Plan Bezpieczeństwa Cyfrowego

Zrealizowany przez zespół

CERT.NGO

CERT.NGO

Spis Treści

Wstęp

Postępująca informatyzacja kolejnych elementów naszego życia prywatnego i służbowego prowadzi wręcz do wykładniczego wzrostu wykorzystywanych przez nas usług i technologii. Internet na dobre zagościł w naszych domach i – jak to zwykle bywa – wiedza człowieka stale goni coraz to nowsze i bardziej zaawansowane techniki komputerowe. Taki stan rzeczy wymaga ciągłego poszerzania wiedzy i umiejętności z zakresu szeroko rozumianego IT, na które to wiele organizacji nie posiada wystarczających zasobów ludzkich i czasowych. Wychodząc z tego założenia, wykorzystując najlepsze praktyki i stale aktualizowaną wiedzę, autorzy postanowili stworzyć niniejszy dokument, który krok po kroku pomoże organizacji przeprowadzić diagnozę wewnętrzny w celu uporządkowania wykorzystywanych technologii, a także wypunktowania niedostatków lub – mówiąc bardziej bezpośrednio – luk w bezpieczeństwie, mogących mieć istotny wpływ na funkcjonowanie organizacji i bezpieczeństwo przechowywanych przez nią danych. Powyższy cel wydaje się zasadny i niezwykle istotny ze względu na coraz bardziej wyrafinowane i agresywne metody ataków na organizacje, zarówno przy wykorzystaniu technicznej wiedzy (rzadziej) jak i socjotechniki (najczęściej).

Rezultatem przeprowadzonej diagnozy powinno być – jak już wspomniano – zwiększenie bezpieczeństwa organizacji, ale również zwiększenie świadomości pracowników i osób na stanowiskach kierowniczych, zebranie informacji dotyczących posiadanej infrastruktury i zasobów (np. w celu jej rozwoju w przyszłości) oraz skonstruowanie planu działania na wypadek wystąpienia incydentu. Te cztery rezultaty uporządkują temat IT w organizacji w sposób wystarczający do zarządzania nim w przyszłości.

Zdajemy sobie sprawę, że duża część poniższego materiału może być dla osób przeprowadzających diagnozę nowością. Aby proces przebiegł sprawnie, a jego wynik był dla organizacji wartością dodaną, podzielono go na części mniej i bardziej techniczne. Dla lepszego

zrozumienia tych drugich, na końcu dokumentu wykonawcy diagnozy odnaleźć mogą glosariusz, wyjaśniający bardziej techniczne terminy.

Każda z części rozpoczyna się od krótkiego wstępu, wyjaśniającego działanie (co będzie przedmiotem działań), cel oraz przewidywany wynik. Następnie zawarte są pytania, dotyczące konkretnych usług, technologii, rozwiązań i polityk, stosowanych w organizacji. To właśnie ta część przysparzać może największych problemów, wobec czego zachęcamy do korzystania z glosariusza (problematyczne terminy zaznaczone są na zielono). Na końcu każdej części znajdują się opisy, wyjaśniające zasadność objęcia danych kwestii zainteresowaniem.

Przed przystąpieniem do procesu, zachęcamy do zapoznania się z sekcją „Przed rozpoczęciem diagnozy". Akapit ten traktuje o informacjach, które przydać się mogą w procesie, pomoże przygotować się do niego, a także wskazać osoby najbardziej kompetentne w danych dziedzinach.

Przed rozpoczęciem diagnozy

Dla sprawnego przeprowadzenia diagnozy, należy wskazać osobę (albo osoby) odpowiedzialną za jej przeprowadzenie. Najlepiej, gdyby była to osoba o największej wiedzy informatycznej. W zależności od rozmiaru organizacji i stopnia złożoności jej infrastruktury, zapewne potrzeba będzie konsultować pewne tematy z zewnętrznymi wykonawcami (np. firmą obsługującą stronę WWW) lub osobami wewnątrz organizacji, odpowiedzialnymi za poszczególne części działalności, np.:

- Dział media/komunikacja może posiadać wiedzę na temat domen, CMS oraz wykorzystywanych do mass-mailingu usług;
- Osoby zarządzające mogą posiadać wiedzę na temat usług pocztowych, polityk bezpieczeństwa i przeprowadzonych szkoleniach;
- Księgowość może posiadać wiedzę na temat liczby urządzeń służbowych (spis środków trwałych), licencji i domen (ze względu na regularne opłaty), wykorzystywanych programów księgowych (a co za tym idzie – serwerów z bazami danych);

W idealnej sytuacji uda się odpowiedzieć na wszystkie pytania. W rzeczywistości wykonawca diagnozy napotka na różnego rodzaju bariery i problemy. Ważne, aby w takiej sytuacji zanotować nawet szczątkowe informacje i zdjęcia, które udało się zebrać. Dla przykładu:

„W pokoju nr 2 odnaleziono urządzenie marki Technicolor, które według tabliczki producenta jest modelem CGA2121. Podłączone jest ono do białego kabla, który prowadzi do skrzynki dostawcy sieci. Do urządzenia Technicolor podłączone jest czarne urządzenie, którego tabliczka informuje o nazwie i modelu – TP-Link Archer C7. Do obu urządzeń organizacja nie posiada danych dostępowych."

Niniejszy dokument zawiera opis zdecydowanej większości technologii, które mogą być stosowane w organizacji. Nie znaczy to, że każda z części będzie konieczna dla przeprowadzenia diagnozy (np. organizacja może nie posiadać w ogóle serwerów lokalnych, toteż ta część może być dla nich nieprzydatna). W przypadku braku opisywanego rozwiązania technologicznego (lub lokalu-siedziby w ogóle), daną część diagnozy można pominąć z adnotacją „nie dotyczy".

