Ministerstwo Cyfryzacji

Rekomendacje cyberbezpieczeństwa dla podmiotów sektora ochrony zdrowia

(Kwiecień 2020 r.)

Informacja o rekomendacjach

Poniższy poradnik jest przeznaczony głównie dla specjalistów ds. bezpieczeństwa IT i administratorów systemów i sieci w podmiotach objętych ustawą o krajowym systemie cyberbezpieczeństwa.

Rekomendacje te nie zawierają wyczerpującej listy wszystkich środków, które można wdrożyć w celu ochrony przed zagrożeniem systemów informacyjnych, ale są przygotowane w celu szybkiego wdrożenia minimalnych zaleceń bezpieczeństwa, z uwagi na wyjątkową sytuację związaną z pandemią COVID-19 i krytycznym znaczeniem zapewnienia niezakłóconego świadczenia usług przez placówki ochrony zdrowia. Wszystkie informacje zawarte w tym materiale są jedynie rekomendacjami. Przyjęcie odpowiednich środków ochrony przed zagrożeniem zawsze należy do konkretnego administratora systemu. Jednak należy pamiętać, że administrator systemu musi również wziąć pod uwagę takie elementy jak: potencjał podmiotu do wdrożenia tych środków, w tym możliwości ich wdrożenia w swoich systemach oraz wpływ na ich działanie, czy świadczenie usług. Należy mieć także na uwadze harmonogram wdrożenia danych środków bezpieczeństwa.

W przypadku podmiotów nieobjętych ustawą o krajowym systemie cyberbezpieczeństwa, niniejszy materiał pomocniczy może być zalecanym przewodnikiem w celu zwiększenia ochrony ich systemów informacyjnych.

W przypadku zgłoszenia cyberataku lub incydentu prosimy o kontakt z zespołem reagownia na incydenty komputerowe CSIRT NASK. Incydenty można zgłaszać poprzez wypełnianie interaktywnego formularza dostępnego na stronie: https://incydent.cert.pl/.

Uwaga:

Niniejszy dokument pierwotnie został **opracowany przez czeski Urząd ds. cyberbezpieczeństwa i bezpieczeństwa informacji (NUKIB)** i służy jako pomocniczy poradnik. Nie zastępuje żadnych przepisów ustawowych, ani wykonawczych. Ministerstwo Cyfryzacji otrzymało zgodę NUKIB na wykorzystanie dokumentu bazowego.

Zestaw rekomendowanych środków przeciwdziałających oraz ograniczających skutki incydentu związanego z cyberbezpieczeństwem

1.1 Podstawowe informacje o zalecanych działaniach dla podmiotów z sektora zdrowia

1.1.1 Należy zwiększyć świadomość użytkowników na zagrożenia związane z spear-phishingiem. Należy poinformować użytkowników, którzy w ostatnich dniach otworzyli podejrzane załączniki, aby skontaktowali się z zarządcą infrastruktury. Ponadto należy ostrzec użytkowników o możliwości „maskowania" phishingu przy pomocy plików wykonywalnych, takich jak: „obraz.png.exe ", „tekst.txt.exe", „dokument.pdf.exe" itp.

Cel środka: zminimalizowanie ryzyka, że atakujący przedostanie się do systemu za pomocą ataku typu **spear-phishing**.

Rekomendacje:

Należy ostrzec użytkowników o ryzyku spear-phishingu, w oparciu o poniższe obszary:

1. Co to jest spear-phishing lub phishing i jak je rozpoznawać?[1]
2. Nastawienie na konieczność weryfikacji tożsamości naszego partnera w przypadku wątpliwości co do autentyczności nadawcy wiadomości.
3. Nieotwieranie załączników i linków w wiadomościach e-mail w przypadku wątpliwości co do autentyczności nadawcy.
4. Wyłączenie „makr" w plikach MS Office.
5. Prawdopodobieństwie „maskowania" plików z rozszerzeniem „.exe" (np. „obraz.png.exe", „tekst.txt.exe", „dokument.pdf.exe" itp.).
6. Jak się zachować i gdzie się zwrócić o pomoc w przypadku podejrzenia spear-phishingu?

