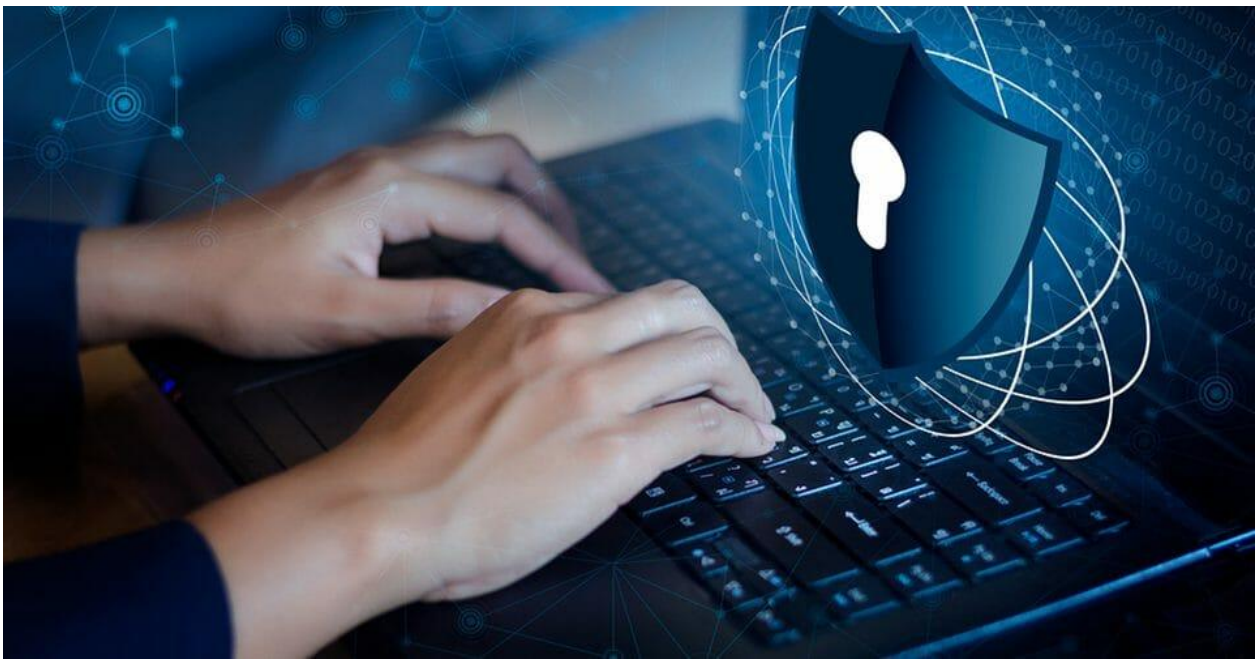
ZALECENIA W ZAKRESIE CYBERBEZPIECZEŃSTWA

dla użytkowników systemów hybrydowych wykorzystujących komponenty chmury publicznej Microsoft



Warszawa, 2023

Spis treści

Podstawowe zalecenia cyberbezpieczeństwa dla użytkowników systemów hybrydowych, wykorzystujących komponenty chmury publicznej Microsoft

Celem dokumentu jest dostarczenie informacji umożliwiających podejmowanie odpowiednich decyzji dotyczących bezpieczeństwa przy posługiwaniu się technologiami informatycznymi w pracy, a w szczególności w przypadku wykorzystywania systemów hybrydowych opartych na komponentach chmury publicznej Microsoft.

Zalecenia dotyczą zarówno obszaru organizacyjnego, jak i wykorzystania konkretnych narzędzi bezpieczeństwa, zarówno dla systemów własnych jak i hybrydowych.

Zastosowanie poniższych zaleceń jednorazowo – mija się z celem. Bezpieczeństwo jest ciągłym procesem wymagającym monitorowania, okresowych przeglądów procesów i stanu systemów, wprowadzania nowych narzędzi i modyfikacji polityk bezpieczeństwa.

Z uwagi na dynamiczne zmiany prawa w tym zakresie (NIS-2, KSC) zaleca się stałe monitorowanie zmian i dokonywanie modyfikacji wdrażanych zaleceń.