Dla uporządkowania zebranych informacji polecamy stworzyć dokument w oparciu o części procesu, opisane dalej. Pomocna okazać się może tabela, zawierająca spis sprzętu, jego lokalizacji, dostępów, przeznaczenia, właściciela i – w określonych przypadkach – adresu IP w sieci wewnętrznej (np. w przypadku serwerów bazodanowych, NASów itp.). Większość pozyskanych informacji będzie miała jednak format tekstowy, toteż dokument o tym charakterze zapewne będzie wiodącym.

Ważne: diagnoza w całości może zostać przeprowadzona samodzielnie. Niemożność odpowiedzi na wiele pytań również jest wartościową informacją zwrotną – pozwala wykazać słabe punkty w wiedzy organizacji.

Część pierwsza: Podstawy funkcjonowania organizacji

- ➔ **Działanie:** spis wykorzystywanych technologii, dostępów administracyjnych, sposobów komunikacji i wymiany danych;
- ➔ **Cel:** identyfikacja technologii niebezpiecznych/przestarzałych, wskazanie luk w systemie, inwentaryzacja dostępów do zasobów;
- ➔ **Wynik:** poprawa bezpieczeństwa wykorzystywanych technologii, ograniczenie dostępu osobom nieuprawnionym, spis dostępnego oprogramowania.

Część pierwsza traktuje o podstawach funkcjonowania organizacji w kontekście IT – mowa tutaj o urządzeniach sieciowych, sposobie przechowywania danych, usługach chmurowych, komunikacji mailowej, domenach, stronach WWW i urządzeniach końcowych. Są to komponenty składające się na ciągłą i stabilną pracę organizacji. Jest to część zdecydowanie najbardziej techniczna, mająca na celu stworzenie ogólnego obrazu wykorzystywanych w organizacji technologii, spisu dostępów do najważniejszych komponentów i przeglądu środków trwałych/wyposażenia.

Wytworzenie dokumentu w oparciu o siedem powyższych akapitów stanowi trzon i punkt wyjścia do dalszej diagnozy infrastruktury organizacji.

1. **Sieć:**
    a. Gdzie znajdują się urządzenia sieciowe
    b. Czy dostęp do nich ma osoba upoważniona
    c. Czy hasła dostępowe zostały zmienione z domyślnych
    d. Czy skonfigurowany jest dostęp do sieci wewnętrznej z miasta (*public internet access*)
    e. Czy stosowane są zabezpieczenia w postaci firewall
    f. Czy wykorzystywany jest VPN
    g. Czy firmware urządzeń sieciowych jest aktualizowany
    h. Czy wydzielona jest sieć gościnna
    i. Czy stosowane są VLANy

2. **Storage on-premise:**
    a. Czy wykorzystywane są serwery plików
    b. W jaki sposób następuje łączenie do serwerów plików
    c. Czy dostęp możliwy jest również spoza sieci organizacji (z miasta)
    d. Czy wykonywana jest kopia bezpieczeństwa plików z udziału sieciowego (serwera plików)
        i. W jakie miejsce jest wykonywana
    e. Czy urządzenie jest aktualizowane
    f. Czy dostęp wymaga logowania loginem i hasłem
        i. Czy login i hasło jest inne dla każdego użytkownika

3. **Cloud:**
    a. Czy wykorzystywane są usługi chmurowe
    b. Czy usługi chmurowe są administrowane przez organizację
    c. Czy w organizacji wydzielona jest osoba odpowiedzialna za określanie poziomu dostępów do zasobów chmurowych
    d. Czy wykonywane są przeglądy bezpieczeństwa kont użytkowników
    e. Czy wymuszane są konkretne polityki dot. bezpieczeństwa na kontach użytkowników

4. **Poczta**
    a. Z usług jakiego dostawcy poczty korzysta organizacja
    b. Czy organizacja posiada dane dostępowe do panelu klienta usługodawcy
    c. Czy stosowane są polityki bezpieczeństwa dotyczące np. przekierowania poczty
    d. Czy organizacja ma poprawnie skonfigurowany SPF, DKIM, DMARC
    e. Czy organizacja korzysta z usług mass-mailingu (mailchimp, mailgun itp.)

f. Co dzieje się z kontami byłych pracowników
g. W jaki sposób archiwizowane są stare wiadomości

5. WWW

a. Ile domen posiada organizacja
b. Czy organizacja panuje nad okresami odnowienia aktywnie wykorzystywanych domen
c. Czy organizacja deleguje zarządzanie stroną WWW firmie/osobie trzeciej
d. Czy organizacja dba o aktualizacje CMS oraz wtyczek do WWW
e. Czy organizacja posiada spis dostępów do paneli klienta oraz stref DNS przypisanych do domen
f. Czy organizacja przeprowadza testy bezpieczeństwa wykorzystywanych stron WWW (szczególnie w przypadku zbierania danych osobowych)
g. Czy organizacja monitoruje dostępy do paneli stron WWW

6. Urządzenia końcowe - komputery

a. Z jakich systemów operacyjnych korzystają użytkownicy
b. Czy występuje podział na urządzenia prywatne i służbowe
c. W jaki sposób następuje logowanie do komputera
d. Czy użytkownicy posiadają uprawnienia administratora
e. Czy stosowane są regularne aktualizacje systemu operacyjnego i zainstalowanych aplikacji
f. Czy dyski z systemem operacyjnym są szyfrowane
g. Czy występują urządzenia, do których dostęp ma więcej niż jedna osoba
h. Czy stosowane są rozwiązania typu MDM do zdalnego zarządzania i implementacji polityk bezpieczeństwa na urządzeniach końcowych

i. Czy użytkownicy korzystają z wtyczek do przeglądarki – jeżeli tak, to z jakich

7. **Urządzenia końcowe – telefony**
    a. Z jakich systemów operacyjnych korzystają użytkownicy
    b. Czy występuje podział na urządzenia prywatne i służbowe
    c. Jakimi kontami zalogowani są do telefonów
    d. W jaki sposób zabezpieczony jest dostęp do telefonów
    e. Czy stosowane są regularne aktualizacje systemu operacyjnego i zainstalowanych aplikacji
    f. Czy wykonywane są kopie zapasowe do chmury
    g. Czy włączone jest zdalna lokalizacja urządzenia w przypadku jego zgubienia/kradzieży

Dlaczego powyższe punkty są ważne?