W tej kwestii można wykorzystywać materiał dot. phishingu przygotowany przez Departament Cyberbezpieczeństwa Ministerstwa Cyfryzacji „Czym jest PHISHING i jak nie dać się nabrać na podejrzane widomości e-mail oraz SMS-y"[2].

Dobrym pomysłem jest również dodanie do tego materiału, udostępnionego w Twojej organizacji, podstawowych informacji kontaktowych do pracowników

[1] Dedykowany poradnik przygotowany przez Ministerstwo Cyfryzacji w oparciu o materiał bazowy National Cyber Security Center z Wielkiej Brytanii „Czym jest PHISHING i jak nie dać się nabrać na podejrzane widomości e-mail oraz SMS-y".
[2] Poradnik dołączony do rekomendacji oraz dostępny na portalu gov.pl.

bezpieczeństwa IT oraz poinformowanie użytkowników o konieczności niezwłocznego zgłoszenia każdej podejrzanej wiadomości phishingowej.

Aby otrzymać więcej informacji i uzyskać dostęp do wszechstronnej analizy metod spear-phishingu, a także poznać zasady obrony przed tego typu atakami, zapraszamy na stronę internetową brytyjskiego NCSC:
https://www.ncsc.gov.uk/guidance/phishing

1.1.2 Zablokuj możliwość uruchamiania, szczególnie w dokumentach .doc i .docx, „active content" i „makr", przy użyciu ustawień systemowych

Cel środka: Zapobieganie możliwości naruszenia bezpieczeństwa systemu za pomocą „makr" z plików MS Office.

Rekomendacje:

„Makra" w dokumentach Microsoft Office są bardzo często wykorzystywane do dystrybucji malware. Aby zminimalizować to ryzyko oraz w związku z ewentualną potrzebą, zalecamy postępowanie w następujący sposób – o ile oczywiście poniższe środki wpisują się w potrzeby Twojej organizacji:

1. Wyłącz „makra" dla wszystkich użytkowników.
2. Zezwól poszczególnym użytkownikom na używanie „makr" jedynie w opcji „na żądanie".

Aby uzyskać instrukcje dotyczące ustawiania odpowiednich zasad, zapoznaj się z dokumentacją na stronie Microsoft[3].

1.1.3 Natychmiast zablokuj zdalny dostęp do Waszej infrastruktury i zablokuj usługi otwarte w sieci publicznej, z wyjątkiem absolutnie tych niezbędnych (publiczne adresy IP urządzeń podłączonych do sieci można wyszukać w dostępnych wyszukiwarkach internetowych, w tym także „open ports" lub „forgotten ports" oraz usługi dostępne z poprzez sieć publiczną)

Cel środka: zminimalizowanie ryzyka, że atakujący przeniknie do systemu, wykorzystując podatności w systemie lub atak typu „brute force".

[3] https://support.office.com/pl-pl/article/W%C5%82%C4%85czanie-i-wy%C5%82%C4%85czanie-makr-w-plikach-pakietu-Office-12b036fd-d140-4e74-b45e-16fed1a7e5c6

Rekomendacje:

Sprawdź usługi udostępniane w sieci publicznej. Pozostaw aktywne tylko te usługi, które są niezbędne do funkcjonowania organizacji. Usługi te obejmują w szczególności komunikację, która jest:

1. Niezbędna do funkcjonowania usług opartych na danym systemie.
2. Niezbędna dla bezpieczeństwa samego systemu (zdalne monitorowanie, aktualizacje bezpieczeństwa systemów itp.).
3. Niezbędna do informowania opinii publicznej (komunikacja e-mail, webprezentacje itp.).
4. Niezbędna do obsługi infrastruktury łączności (protokoły DNS, Border Gateway Protocol, sprawdzanie ważności certyfikatów itp.) oraz serwery proxy.

Efektem będzie ograniczenie dostępu do usług z sieci publicznej – Internetu - (także takich dostępnych za pośrednictwem VPN, czy protokołów RDP, SSH, SMB, dostępu do bazy danych, czy administracji systemem), jeśli są one podłączone do ważnych systemów i nie spełniają jednego z powyższych warunków.

Jeśli nie możesz zablokować niektórych dostępów, zaleca się zezwolenie na dostęp tylko przez VPN lub tylko dla określonych adresów IP.