Paweł Walczak

1. Definicja cyberbezpieczeństwa.

Przez cyberbezpieczeństwo rozumie się zapewnienie ochrony przed atakami, uszkodzeniami lub nieautoryzowanym dostępem. Cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Aby zapewnić zasady bezpieczeństwa należy zachować:

a) Poufności informacji, czyli uniemożliwienie dostępu do danych osobom trzecim,
b) Integralności informacji, czyli uniknięcie nieautoryzowanych zmian w danych,
c) Dostępności informacji, czyli zapewnienie dostępu do danych gdy są one niezbędne uprawnionym użytkownikom i nie udzielanie dostępu, gdy nie jest on potrzebny,

d) Rozliczalności wykonywanych operacji, czyli zapewnienie przechowywania pełnej historii dostępu do danych, wraz z informacją kto taki dostęp uzyskał.

Każdy pracownik zobowiązany jest do przestrzegania zasad cyberbezpieczeństwa, co warunkuje dostęp do zasobów i danych w miejscu pracy oraz pracy zdalnej – z dowolnego miejsca.

2. Zasady kreowania i wdrażania polityk bezpieczeństwa

Niniejszy dokument jest wstępnym zbiorem zasad cyberbezpieczeństwa i wymaga dostosowania do konkretnych warunków w jednostce. Należy pamiętać, że polityki bezpieczeństwa muszą się ustawicznie zmieniać, podążając za zmianami w systemach teleinformatycznych, procesach biznesowych oraz zewnętrznych i wewnętrznych zagrożeniach. W związku z tym, powinny być one rewidowane i uaktualniane:

1. Co najmniej raz do roku lub inaczej jeżeli wynika to z już przyjętej polityki bezpieczeństwa,
2. Przy każdej znaczącej zmianie technologicznej, procesowej i organizacyjnej.

2.1. Przeprowadzenie analizy ryzyka

Przed wdrożeniem polityk bezpieczeństwa należy przeprowadzić analizę ryzyka, składającej się przynajmniej z następujących kroków:

1. Wykonanie audytu bieżącego stanu systemów informacyjnych w oparciu o uznane metodyki,[1]
2. Zapoznanie się z rekomendacjami w zakresie cyberbezpieczeństwa producentów sprzętu, oprogramowania i systemów teleinformatycznych,
3. Identyfikacja i oszacowanie wpływu komponentów systemów na ciągłość działania organizacji i jej usług,
4. Ustalenie metryk poprawnego stanu bezpieczeństwa.

2.2. Wdrażanie polityk cyberbezpieczeństwa

Wdrażając lub aktualizując polityki bezpieczeństwa należy:

[1] Proponowane metodyki w załączniku nr. 1

1. Zidentyfikować wszystkie źródła informacji w jednostce i dokonać ich klasyfikacji na przynajmniej pięć poziomów – od najmniej istotnych do najbardziej istotnych ze względu na bezpieczeństwo funkcjonowania organizacji i jej pracowników oraz klientów:
    a. Dane publiczne,
    b. Dane zastrzeżone dla pracowników i upoważnionych użytkowników zewnętrznych,
    c. Dane zawierające dane osobowe,
    d. Dane objęte tajemnicą przedsiębiorstwa,
    e. Dane niejawne.
2. Zidentyfikować zewnętrzne źródła danych i ocenić stan bezpieczeństwa korzystania z nich.
3. Ustalić w jakich procesach wykorzystywane są zidentyfikowane zbiory danych.
4. Zidentyfikować systemy w jednostce i sprawdzić ich stan zabezpieczeń (wdrożone narzędzia ochrony przed atakami, stan techniczny, dostępność wsparcia technicznego, aktualność oprogramowania – szczególnie w zakresie poprawek bezpieczeństwa).
5. Zidentyfikować systemy zewnętrzne, z którymi współpracują systemy organizacji,
6. Przeprowadzić kontrolę zarządzania tożsamością użytkowników w zakresie:
    a. Czy posługujemy się jednolitą tożsamością użytkownika, czy też użytkownik ma kilka tożsamości cyfrowych,
    b. Czy utworzono prawidłowo grupy użytkowników opierając się na ich rolach w organizacji,
    c. Jakie są poziomy uprawnień dla użytkowników, ich grup i usług (jakie poziomy uprawnień istnieją i jakie są zasady ich przyznawania),
    d. Czy wszystkie usługi w organizacji wymagają uwierzytelnienia i na jakim poziomie,
    e. Czy wprowadzone mechanizmy uwierzytelniania użytkowników zapewniają:
        i. Niezaprzeczalność uwierzytelnienia, czyli każdorazową identyfikację użytkownika,
        ii. Poufności informacji, czyli uniemożliwienie dostępu do danych osobom trzecim,