↘ **Sieć** – szczególnie istotny dla bezpieczeństwa komponent. Znajomość infrastruktury sieciowej organizacji pomaga identyfikować słabe punkty (nieaktualizowane urządzenia) oraz jej wąskie gardła, utrudniające pracę (przestarzałe, wadliwe lub zepsute urządzenia). Spisanie dostępów do urządzeń sieciowych daje możliwość kontroli nad ruchem przychodzącym i wychodzącym. Odpowiednia konfiguracja ruchu sieciowego ma istotny wpływ na niskopoziomowe bezpieczeństwo organizacji. Przegląd sieci może również pomóc w poprawie jakości połączenia przewodowego/bezprzewodowego.

↘ **Storage on-premise** – wykorzystanie infrastruktury serwerowej w organizacji niesie za sobą odpowiedzialność dot. utrzymania działania usługi i jej bezpieczeństwa. Wykazanie obecnych w organizacji serwerów lokalnych może pomóc w inwentaryzacji takich zasobów nie tylko pod kątem zawartości, a także zastosowanych systemów operacyjnych czy połączeń oraz ich bezpieczeństwa.

↘ **Cloud** – rozwiązania chmurowe są szczególnie istotne w dobie pracy hybrydowej albo zdalnej. Przegląd wykorzystywanych przez użytkowników chmur publicznych pozwoli na ujednolicenie przepływu dokumentów i komunikacji. Przeprowadzoną diagnozę wykorzystać można również do przeglądu dostępów i kont użytkowników w celu eliminacji nadmiernych uprawnień lub kont nieaktywnych. W przypadku braku implementacji chmury, zaproponowane mogą zostać konkretne platformy różnych dostawców, usprawniające i wspomagające pracę w organizacji.

↘ **Poczta** – nieodzowny element infrastruktury każdej, nawet najmniejszej organizacji. Ustalenie dostawcy poczty, jej konfiguracji i zabezpieczeń ma wpływ na jakość korzystania z usługi oraz bezpieczeństwo wymiany wiadomości między pracownikami i nie tylko. Konta email są również najczęstszym wektorem ataku; nieodpowiednio zabezpieczone mogą doprowadzić do włamania na konto i ewentualnego wycieku danych.

↘ **WWW** – zarówno od strony zarządzania domenami i strefami DNS, jak i od strony swoistej wizytówki organizacji, strona WWW powinna być objęta szczególnym zainteresowaniem podczas procesu diagnozy. Spis domen, ich dat wygaśnięcia oraz aktualizacje silnika pozwalają uniknąć nieprzyjemnych sytuacji związanych z utraceniem domeny, przejęciem serwisu bądź utratą zaufania ze strony odbiorców. Okresowe testy bezpieczeństwa pozwalają na identyfikację luk bezpieczeństwa w wykorzystywanych technologiach WWW.

↘ **Urządzenia końcowe (komputery i telefony)** – odpowiednio skonfigurowane urządzenia końcowe to klucz do bezpiecznej pracy zarówno w środowisku służbowym, jak i poza nim. Składają się na to elementy związane z logowaniem, politykami bezpieczeństwa, wykorzystywanymi aplikacjami oraz uprawnieniami użytkownika. To właśnie urządzenia końcowe, wykorzystywane na co dzień, skupiają w sobie usługi i dostępy wymienione we wcześniejszych punktach, toteż często stają się punktem zapalnym incydentu.

Część druga: Bezpieczeństwo użytkowników i komunikacji

- ➔ **Działanie:** przegląd polityk bezpieczeństwa
- ➔ **Cel:** identyfikacja słabych punktów, wskazanie najlepszych praktyk
- ➔ **Wynik:** poprawa bezpieczeństwa kont użytkowników

Część druga odnosi się do kwestii bezpieczeństwa użytkowników oraz sposobów komunikacji wewnątrz organizacji. Najbardziej palące problemy – 2FA (weryfikacja dwuetapowa), hasła, bezpieczeństwo poczty i kont, kanały komunikacji i aktualizacje – zostały rozbite na bardziej szczegółowe pytania dotyczące konfiguracji, nadzoru i egzekwowania polityk.

Wnioski z odpowiedzi posłużą wyklarowaniu braków w politykach bezpieczeństwa i konfiguracjach kont użytkowników. Podsumowanie pozwoli na zastosowanie odpowiednich zabezpieczeń w kontekście kont i komunikacji bez szczególnej wiedzy technicznej, ponieważ większość z opisywanych funkcji jest możliwa do włączenia przez samego użytkownika.