1.1.4 Błyskawicznie utwórz kopie zapasowe „offline" i kontynuuj tworzenie takich kopii zapasowych zgodnie z zasadami istotności danych w Twojej organizacji

Cel środka: Zapewnienie dostępności kopii zapasowych nawet w przypadku wystąpienia incydentu.

Rekomendacje:

Aby zapewnić bezpieczne przechowywanie kopii zapasowych, należy je skopiować na nośnik danych offline (pamięć flash, dysk twardy lub inny) i zweryfikować przesłane dane. Najlepiej można to zrobić, przywracając kopię zapasową z nowo utworzonego nośnika. Pamiętaj, że można to zrobić tylko poza środowiskiem produkcyjnym. Jeśli nie jest to możliwe z powodów technicznych, można sprawdzić przynajmniej skróty plików (hashe) kopii zapasowych offline. Procedura ta jest kluczowa dla zapewnienia, że kopie zapasowe nie zostaną utracone, jeśli serwer kopii zapasowych lub platforma wirtualna zostaną naruszone (lub zaszyfrowane) np. w wyniku ataku typu ransomware.

1.1.5 Sprawdź spójność już utworzonych kopii zapasowych

Cel środka: Zapewnienie funkcjonalności kopii zapasowych nawet w przypadku wystąpienia incydentu.

Rekomendacje:

Sprawdź, czy istniejące pliki kopii zapasowych działają. Wykonaj testowe przywracanie serwerów i stacji. Pamiętaj, że można to zrobić tylko poza środowiskiem produkcyjnym. W przypadku stwierdzenia, że jeden lub więcej plików kopii zapasowej nie działa, należy natychmiast wykonać nową kopię zapasową systemu. Kroki te należy podjąć w przypadku najbardziej krytycznych systemów. Podczas badania plików kopii zapasowych nie należy ignorować żadnych wzajemnych zależności. Jednym z przykładów może być serwer bazy danych lub cały klaster bazy danych przechowywany w innym miejscu. W takich przypadkach należy również sprawdzić te systemy.

1.1.6 Zaktualizuj oprogramowanie antywirusowe

Cel środka: Zapewnienie podstawowej ochrony urządzenia przed szkodliwym kodem.

Rekomendacje:

Narzędzie do ochrony przed złośliwym kodem (program antywirusowy, czy antymalware) powinno być zainstalowane we wszystkich możliwych systemach operacyjnych. W pierwszej kolejności zrób to dla urządzeń z zainstalowanym systemem Windows, gdyż większość tego typu złośliwych kodów jest napisanych pod system firmy Microsoft. W przypadku systemów wirtualnych, ochrona za pomocą rozwiązania bezagentowego („agentless") nie może być uznana za wystarczającą.

Jeśli Twojej w organizacji nie jest używane żadne narzędzie/oprogramowanie do ochrony przed złośliwym kodem, konieczne jest przynajmniej aktywowanie wbudowanej domyślnej ochrony w danym systemie - jeśli jest.

1.2 Inne zalecenia, które można wdrożyć, aby zapobiec skutkom incydentu lub je ograniczyć

Poniższe rekomendacje są uszeregowane według priorytetu, który należy im przypisać.

1.2.1 W systemach zmień hasła do kont uprzywilejowanych. Przejrzyj polityki bezpieczeństwa, i w razie potrzeby, zaktualizuj odpowiednie zasady korzystania z kont uprzywilejowanych.

Cel środka: Zapobieganie ewentualnemu atakującemu, który już wdarł się do Twojego systemu, dalszej aktywności.

Rekomendacje:

Wymuszenie zmiany haseł wszystkich kont uprzywilejowanych jest konieczne. Warto pamiętać o podstawowych zasadach bezpieczeństwa haseł do kont uprzywilejowanych m.in. w oparciu o dobre praktyki opracowane przez ekspertów z brytyjskiego NCSC https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/managing-user-privileges

Co więcej, zalecana jest także kontrola wszystkich kont uprzywilejowanych i blokowanie tych, które nie są już używane, lub usunięcie uprawnień dla tych kont, które nie potrzebują tych uprawnień.

