagę w przyszłości, aby wykryć podobne incydenty?
- jakie dodatkowe narzędzia lub zasoby są potrzebne do wykrywania, analizowania i łagodzenia skutków przyszłych incydentów?
- jakie informacje potrzebne były wcześniej?
- czy kierownictwo i personel poradzili sobie z incydentem? Czy istniały procedury? Czy procedury były adekwatne?
- co kierownictwo i personel powinni zrobić inaczej, jeśli w przyszłości wystąpi podobny incydent?
- czy i jakie działania negatywnie wpłynęły na odtworzenie po incydencie?
- w jaki sposób poprawić wymianę informacji z innymi organizacjami?

Wersja 1.0.2

2021.04.22

Licencja