1. **Weryfikacja dwuetapowa**
    a. Czy na kontach służbowych, służących do łączenia się z zasobami służbowymi, wymuszana jest weryfikacja dwuetapowa
    b. Czy – w przypadku wykorzystania urządzeń prywatnych – na kontach prywatnych wymuszana jest weryfikacja dwuetapowa
    c. Czy wszystkie wykorzystywane technologie pozwalają na zastosowanie weryfikacji dwuetapowej przy połączeniu do zasobów służbowych
    d. Z jakich rozwiązań korzysta się przy konfiguracji weryfikacji dwuetapowej (SMS, email, aplikacja, klucz bezpieczeństwa)

2. **Polityka haseł**

a. Czy organizacja wymusza regularną zmianę haseł
b. Czy organizacja określa stopień złożoności hasła i wymusza stosowanie się do niego podczas zmiany hasła
c. Czy organizacja korzysta z rozwiązań typu menedżer haseł
d. Czy organizacja monitoruje wycieki haseł użytkowników przy użyciu portali typu haveibeenpwned.com
e. Czy organizacja pozwala na wykorzystywanie prywatnych menedżerów haseł do przechowywania haseł powiązanych z zasobami służbowymi
f. Czy organizacja pozwala na zapisywanie haseł w przeglądarce
g. Czy organizacja zezwala na samodzielne resetowanie haseł użytkownikom

3. Konta pocztowe

a. Czy wymuszane jest stosowanie weryfikacji dwuetapowej przy logowaniu do kont pocztowych
b. Czy ogranicza się logowanie w klientach pocztowych do programów od zaufanych dostawców
c. Czy monitoruje się alerty oraz podejrzane logowania do usług mailowych
d. Czy zezwala się na logowanie do klientów pocztowych w aplikacjach mobilnych

4. Konta chmurowe

a. Czy organizacja ma świadomość na temat wszystkich usług chmurowych, wykorzystywanych w środowisku służbowym (mowa tu o występowaniu zjawiska tzw. *shadow IT*)
    i. Czy organizacja napotyka problemy z wdrożonymi usługami chmurowymi, przez co użytkownicy unikają korzystania z nich i znajdują własne „boczne kanały”

b. Czy organizacja administruje wszystkimi usługami chmurowymi przez nią wykorzystywanymi
c. Czy organizacja wykorzystuje platformy chmurowe zgodnie z regulaminem licencjonowania dostawcy

5. Kanały komunikacji

a. Jakie komunikatory wykorzystywane są w organizacji
b. W przypadku komunikatorów połączonych z numerem telefonu – jakie numery (prywatne czy służbowe) są do nich wykorzystywane
c. Czy komunikatory zewnętrzne (niepowiązane z usługami chmurowymi takimi jak M365 czy Google Workspace) wykorzystywane są do wymiany dokumentów lub informacji poufnych
d. Czy do komunikacji wykorzystuje się programy, które szyfrują komunikację między użytkownikami

6. Aktualizacje

a. Czy w organizacji obecna jest osoba, odpowiadająca za regularne aktualizacje urządzeń końcowych i urządzeń sieciowych
b. Czy przypomina się użytkownikom o konieczności regularnej instalacji aktualizacji dla zwiększenia bezpieczeństwa wykorzystywanych rozwiązań
c. Czy w organizacji wykorzystuje się oprogramowanie antywirusowe

Dlaczego powyższe punkty są ważne?

↘ **Uwierzytelnianie dwuskładnikowe (2FA)** – jeden z najważniejszych elementów zabezpieczających konta użytkowników. Mechanizm 2FA dodaje do zabezpieczeń konta drugi

czynnik, który oprócz hasła wymagany jest podczas logowania. Jest to jedna z najważniejszych metod chroniących użytkowników przed przejęciem konta w wyniku phishingu/wycieku danych logowania. Wymuszenie stosowania 2FA w organizacji powinno być jednym z pierwszych kroków, podjętych w procesie hardeningu organizacji. Znane są różne metody 2FA – od kodów SMS (powoli wycofywanych), przez kody i powiadomienia push z aplikacji aż po klucze bezpieczeństwa (np. Yubico). Metoda 2FA powinna być dopasowana do stopnia zaawansowana i świadomości użytkowników.

↘ **Polityka haseł** – odpowiednia polityka haseł zdecydowanie poprawia bezpieczeństwo kont użytkowników. Powinna być oparta o najlepsze praktyki, zawarte w dokumentacji dużych instytucji i dostawców (np. NIST, Google, Microsoft, instytucje rządowe o charakterze cyber). Idealnym rozwiązaniem jest wdrożenie menedżera haseł zarządzanego z poziomu organizacji, który wspomagać może użytkowników w generowaniu odpowiednio skomplikowanych haseł, przechowywaniu ich oraz autouzupełnianiu na właściwych stronach.

↘ **Konta pocztowe** – w tym kontekście konta pocztowe traktujemy jak każde inne konto, jednak ze szczególnym uwzględnieniem jego przeznaczenia, tj. wymiana korespondencji. Wyodrębnienie kont pocztowych jako objętych szczególnym zainteresowaniem w trakcie diagnozy ma uwypuklić ich szczególne narażenie na ataki i zwrócić uwagę organizacji na zastosowane na nich zabezpieczenia i polityki, takie jak 2FA i określone programy pocztowe.

↘ **Konta chmurowe** – nierzadko zdarza się, że dane służbowe przetwarzane są na dyskach chmurowych bez nadzoru organizacji (konta M365 Personal, konta Google, prywatny Dropbox, iCloud). Część dot. kont chmurowych ma na celu identyfikację takich niezarządzanych rozwiązań (*shadow IT*) lub – w przypadku istnienia instancji chmurowej – przegląd dostępów i wykorzystywanych zasobów chmurowych w celu ich optymalizacji, klasyfikacji i obniżenia kosztów licencjonowania.

↘ **Kanały komunikacji** – podobnie jak w przypadku kont chmurowych, do komunikacji mogą być wykorzystywane kanały, nad którymi nie panuje organizacja. W taki sposób pracownicy mogą

wymieniać się informacjami na tematy służbowe. Zidentyfikowanie takich kanałów oraz odpowiednie zabezpieczenie kont użytkowników wprowadza wartość dodaną do bezpieczeństwa organizacji.

↘ **Aktualizacje** – szeroko rozumiana potrzeba aktualizacji urządzeń końcowych (po stronie użytkownika) oraz sprzętu utrzymującego ruch (Access Pointy, routery, drukarki) sprzyja wzmacnianiu bezpieczeństwa organizacji. Aktualizacje systemów i aplikacji łatają podatności nierzadko aktywnie wykorzystywane przez atakujących.