Zalecamy korzystanie z poradnika *Fine Grained Password Policies* [4], aby ustawić politykę tworzenia haseł, które pozwolą ustalić zasady tworzenia haseł dla różnych grup użytkowników.

Zalecamy także użycie *Active Directory administrative tier model* [5], w celu ustawienia odpowiednich polityk korzystania z kont uprzywilejowanych.

Co więcej, konieczne jest również uniemożliwienie administratorom domen logowania się na dowolnych stacjach roboczych i serwerach, oprócz stacji „domain controller". Poprzez to uniemożliwimy atakującemu przejęcie konta uprzywilejowanego. Ponieważ hash administratora pozostaje zapisany w pamięci podręcznej stacji, atakujący mógłby uzyskać autoryzację administratora domeny, gdyby stacja robocza została zaatakowana.

1.2.2 Sprawdź i upewnij się, że system tworzenia kopii zapasowych jest oddzielony od innych systemów, aby nawet uzyskanie „highest-level" uprawnień autoryzacyjnych do systemu, dla którego utworzono kopię zapasową, nie pozwoliło na usunięcie kopii zapasowych.

Cel środka: Uniemożliwienie atakującemu usunięcie kopii zapasowych, nawet jeśli uzyska uprawnienia administratora domeny.

Rekomendacje:

Zabezpiecz systemy kopii zapasowych w taki sposób, aby nie można było uszkodzić systemów kopii zapasowych i usunąć lub uszkodzić kopii zapasowych, nawet

[4] https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-functional-levels
[5] https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

w sytuacji, gdy zagrożone jest konto uprzywilejowane (np. administratora domeny/firmy).

Jeśli systemem kopii zapasowych można zarządzać za pośrednictwem współużytkowanego, uprzywilejowanego konta (np. konta administratora domeny/firmy), wówczas napastnik będzie mógł usunąć, uszkodzić lub zaszyfrować pliki kopii zapasowych.

W środowisku Microsoft Office można to rozwiązać, odłączając od domeny zarówno fizyczne, jak i wirtualne maszyny, które świadczą usługę tworzenia kopii zapasowych oraz korzystając z lokalnych kont do logowania się. Ewentualnie można utworzyć specjalne konto zarezerwowane dla tej czynności. Istnieje jednak potrzeba oceny wpływu na inne usługi i funkcje systemu.

1.2.3 Zapobieganie wszelkim dostępom i wzajemnym połączeniom między systemami ważnymi dla zapewnienia funkcjonowania organizacji i systemów lub sieci, które nie są ważne dla świadczenia usług lub bezpieczeństwa systemu

Cel środka: Zapobieganie wszelkim połączeniom międzysystemowym (poza przypadkami, gdy jest to konieczne) i tym samym ograniczanie możliwości rozprzestrzeniania się złośliwego oprogramowania.

Rekomendacje:

Pociąga to za sobą ograniczenie wszelkiej komunikacji do systemów istotnych dla funkcjonowania organizacji (w szczególności świadczenia usług). Jeżeli inna sieć (np. Internet, sieć innej organizacji lub inna sieć tej samej organizacji) może uzyskać dostęp do sieci, która jest niezbędna do zapewnienia funkcjonowania organizacji, rozważ, jak ważne jest to połączenie dla świadczenia usług lub bezpieczeństwa systemu.

W miarę możliwości należy ograniczyć komunikację pomiędzy stacjami roboczymi.

1.2.4 Sprawdź segmentację sieci i zarządzanie ruchem między segmentami, oceń sytuację i podejmij niezbędne środki, aby zapewnić przynajmniej podstawową segmentację.

Cel środka:

Zapobieganie rozprzestrzenianiu się malware lub ograniczenie ruchu napastnika.

Rekomendacje:

Segmentacja sieci i zarządzanie ruchem między segmentami (porty między segmentami, ograniczenia dotyczące dozwolonych usług) mogą znacząco ograniczyć skutki potencjalnego zdarzenia związanego z incydentem. Sprawdź konfigurację

elementów sieci pod kątem słabych punktów lub reguł. Przeprowadź kontrolę ruchu pomiędzy siecią zewnętrzną i wewnętrzną. Reguły ograniczające mogą skomplikować sprawę dla atakujących i dać organizacji czas na reakcję.