iii. Rozliczalności wykonywanych operacji, czyli zapewnienie przechowywania pełnej historii dostępu do danych, wraz z informacją kto taki dostęp uzyskał,
iv. Nadawanie i usuwanie uprawnień użytkowników i ich grup w zależności od ich aktualnej roli w organizacji.

7. Wdrożyć i zweryfikować działanie systemów zarządzania bezpieczeństwem oraz monitoringu systemów i użytkowników, wraz z raportowaniem.
8. Wdrożyć adekwatne do potrzeb narzędzia i procedury ochrony przed atakami.
9. Stworzyć listę działań naprawczych dla wykrytych nieprawidłowości lub podatności, podzielić je pod względem krytyczności dla funkcjonowania organizacji. Wyznaczyć harmonogram korygowania nieprawidłowości i usuwania podatności, a następnie wdrożyć je.
10. Stworzyć i aktualizować listę aktów prawnych i regulacji wewnętrznych dotyczących bezpieczeństwa informacji.[2]
11. Stworzyć listę norm i certyfikacji, posiadanych i mogących mieć zastosowanie w ochronie informacji w organizacji,
12. Stworzyć listę ról i osób odpowiedzialnych za wdrożenie, utrzymanie, aktualizację i audyt polityk bezpieczeństwa.
13. Ustalić role i procesy odpowiedzialne za utrzymanie i audyty bezpieczeństwa technicznego systemów.
14. Ustalić procedury zgłaszania incydentów cyberbezpieczeństwa przez pracowników.
15. Ustalić procedury zgłaszania incydentów cyberbezpieczeństwa przez organizację do właściwego CSIRT.[3]
16. Opracowanie planu wdrożenia i utrzymania polityk bezpieczeństwa wraz komunikacją dla wszystkich pracowników organizacji.
17. Przygotowanie i przeprowadzanie cyklicznych szkoleń z zakresu cyberbezpieczeństwa dla pracowników.

[2] Lista aktów prawnych w załączniku nr. 2
[3] Procedura zgłaszania incydentów do CSIRT – Załącznik nr. 3

18. Stworzyć raporty z wszystkich wymienionych czynności dla kierownictwa organizacji i dla celów audytowych.

3. Realizacja polityk bezpieczeństwa

Bezpieczeństwo w systemach teleinformatycznych należy traktować zawsze jako ciągły proces uzupełniony odpowiednimi narzędziami, procedurami i kompetencjami.

3.1. Zasada „Zero zaufania”

Zerowe zaufanie (Zero Trust) to proaktywne, zintegrowane podejście do bezpieczeństwa na wszystkich warstwach zasobów cyfrowych, które stale weryfikuje każde działanie, redukuje uprawnienia do niezbędnych i opiera się na zaawansowanej analizie, wykrywaniu i reagowaniu w czasie rzeczywistym na zagrożenia.

Konieczność stosowania zasady Zero zaufania wynika z tego, że:

1. Bezpieczeństwo IT jest złożone - wiele urządzeń, użytkowników, procesów i połączeń – każdy z tych elementów jest potencjalnym przedmiotem ataku.
2. Stosowana uprzednio strategia bezpieczeństwa "Zaufana sieć" była adekwatna do typowych ataków skupionych na sieci. Prosta i ekonomiczna ochrona przed nimi okazała się zawodna wobec obecnie stosowanych wektorów ataku.
3. Zasoby coraz częściej opuszczają sieć, zgodnie z zasadami mobilności BYOD (Bring your own Device), WFH (work from home) i stosowania rozwiązań z chmury.
4. Atakujący przeszli na ataki tożsamości oparte o wyłudzanie informacji i kradzież danych uwierzytelniających.
5. Mnogość istniejących wektorów ataku powoduje, że praktycznie każdy element techniczny, organizacyjny czy ludzki jest zagrożony.
6. Zespoły ds. bezpieczeństwa są często przeciążone i nieskuteczne.