Część trzecia: Szkolenia i zarządzanie incydentami

- ➔ **Działanie:** podjęcie tematów na styku bezpieczeństwa/świadomości użytkownika
- ➔ **Cel:** wskazanie dobrych praktyk i wzmocnienie bezpieczeństwa organizacji
- ➔ **Wynik:** świadome korzystanie z urządzeń i oprogramowania w kontekście zagrożeń w sieci

Trzecia część pomoże rozstrzygnąć, jak prezentuje się podejście organizacji do szkolenia pracowników i uczulania ich na kwestie bezpieczeństwa w sieci. Podejmuje również temat procedur na wypadek wystąpienia incydentu bezpieczeństwa, zarówno od strony zarządzania, jak i technicznej.

Odpowiedzi na poniższe pytania pomogą wykazać luki w procesie wdrażania użytkowników i utrzymywania ich wiedzy na temat bezpieczeństwa w sieci na zadowalającym poziomie.

1. **Szkolenia**
    a. Czy przeprowadzane są regularne szkolenia dot. aktualnych zagrożeń w sieci dla pracowników i kadry zarządzającej
    b. Czy użytkownicy informowani są o przyczynach wprowadzania zabezpieczeń (złożone hasła, menedżery haseł, weryfikacja dwuetapowa) podczas ich implementacji

c. Czy użytkownicy poddawani są np. testom phishingowym
d. Czy użytkownicy wiedzą, jak identyfikować IoC w kontekście ich kont służbowych
e. Czy użytkownicy wiedzą, do kogo mogą zgłosić się w przypadku wystąpienia incydentu
f. Czy użytkownicy rozumieją podstawowe zagadnienia z zakresu cyberprzestępczości (phishing, fałszywe strony WWW, podszywanie się pod nadawcę wiadomości)

2. Bezpieczeństwo w sieci

a. Czy użytkownicy potrafią rozpoznać różne metody przestępców, mające wyłudzić od nich dane logowania
b. Czy użytkownicy wiedzą, w jaki sposób mogą sprawdzić swoje konta prywatne w celu ochrony przed atakiem celowanym (ustawienia bezpieczeństwa, miejsca logowania, zaufane urządzenia)

3. Zarządzanie incydentami

a. Czy pracownicy i kadra zarządzająca ma świadomość, czym jest incydent bezpieczeństwa
b. Czy organizacja posiada zatwierdzony plan działania w przypadku wystąpienia incydentu
c. Czy organizacja posiada osobę delegowaną do jak najszybszej obsługi incydentu
d. Czy wyklarowane zostały konkretne procedury, mające jak najbardziej zniwelować skutki incydentu
e. Czy organizacja wie, w jaki sposób może zabezpieczyć logi dotyczące incydentu, mogące służyć za dowody w ewentualnym postępowaniu przed sądem

Dlaczego powyższe punkty są ważne?

↘ **Szkolenia** – stanowią niezwykle ważny element budowania odporności organizacji. Odpowiednio przeszkoleni pracownicy (stanowiący pierwszą linię obrony przed większością ataków) potrafią samodzielnie wykrywać ataki i bronić się przed nimi. Prowadzenie regularnych szkoleń pozwala na aktualizację wiedzy na temat zagrożeń zarówno po stronie administratora, jak i samych pracowników, którzy poznać mogą najczęstsze wektory ataku i uwrażliwić się na ich występowanie.

↘ **Bezpieczeństwo w sieci** – punkt łączący się bezpośrednio ze szkoleniami. Użytkownicy, którzy zostali odpowiednio przeszkoleni w związku ze środowiskiem służbowym, powinni mieć również wiedzę na temat możliwości zabezpieczenia siebie i swojej rodziny w życiu prywatnym. Nierzadko zdarza się, że zasoby firmowe obsługiwane są na komputerach prywatnych lub poprzez prywatne konta w social media. Taki stan rzeczy sprawia, że świadomość użytkowników dot. zagrożeń w sieci powinna być także budowana w kontekście życia prywatnego, bowiem zagrożenie atakiem nie kończy się w momencie wyjścia z pracy.

↘ **Zarządzanie incydentami** – w przypadku wystąpienia incydentu ważna jest zdecydowana i właściwa reakcja. Stworzenie planu działania „na wszelki wypadek" pozwoli w kompleksowy sposób obsłużyć incydent bez wprowadzania niepotrzebnego chaosu i zamieszania. Incydent może mieć różne oblicza – od włamania na skrzynkę aż po zaszyfrowanie danych organizacji. Plan działania powinien być możliwe ogólny, a do jego każdego elementu powinna być przypisana konkretna osoba, odpowiedzialna za daną część działań. Pozwoli to na sprawne działanie, komunikację i szybką reakcję.

Plan działania po diagnozie

Po przeprowadzonej diagnozie zapewne uwypuklone zostaną słabe punkty i białe plamy na mapie wiedzy organizacji. Problematyczne kwestie należy omówić z osobami zarządzającymi organizacją w celu wyeliminowania luk. Można to zrobić w następujący sposób:

- Spis problemów – od najbardziej palących aż po kwestie kosmetyczne;
- Rozpisanie możliwych rozwiązań – w jaki sposób można brakującą wiedzę uzupełnić, ewentualnie po czyją wiedzę/usługi sięgnąć oraz jakimi problemami zająć się w pierwszej kolejności;
- Planowanie – w jaki sposób zapobiegać powstawaniu białych plam w przyszłości;
    - Kogo oddelegować do zajmowania się sprawami IT w organizacji
    - W jaki sposób zbierać informacje o posiadanej infrastrukturze i dostępach
    - Kto powinien, a kto nie powinien mieć dostępu do konkretnych usług/zasobów
- Stworzenie dokumentu, określającego daty wdrożenia nowych, wyklarowanych w ramach przeglądu rozwiązań – stanowić będzie motywator, określi też ramy czasowe i osoby odpowiedzialne za konkretne zadania.
- Lista potencjalnych polityk bezpieczeństwa, np.
    - Polityka dotycząca sposobu logowania do poczty (hasła, uwierzytelnianie dwuskładnikowe, przekazywanie poczty)
    - Polityka wymiany dokumentów służbowych i udostępniania ich poza organizację
    - Polityka dotycząca onboardingu nowych pracowników (spis otrzymanego sprzętu, dostępów, szkolenie)
    - Polityka dotycząca przechowywania i przekazywania danych dostępowych do systemów
    - Polityka reakcji na podejrzane wiadomości/włamania na konta służbowe