1.2.5 Rozważ aktualizację wszystkich używanych systemów, oczywiście pod warunkiem, że aktualizacja jest już sprawdzona. Jeśli aktualizacja została przetestowana i działa, wykonaj ją.

Cel środka:

Zapewnienie aktualności używanych systemów, a tym samym zwiększenie ich bezpieczeństwa i odporności na incydenty.

Rekomendacje:

Nieaktualizowane systemy często zawierają znane podatności, które atakujący wykorzystują do naruszenia bezpieczeństwa systemu. Dlatego konieczne jest zapewnienie aktualności używanych systemów. Jeżeli istnieje niepodważalny powód, aby nie dokonywać aktualizacji systemu (na przykład, aktualizacja spowodowałaby unieważnienie gwarancji, system mógłby się rozpaść, przestać działać lub mogłyby wystąpić inne niedopuszczalne skutki), nie ma potrzeby dokonywania aktualizacji takiego systemu. Konieczne będzie jednak podjęcie zastępczych środków bezpieczeństwa.

Należy pamiętać, że aktualizacja nie powinna być przeprowadzana, jeżeli mogłaby spowodować większe szkody niż potencjalne zdarzenie związane z incydentem lub jeżeli wykonanie takiego zadania miałoby negatywny wpływ na świadczenie usług.

Pamiętaj, każda aktualizacja musi zostać przetestowana poza środowiskiem produkcyjnym przed jej użyciem, jak opisano powyżej.

1.2.6 Zbadaj ważne plany ciągłości działania i plany działania na wypadek awarii związane z funkcjonowaniem systemów, aby zweryfikować ich ważność, skuteczność i przydatność, w szczególności w odniesieniu do możliwej niedostępności tych systemów.

Cel środka: sprawdzenie, czy istnieją plany ciągłości działania i czy plany na wypadek sytuacji awaryjnej są aktualne i można je stosować w razie potrzeby.

Rekomendacje:

Sprawdź, czy istnieją plany ciągłości działania i plany reagowania na wypadek awarii oraz czy są one uaktualniane i ważne. Sprawdź, czy nie ma brakujących planów. Taka weryfikacja powinna dotyczyć przede wszystkim następujących kwestii:

1. Czy plany podkreślają znaczenie systemów i przewidują priorytetowe przywrócenie systemów krytycznych;
    a. Czy priorytetyzacja przywracania systemów uwzględnia współzależność systemów i usług.
2. Czy plany zawierają listy osób odpowiedzialnych za poszczególne elementy systemu, a także dostępne są aktualne dane kontaktowe osób odpowiedzialnych.
3. Czy istnieje zaktualizowana lista dostawców sprzętu/oprogramowania i ich osób kontaktowych, zawierająca dane kontaktowe (telefony komórkowe, e-maile); ważna jest weryfikacja procedur współpracy z dostawcami w przypadku wystąpienia sytuacji awaryjnej, uzgodnionych czasów reakcji itp. (w przypadku problemów lub braku porozumienia, zalecamy uzgodnienie z dostawcami zasad współpracy w nagłych przypadkach).

1.2.7 Zagwarantowanie, że plany ciągłości działania i plany na wypadek sytuacji awaryjnej związane z działaniem systemów będą przechowywane oddzielnie od systemów, dla których plany te są przetwarzane (np. na oddzielnym nośniku pamięci, w formie drukowanej itp.).

Cel środka: Zapewnienie dostępności planów na wypadek incydentu do wykorzystania w razie potrzeby.

Rekomendacje:

Doświadczenia z atakami ransomware pokazały, że plany ciągłości działania, plany awaryjne i podobne dokumenty są często przechowywane na systemach/mediach, które atakujący może zaszyfrować lub usunąć, lub które są wyłączone w celu ochrony innych systemów. W związku z tym, plany te nie są dostępne w krytycznym momencie. Dlatego też plany takie muszą być przechowywane poza systemami, na przykład na zabezpieczonym przed zapisem nośniku wymiennym (jeżeli konieczne jest podłączenie takiego nośnika do potencjalnie zagrożonego komputera) lub w formie wydruku.