Strategia zwiększania bezpieczeństwa obowiązuje dla wszystkich użytkowników, zasobów i aplikacji - wszędzie, w tym w własnych, sieciach publicznych i niezaufanych.

Wynikają z tego następujące zasady:

1. Egzekwowanie niezaprzeczalnej weryfikacji,

2. Udzielanie dostępu z jak najmniejszymi uprawnieniami, a w przypadku kont uprzywilejowanych – tylko na przyjęty okres czasu,
3. Przyjęcie założenia, że naruszenia bezpieczeństwa wystąpią.

3.2. Podstawowe wymagania bezpieczeństwa

Realizacja wymagań prawnych w zakresie bezpieczeństwa, w tym uwierzytelniania, niezaprzeczalności działań oraz monitorowania następuje poprzez:

1. Przyjęcie jako priorytetu ochrony tożsamości cyfrowej użytkowników systemów.
2. Wdrożenie i pielęgnację usług katalogowych lub mechanizmów zarządzania tożsamością obejmujących wszystkich użytkowników systemów danego podmiotu. Zaleca się wykorzystanie, niezależnej od wewnętrznej, usługi katalogowej dla użytkowników zewnętrznych.
3. Tam, gdzie jest to możliwe, korzystanie usługi katalogowej jako podstawy uwierzytelnienia i nadawania uprawnień do wszystkich systemów teleinformatycznych danego podmiotu z wprowadzeniem mechanizmu pojedynczego logowania (single sign-on).
4. Tam, gdzie nie jest możliwa realizacja globalnego mechanizmu single sign-on, należy objąć bazy tożsamości użytkowników w poszczególnych systemach jednym wspólnym systemem zarządzania tożsamością.
5. Nadawanie uprawnień dostępu do danych i usług ról i grup ról, a nie dla użytkowników i ich grup.
6. Wykorzystanie uwierzytelnienia wieloskładnikowego dla dostępu do danych wrażliwych oraz w przypadku uwierzytelniania spoza chronionych sieci wewnętrznych.
7. W każdym przypadku rozdzielenie funkcji kont administratorskich i kont użytkownika systemów oraz izolacja tych typów kont.
8. Wdrożenie mechanizmów wymuszających zmianę haseł użytkowników lub odnawiania certyfikatów w zgodzie z zapisami polityk bezpieczeństwa.
9. Wdrożenie mechanizmów samoobsługi użytkownika w przypadku konieczności zmiany lub utraty poświadczeń do systemu.

10. Przygotowanie bezpiecznych środowisk klienckich poprzez przygotowywanie sprawdzonych, testowanych i monitorowanych „obrazów" oprogramowania, zawierających system operacyjny wraz z kompletem aplikacji niezbędnych dla danej grupy użytkowników, systemy firewall i antywirusowy, oraz narzędzia pozwalające na:
    i. monitorowanie stanu sprzętu i jego inwentaryzację,
    ii. monitorowanie działania oprogramowania i jego inwentaryzację,
    iii. zarządzanie konfiguracją środowisk klienckich,
    iv. udostępnienie możliwości instalacji przez użytkownika tylko wybranych aplikacji pozwalających na realizację jego zadań.
11. Przygotowanie schematów implementacji środowisk serwerowych pozwalających na ich monitorowanie i zarządzanie.
12. Wprowadzenie spójnych mechanizmów klasyfikacji informacji i danych.
13. Wprowadzenie mechanizmów wymuszających szyfrowanie plików zawierających informację wrażliwą wraz z mechanizmami gwarantującymi niezaprzeczalność dostępu do nich.
14. Wprowadzenie mechanizmów wymuszających szyfrowanie zasobów dyskowych i nośników zawierających informację wrażliwą, które mogą być wynoszone poza teren organizacji wraz z mechanizmami gwarantującymi niezaprzeczalność dostępu do nich.
15. Przeprowadzanie regularnych (przynajmniej raz do roku lub zgodnie z przyjętą polityką bezpieczeństwa) audytów wewnętrznych i zewnętrznych - oparcie się o audyty niezależnych, uznanych firm, szczególnie w przypadku wykorzystywania usług chmury publicznej.