Na podstawie nowych praktyk i polityk organizacja może podjąć się stworzenia planu reakcji na incydent. Pomoże w tym nowo nabyta znajomość stosowanych technologii, a także określenie osób odpowiedzialnych za IT, które – jako najbardziej doświadczone w organizacji – będą potrafiły w odpowiedni sposób zachować się w przypadku incydentu. Nie musi być to szczegółowy plan

działań; wystarczy szkielet, wskazujący na osoby odpowiedzialne i priorytetowe działania, które należałoby podjąć w danych przypadkach. W trakcie uzupełniania wiedzy w przyszłości (przy implementacji kolejnych rozwiązań IT) taki szkielet można uzupełniać o konkretne przykłady działania w nowych warunkach. Poniżej przedstawiono przykładowy plan działania w przypadku włamania na skrzynkę pocztową:

W przypadku wykrycia włamania na skrzynkę pocztową użytkownika, należy:

1. *W pierwszej kolejności zmienić hasło do skrzynki użytkownika, wykorzystując panel administratora. Osobą odpowiedzialną za konta pocztowe w organizacji jest Jan Kowalski (nr tel: 111-222-333);*
2. *Z poziomu administratora lub konta użytkownika, wymusić usunięcie sesji ze wszystkich zalogowanych urządzeń;*
3. *Przejrzeć działania intruza na rzeczonej skrzynce (email forwarding, ustawienia reguł wiadomości, wysłane wiadomości, miejsca logowania);*
4. *Każdą informację nt włamania należy zapisać, aby w dalszej części móc ustalić przebieg incydentu;*
5. *Ustalić, czy logi i powzięte informacje pozwalają na stwierdzenie wyprowadzenia danych ze skrzynki pocztowej;*
6. *W przypadku wysyłki spamu/wiadomości podszywających się przez intruza w imieniu właściciela skrzynki, określić adresatów wiadomości i niezwłocznie poinformować o incydencie w celu redukcji rozprzestrzeniania się malware/wiadomości phishingowych/wyłudzeń;*
7. *Przeprowadzić analizę wektora ataku w celu wyłonienia innych potencjalnych ofiar wewnątrz organizacji;*
8. *Komunikacja wewnętrzna z pracownikami w celu uczulenia na potencjalne ataki;*
9. *Wprowadzić odpowiednie metody zabezpieczające (2FA, odpowiednie hasło) na skrzynce;*

10. *Opcjonalnie: przeprowadzić szkolenie na bazie powyższego przykładu w celu wzmocnienia świadomości pracowników na temat zagrożeń cyber.*

Dobrym pomysłem byłoby również wytworzenie procedury onboardingu nowych pracowników – wdrożenia ich w wykorzystywane środowisko, przeszkolenia z zagrożeń/problemów, które mogą wystąpić w celu uniknięcia wspomnianego wcześniej zjawiska *shadow IT* (użytkownicy nierzadko przychodzą do organizacji ze swoimi przyzwyczajeniami, które – mocno zakorzenione – mogą ich prowadzić do wykorzystania rozwiązań nienadzorowanych przez organizację). Regularne szkolenia z bezpieczeństwa komputerowego (nawet w formie krótkich przykładów-anegdot) mogą podnosić czujność pracowników, a co za tym idzie, zwiększać odporność całej organizacji.

W ramach diagnozy może okazać się, że wykorzystywane technologie i usługi nie spełniają swojej roli w organizacji. Przykładem może być poczta, która sprawia dużo problemów albo wymiana plików przez udział sieciowy, co eliminuje pracę zdalną (aby dostać się do plików należy pracować z sieci lokalnej, a brak jest rozwiązań typu VPN). Może być to przyczynek do rozmów nad migracją do usług bardziej elastycznych i bezpieczniejszych. Ignorowanie postulatów użytkowników może skutkować wykorzystaniem prywatnych zasobów (poczty, dysków chmurowych) do wymiany plików i wiadomości służbowych.

Glosariusz

- **Urządzenia sieciowe** – zespół urządzeń, łączących urządzenia końcowe (komputery, telefony, drukarki). Pozwalają na przesyłanie danych przez sieć, tj. odpowiednio kierują ruchem w sieci wewnętrznej (LAN) i pozwalają na połączenie z siecią zewnętrzną (WAN). Przez zespół urządzeń rozumieć należy np. routery, przełączniki (switche) czy access pointy (punkty dostępowe, pozwalające na połączenie bezprzewodowe). Urządzenia sieciowe nie są „widoczne” dla użytkownika, jednak ich poprawna konfiguracja wpływa bezpośrednio na jakość i bezpieczeństwo połączenia pracowników z siecią Internet.