1.2.8 Jeśli plany ciągłości działania i plany na wypadek sytuacji nadzwyczajnej związane z działaniem systemów nie są aktualne lub nie zostały przygotowane, przygotuj je co najmniej dla najbardziej krytycznych systemów istotnych dla świadczenia usług.

Cel środka: posiadanie aktualnych i dających się wdrożyć planów ciągłości działania i planów awaryjnych, aby Twoja organizacja mogła funkcjonować nawet w przypadku incydentu. Rekomendacje:

W przypadku braku planów ciągłości operacyjnej i planów reagowania na wypadek awarii muszą one być przygotowane przynajmniej w takim zakresie, aby na ich podstawie można było przywrócić dostępność ważnych systemów. W pierwszej kolejności należy zająć się następującymi kwestiami:

1. Określenie praw i obowiązków administratorów i osób zaangażowanych w zapewnienie funkcjonowania organizacji. Kto będzie to robił, co i kiedy w sytuacji awaryjnej, procedury eskalacji itp.
2. Wykorzystanie szacowania ryzyka i analizy skutków do oceny i oszacowania potencjalnego ryzyka związanego z zagrożeniem dla ciągłości działania. Należy stworzyć podstawowy scenariusz postępowania w przypadku zagrożenia poufności, dostępności i integralności danych w systemach, a także wpływu na świadczenie danej usługi.
3. W oparciu o wyniki oceny ryzyka i analizy skutków należy określić cele zarządzania ciągłością operacyjną poprzez:
    a. określenie minimalnego poziomu świadczonych usług dopuszczalnego w zakresie użytkowania, obsługi i administrowania systemem;
    b. określenie czasu niezbędnego do przywrócenia minimalnego poziomu działania świadczonych usług systemowych po wystąpieniu incydentu; oraz
    c. określenie punktu odzyskiwania danych jako okresu, za który dane zostaną odzyskane po incydencie.
4. Stworzenie procedur służących realizacji powyższych celów, tj. sposobu, w jaki organizacja zapewni utrzymanie określonego poziomu usług, że dane rzeczywiście zostaną odzyskane itp.

1.2.9 Nie usuwaj żadnych danych dotyczących incydentu bez zgody organów ścigania. Poinformuj wszystkich administratorów oraz wszystkich zajmujących się w Twojej organizacji bezpieczeństwem i bezpieczeństwem IT (operacyjne) na temat tego obowiązku.

Cel środka: Zapewnienie możliwości przeprowadzenia pełnego „forensic".

Rekomendacje:

Wszystkie dane (obrazy serwerów, pliki bezpieczeństwa, zapisy dotyczące monitoringu sieci, historia logów itp.) są ważne w śledztwie w sprawie incydentu, w szczególności do identyfikacji źródła i metody rozprzestrzeniania się malware w sieci oraz identyfikacji urządzeń, które mogły zostać zainfekowane. W przypadku niektórych rodzajów ransomware odszyfrowanie danych może być dostępne dopiero w późniejszym terminie. Dlatego ważne jest, aby nie usuwać żadnych danych bez zgody organów ścigania.

Należy podkreślić, że nawet nieostrożne obchodzenie się z danymi może prowadzić do utraty metadanych istotnych dla dochodzenia w sprawie zdarzenia. Może to jeszcze bardziej skomplikować działania naprawcze po incydencie.

1.2.10 Wyłącznie dla podmiotów świadczących usługi zdrowotne: Odseparowanie sprzętu medycznego np. tomografów komputerowych, urządzeń rentgenowskich, od reszty sieci.

Cel środka: Oddzielenie sprzętu medycznego od pozostałej części sieci, a tym samym ograniczenie rozprzestrzeniania się malware.

Zalecenie:

Aby móc świadczyć wymagane usługi nawet po incydencie, sprzęt medyczny musi być oddzielony od innych systemów w taki sposób, aby sprzęt ten był sprawny nawet po odłączeniu od reszty sieci. Otwarte porty między sieciami są dozwolone, ale muszą być zarządzane za pomocą listy dozwolonej łączności. Środki te są istotne dla zachowania bezpieczeństwa tych systemów. Te wyspecjalizowane systemy często działają na unikalnych i przestarzałych systemach operacyjnych, a inne środki zabezpieczenia tych systemów nie zawsze mają zastosowanie.