3.3. Obowiązujące zasady bezpieczeństwa

3.3.1. Zasada minimalnych uprawnień

W ramach nadawania uprawnień do danych przetwarzanych w systemach IT organizacji należy stosować zasadę „minimalnych uprawnień", to znaczy przydzielać minimalne uprawnienia, które są konieczne do wykonywania pracy na danym stanowisku.

Przykładowo: pracując na komputerze PC każdy pracownik powinien posiadać tylko takie uprawnienia jakie są wymagane do realizacji swoich obowiązków (a nie na przykład uprawnienia administracyjne lub przydzielanie uprawnień administracyjnych domyślnie).

3.3.2. Zasada wielowarstwowych zabezpieczeń

System IT organizacji powinien być chroniony równolegle na wielu poziomach. Zapewnia to pełniejszą oraz skuteczniejszą ochronę danych.

Przykładowo: w celu ochrony przed wirusami stosuje się równolegle wiele technik: oprogramowanie antywirusowe, systemy typu firewall, odpowiednią konfigurację systemu aktualizacji Windows.

3.3.3. Zasada ograniczania dostępu

Domyślnymi uprawnieniami w systemach IT powinno być zabronienie dostępu. Dopiero w przypadku zaistnienia odpowiedniej potrzeby, administrator IT przyznaje stosowne uprawnienia.

Przykładowo: domyślnie dostęp do bazy przechowującej dane klientów jest zabroniony. Stosowny dostęp zostaje przyznany osobie, której zajmowane stanowisko wiąże się z koniecznością pracy w tego typu systemie.

3.3.4. Dostęp do danych poufnych na stacjach PC.

- Dostęp do danych poufnych w LAN realizowany jest na przeznaczonych do tego serwerach.
- Dostęp do danych poufnych (udany lub nieudany) na serwerach jest odnotowywany. Lista systemów objętych tego typu działaniami dostępna jest w osobnym dokumencie.
- Jeśli stacja PC jest komputerem przenośnym (laptopem) to musi ona być dodatkowo zabezpieczona (np. z wykorzystaniem szyfrowania dysku twardego – FDE).
- Dostęp do danych poufnych z zewnątrz firmy powinien odbywać się z wykorzystaniem kanału szyfrowanego (np. VPN, dostęp do e-mail poprzez protokół szyfrowany).
- Dostęp do danych poufnych poprzez firmową sieć WiFi powinien odbywać się z wykorzystaniem kanału szyfrowanego (np. VPN).

3.3.5. Zabezpieczenie stacji roboczych

Stacje robocze powinny być zabezpieczone przed nieautoryzowanych dostępem osób trzecich. Minimalne środki ochrony to:

- zapewnienie automatycznego połączenia stacji do systemów organizacji za pomocą VPN przy starcie systemu,
- zainstalowane na stacjach systemy typu: firewall oraz antywirus,
- wdrożony system aktualizacji systemu operacyjnego oraz jego składników,
- wymaganie podania hasła przed uzyskaniem dostępu do stacji,
- niepozostawianie niezablokowanych stacji PC bez nadzoru,
- bieżąca praca z wykorzystaniem konta nieposiadającego uprawnień administracyjnych.

Wymagana jest ocena bezpieczeństwa stacji przy pomocy Secure Score zawartego w pakiecie Microsoft Defender for Endpoint (lub odpowiednikiem). Mechanizm ten pozwala ocenić, czy podstawowe elementy ochrony urządzenia są zaimplementowane i działają poprawnie, dając w skali punktowej wynik dla każdej z zdefiniowanych metryk. Jednocześnie rekomendowane są podstawowe działania podwyższające wynik dla urządzenia, takie jak:

- zainstalowane aktualne poprawki bezpieczeństwa dla systemu operacyjnego – do 72 pkt;
- włączone mechanizmy Exploit Guard – do 33 pkt;
- zdefiniowane foldery dla działania Exploit Guard – do 32 pkt;
- skonfigurowane raporty i akcje systemu antywirusowego – do 19 pkt;
- włączony Credential Guard – do 17 pkt;
- włączona ochrona BitLocker – do 17 pkt;
- szyfrowanie dysków – do 8 pkt;
- skonfigurowany mechanizm Windows Hello – do 7 pkt

Szczegółowe informacje dotyczące korzystania ze stacji roboczych można znaleźć w stosownym dokumencie.