- **Dostęp „z miasta”** (*public internet access*)– dostęp do sieci wewnętrznej organizacji (LAN) z sieci zewnętrznej („z miasta”). Terminem tym określa się połączenie np. poprzez tunel VPN, który – odpowiednio skonfigurowany – pozwala na dostęp do zasobów wewnątrz organizacji (np. serwerów plików, pulpitów zdalnych). Może być to również wystawiony publicznie panel logowania do zasobów wewnętrznych
- **VPN (*virtual private network*)** – tunel, kierujący ruch od nadawcy do odbiorcy za pośrednictwem publicznej sieci. Jest to swoistego rodzaju prywatny kanał komunikacji uprawnionego urządzenia z konkretną siecią wewnętrzną. Służyć może np. do zdalnego dostępu do urządzeń sieciowych przez administratorów czy zdalnego dostępu do plików, znajdujących się na serwerze w sieci wewnętrznej organizacji. Zastosowań VPN jest wiele; komercyjnie używa się go do ukrycia ruchu sieciowego przed dostawcą połączenia Internetowego czy administratorem sieci.
- **Firewall** – zapora między siecią wewnętrzną (LAN) i zewnętrzną (WAN). Przybiera formę fizycznego urządzenia (jako część urządzeń sieciowych) lub oprogramowania, zainstalowanego na jednym z urządzeń sieciowych. Jej zadaniem jest filtrowanie pakietów danych w czasie rzeczywistym i zabezpieczanie wymiany danych między użytkownikami a siecią Internet. Bardziej zaawansowane firewalle stanowią część systemu IDS (*intrusion detection system*).
- **VLAN (*virtual local area network*)** – sieć wewnętrzna, wydzielona w ramach jednej fizycznej sieci wewnętrznej. Przykładem może być osobna sieć gościnna, sieć dla pracowników i sieć dla księgowości; pierwsza grupa nie będzie widzieć żadnych urządzeń wewnątrz sieci, ponieważ interesuje ją wyłącznie połączenie z internetem, druga widzieć będzie np. drukarki i udziały sieciowe, natomiast trzecia zobaczy drukarki, udziały sieciowe i będzie miała również dostęp do serwerów, na których działają bazy i programy sieciowe.
- **Oprogramowanie on-premises** – oprogramowanie instalowane i uruchamiane lokalnie, tj. w sieci i na urządzeniach należących do organizacji. Za instalację, aktualizację i rozwiązywanie problemów w takim środowisku w pełni odpowiada organizacja. W dużym skrócie – jest to przeciwieństwo usług chmurowych.

- **Serwer plików** – odpowiednio skonfigurowany serwer lub urządzenie typu NAS, udostępniające w sieci wewnętrznej swoje zasoby. Może służyć do przechowywania danych (plików, folderów) organizacji.
- **Kopia bezpieczeństwa (*backup*)** – kopia zapasowa, stosowana w celu zabezpieczenia przed utratą danych. Wykonuje się ją zwyczajowo na nośnik zewnętrzny lub do miejsca, niepowiązanego ze źródłem.
- **Firmware** – oprogramowanie sprzętowe, zainstalowane na stałe w urządzeniu, służące podtrzymaniu i właściwemu działaniu urządzenia.
- **Cloud (*chmura*)** – usługa dzierżawienia pewnych zasobów, udostępnianych przez usługodawcę. W tym modelu użytkownik nie jest odpowiedzialny za infrastrukturę; interesuje go wyłącznie sama usługa oraz jej ewentualna konfiguracja/dopasowanie. Model ten działa w oparciu o licencjonowanie na dany okres. Dobrym przykładem jest *cloud storage* czyli przechowywanie plików w chmurze – usługodawca odpowiedzialny jest za bezproblemowe działanie i ciągłość usługi, a użytkownik nie przejmuje się kwestiami związanymi z aktualizacją i utrzymaniem infrastruktury.
- Mechanizmy zabezpieczające pocztę
    - **SPF (*sender policy framework*)** – mechanizm, pozwalający właścicielowi domeny na zdefiniowanie uprawnionych do wysyłki adresów IP. W rezultacie wyłącznie określone we wpisie adresy będą przez inne serwery pocztowe uznawane za wiarygodne w przypadku wysyłki wiadomości email z naszej domeny.
    - **DKIM (*domain keys identified mail*)** – mechanizm, utrudniający podszywanie się pod nadawcę wiadomości email. Działa poprzez dodanie do wiadomości podpisu, który zweryfikowany może zostać przez serwer odbiorcy.
    - **DMARC (*domain-based message authentication, reporting & conformance*)** – zestaw reguł, bazujący na dwóch wcześniejszych mechanizmach. Na ich podstawie może zdecydować, czy wiadomość przyszła od zweryfikowanego dostawcy, a jeżeli nie – co z nią zrobić.

- **DNS (*domain name system*)** – wysokopoziomowo rozumiany rozproszony system nazw sieciowych, który służy m.in. rozwijaniu zapytań o nazwy domen internetowych. Od strony organizacji, DNS możemy rozumieć jako strefy w hostingu, przypisane do obsługiwanej domeny, pozwalające na określenie odpowiedniej komunikacji między serwerami i klientami (komputerami użytkowników). DNS jest systemem nieodzownym do działania wielu usług Internetowych.
- **Domena** – ciąg identyfikacyjny systemu DNS, określający zakres panowania nad danym adresem. Składa się najczęściej z domeny najwyższego poziomu (.net, .org, .com) oraz poprzedzającej ją nazwy (google.com, onet.pl, wikipedia.org). Przez domenę w kontekście niniejszego dokumentu rozumieć będziemy przede wszystkim wykorzystywany na stronie WWW i poczcie adres, np. techsoup.pl.
- **Klient pocztowy** – program, służący do obsługi kont pocztowych różnego rodzaju.
- **CMS (*content management system*)** – oprogramowanie służące do łatwego zarządzania i wprowadzania zawartości na strony internetowe WWW (np. Wordpress, Drupal, Joomla)
- **Szyfrowanie** – zbiór technik kryptograficznych, mających za zadanie zabezpieczyć dane i zachować ich poufność. Szyfrowanie obecne jest w wielu usługach sieciowych.
- **Urządzenia końcowe** – urządzenia wykonujące pracę bezpośrednio dla użytkownika (telefony, komputery, drukarki).
- **MDM (*mobile device management*)** – oprogramowanie służące do monitorowania, zarządzania i zabezpieczania urządzeń końcowych użytkowników.
- **Uwierzytelnianie dwuskładnikowe (*2FA, two-factor authentication*)** – sposób logowania do usług, wymagający dwóch składników logowania, np. hasła i kodu z aplikacji/kodu z SMS/fizycznego klucza bezpieczeństwa.
- **Klucz bezpieczeństwa** – fizyczne urządzenie, najczęściej działające przy użyciu portu USB-A/USB-C/Lightning oraz komunikacji bezprzewodowej NFC. Służy jako drugi składnik uwierzytelniania dwuskładnikowego (może być również wykorzystywane do logowania bez wykorzystania hasła, tzw. *passwordless*). Na kluczu wykonywane są pewne obliczenia kryptograficzne, które sprawdzają poprawność danych logowania na linii klient-usługa.

- **Menedżer haseł** – oprogramowanie, mające za zadanie przechowywanie haseł użytkownika w scentralizowanej bazie, zabezpieczonej hasłem głównym (tzw. *master password*). Pozwala na przechowywanie haseł, generowanie skomplikowanych haseł czy podpowiadanie zapisanych danych logowania na prawdziwych stronach. Na rynku dostępne są rozwiązania, przechowujące hasła lokalnie na urządzeniu użytkownika (KeePass) albo w chmurze (modele subskrypcyjne oraz darmowe, mające pewne ograniczenia).
- **Antywirus** – oprogramowanie, analizujące pliki i – w niektórych przypadkach – ruch sieciowy w poszukiwaniu złośliwego oprogramowania. Zabezpiecza użytkownika przed pobraniem lub uruchomieniem różnego rodzaju złośliwego oprogramowania (*malware*) przy wykorzystaniu zebranej bazy danych (haszy, plików binarnych, nazw, adresów).
- **Shadow IT** – różnego rodzaju wdrożone poza systemem i wiedzą zespołu IT rozwiązania, mające za zadanie wykonywanie pracy w środowisku niekontrolowanym przez wspomniany zespół. Objawia się przede wszystkim wykorzystaniem innego od zalecanego wewnątrz organizacji oprogramowania w celu ominięcia blokad i ograniczeń, nałożonych przez administratora.
- **Zagrożenia cyber** – wszelkiego rodzaju złośliwe i szkodliwe dla bezpieczeństwa sieci, urządzeń końcowych i danych użytkownika działania, mające charakter najczęściej przestępczy (rzadziej występujące w formie żartu). Najczęstsze przypadki dotyczą wyłudzenia danych i pieniędzy, infekcji urządzenia w celu kradzieży danych, przejęcie urządzenia, zaszyfrowanie infrastruktury w celu wymuszenia okupu itp.
- **Incydent** – nieplanowane i nieoczekiwane zdarzenie, mające wpływ na prawidłowe działanie systemów organizacji i bezpieczeństwo danych. Incydentem może być zarówno włamanie do skrzynki użytkownika i rozsyłanie spamu, jak i włamanie do infrastruktury organizacji w celu kradzieży danych i ich zaszyfrowania.
- **IoC (*indicator of compromise)*** – zbiór dowodów i poszlak, świadczących o wystąpieniu incydentu bezpieczeństwa.

➔ **Logi** – różnego rodzaju informacje dot. aktywności systemu informatycznego, mogące służyć prześledzeniu działania usługi, logowania użytkowników czy nieautoryzowanego działania wewnątrz.

Przydatne linki i źródła (wersja polska):

Proces wzmacniania bezpieczeństwa informatycznego organizacji ma charakter ciągły. Zmieniające się technologie, a także coraz bardziej wysublimowane metody działania cyberprzestępców wymagają regularnej aktualizacji wiedzy. Pomocne mogą okazać się źródła, na bieżąco informujące o popularnych atakach, lukach w systemach oraz wyciekach. Poniżej znaleźć można kilka odnośników do rzetelnych i aktualnych źródeł informacji na temat bezpieczeństwa informatycznego.

- HaveIBeenPwned
  https://haveibeenpwned.com/
- NASK (Naukowa i Akademicka Sieć Komputerowa)
  https://www.nask.pl/
- Portal „Zaufana Trzecia Strona”
  https://zaufanatrzeciastrona.pl/
- CERT Polska (Zespół Reagowania na Incydenty Komputerowe)
  https://twitter.com/CERT_Polska
  https://bezpiecznapoczta.cert.pl/
- Sekurak
  https://sekurak.pl/
- „Informatyk Zakładowy”
  https://twitter.com/InfZakladowy

- Portal „Niebezpiecznik”
  https://niebezpiecznik.pl/
- Bleeping Computer
  https://www.bleepingcomputer.com/
- The Hacker News
  https://thehackernews.com/
- National Cyber Security Centre UK
  https://www.ncsc.gov.uk/section/advice-guidance/all-topics
- WeLiveSecurity by ESET
  https://www.welivesecurity.com/en/
- Computer World
  https://www.computerworld.com/category/emerging-technology/
- The DFIR Report
  https://thedfirreport.com/
- Microsoft Threat Intelligence
  https://www.microsoft.com/en-us/security/blog/topic/threat-intelligence/?sort-by=newest-oldest&date=any
- Mandiant
  https://twitter.com/Mandiant
- Zero Security
  https://zerosecurity.org/
- Symantec
  https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence
- NSA
  https://www.nsa.gov/
    - CYWARE
      https://cyware.com/cyber-security-news-articles

- DarkReading
  https://www.darkreading.com/
- ENISA (European Union Agency for Cybersecurity)
  https://www.enisa.europa.eu/news
- Infosecurity Magazine
  https://www.infosecurity-magazine.com/
- Tech Crunch
  https://techcrunch.com/