3.3.6. Klasyfikacja stacji roboczych

Podział na grupy bezpieczeństwa urządzeń końcowych wygląda następująco:

Dla typowych stacji roboczych

- Poziom 5 – poziom podstawowy – określony jako minimalne wymagania bezpieczeństwa dla wszystkich urządzeń.
- Poziom 4 – poziom podstawowy podwyższony – dla stacji roboczych których użytkownicy mają dostęp do danych wrażliwych.
- Poziom 3 – poziom wysoki – dla urządzeń wykorzystywanych przez użytkowników mających dostęp do danych mających krytyczny wpływ na działanie organizacji, na przykład objętych tajemnicą przedsiębiorstwa.

Dla stacji z uprzywilejowanym dostępem

- Poziom 2- poziom uprzywilejowany podstawowy – dla urządzeń wykorzystywanych przez programistów czy testerów stanowiących atrakcyjny cel ataków.
- Poziom 1 – poziom uprzywilejowany wysoki – dla urządzeń wykorzystywanych przez administratorów systemów, w szczególności, gdy ich uprawnienia nie mają ograniczeń czasowych i zakresu uprawnionych działań.

3.3.7. Wykorzystanie haseł

1. Hasła powinny być okresowo zmieniane – zgodnie z przyjętą polityką bezpieczeństwa lub minimalnie raz w roku.
2. Hasła nie mogą być przechowywane w formie otwartej (nie zaszyfrowanej).
3. Hasła nie powinny być łatwe do odgadnięcia, to znaczy:
4. powinny składać się z minimum 10 znaków, w tym jeden znak specjalny i jedna cyfra, nie mogą przybierać prostych form, np. 123456789, stanislaw, dom99, haslo, Magda8, itp.
5. Hasła mogą być tworzone według łączenia „losowych” (tj nie istniejących w popularnych słownikach) sylab/słów, np,: mal-tra-laza-#topa. W ten sposób można uzyskać długie hasło stosunkowo proste do zapamiętania.

3.3.8. Odpowiedzialność pracowników za dane poufne

Każdy pracownik odpowiada za utrzymanie w tajemnicy danych poufnych, do których dostęp został mu powierzony.

3.3.9. Monitoring bezpieczeństwa

W celu zapewnienia ochrony informacji Zarząd może stosować monitoring wykorzystania firmowej infrastruktury informatycznej, w szczególności obejmujący następujące elementy:

- analiza oprogramowania wykorzystanego na stacjach roboczych,
- analiza stacji roboczych pod względem wykorzystania nielegalnego oprogramowania / plików multimedialnych oraz innych elementów naruszających Prawo Autorskie,
- analiza odwiedzanych stron WWW,
- analiza godzin pracy na stanowiskach komputerowych,
- analiza wszelakich dostępów (autoryzowanych oraz nieautoryzowanych) do systemów IT będących w posiadaniu Firmy,
- analiza ruchu sieciowego pod względem komunikacji, szkodliwej dla bezpieczeństwa danych Firmy.

Monitoring bezpieczeństwa musi odbywać się z zachowaniem obowiązującego prawa.

3.3.10. Zabezpieczenia na poziomie użytkownika

Użytkownik systemu jest zwykle najsłabszym ogniwem w systemie cyberbezpieczeństwa. Konieczne jest wprowadzenie wszystkich wymienionych procedur i mechanizmów ochrony jego tożsamości i środowiska pracy. Kluczowym elementem tych działań są okresowe szkolenia użytkowników, aktualizujące wiedzę o potencjalnych zagrożeniach, wdrożonych politykach bezpieczeństwa i wymaganych scenariuszach zachowań.

Dużym problemem jest wyciek czy nieuprawniony dostęp do informacji w wypadku kradzieży komputerów z dyskami zawierającymi dane lub wynoszenia czy zgubienia pamięci przenośnych, na przykład kluczy USB. W tych przypadkach standardowym działaniem powinno być szyfrowanie danych na dyskach i nośnikach danych. Mechanizm taki powinien umożliwiać centralnie zarządzanie zgodnie z ustalonymi politykami

bezpieczeństwa poprzez Group Policy przez jednoznaczne określenie i wymuszenie konieczności szyfrowania informacji pod rygorem odcięcia dostępu do danych.

3.3.11. Zabezpieczenie danych, a nie tylko miejsca składowania

Zabezpieczanie samych danych umożliwia ich ochronę przed celową lub niecelową działalnością pracowników wynoszących lub udostępniających dane, do których mają dostęp. Konieczne jest zabezpieczanie samych danych niezależnie od miejsca ich przechowywania przy pomocy mechanizmów Rights Management, czyli zarządzania prawami dostępu do informacji wiadomości poczty elektronicznej czy plików.

3.4. Bezpieczeństwo centrum przetwarzania

Zabezpieczenia muszą być wbudowane w kompleksowy projekt Centrum Przetwarzania (CP) zgodnie z zasadą *Security by design* oraz zasadą Zero zaufania. Architekturę i procedury zabezpieczeń należy zaprojektować wraz z całym CP lub każdorazowo w trakcie jego modyfikacji.

1. Priorytetem zachowania bezpieczeństwa CP jest prewencja, obejmująca projekt zabezpieczeń, które przewidują wszelkiego rodzaju znane ataki czy zdarzenia, ale też przewidują ich rozwój i zmiany.
2. Należy zapewnić niezawodną separację danych. Separacja taka polegająca na logicznej izolacji danych poszczególnych użytkowników musi być zagwarantowana mechanizmem niezaprzeczalnego uwierzytelnienia i autoryzacji dostępu do danych. Wdrożenie odpowiednich mechanizmów dostępu do danych powinno łączyć się z ich klasyfikacją i zastosowaniem dla poszczególnych klas danych odpowiednich procedur dostępu. Na przykład, dla danych osobowych, wrażliwych czy objętych tajemnicą przedsiębiorstwa powinien być zastosowany mechanizm uwierzytelnienia wieloskładnikowego.
3. W stosunku do danych składowanych w CP należy zapewnić możliwość szyfrowania danych, przestrzeni dyskowych czy też maszyn wirtualnych.
4. Wymagana jest możliwość szyfrowania danych w trakcie przesyłu – zarówno do i z CP, jak i wewnątrz CP.
5. Wymagane jest wdrożenie mechanizmów zabezpieczających przed utratą danych w CP:

- Nadmiarowość (redundancja) danych - w tym zakresie zalecane jest tworzenie 2-3 kopii danych w jednym CP,
- Dla danych usług kluczowych wymagana jest tzw. georedundancja pozwalająca na tworzenie kopii zapasowych danych (lub całych systemów) w drugim CP oddalonym o kilkadziesiąt do kilkuset kilometrów.

6. Wymagane jest wdrożenie procesu trwałego usuwania lub retencji danych użytkowników po zakończeniu przez nich korzystania z usługi CP, z zaplanowaniem uzgodnionego z użytkownikiem okresu karencji, w czasie którego dane są nadal dla niego dostępne przed ostatecznym ich usunięciem.
7. Wymagane jest wdrożenie procedur upoważnionego dostępu do danych dla pracowników CP. Założeniem podstawowym jest zasada, że administratorzy CP nie mają dostępu do danych użytkowników usług CP. W przypadku, gdy wystąpi konieczność takiego dostępu musi być ona obwarowana szczegółowymi procedurami, wymagającymi sprawnej, wieloetapowej ścieżki akceptacyjnej, zgody uprawnionego reprezentanta użytkownika oraz jasnych zasad – komu, w jakim celu i na jaki okres takie uprawnienia zostały udzielone.
8. Wymagane jest monitorowanie i dokumentowanie wszystkich działań związanych z dostępem do danych.

3.5. Dostęp do sieci wewnętrznych i zewnętrznych

System dostępowy musi zapewnić łatwość obsługi, zaawansowaną ochronę oraz szybki i bezpieczny dostęp do wszystkich typów sieci.

W skład podsystemu musi wejść rozbudowana zapora filtrująca ruch do warstwy aplikacji włącznie. Zapewni ona organizacji podstawową ochronę przed zagrożeniami zarówno zewnętrznymi, jak i wewnętrznymi. Rozwiązanie ma integrować funkcje zapory z architekturą VPN (virtual private network) w postaci dwukierunkowych kanałów do transmisji danych, tworzonych w oparciu o sieć publiczną (Internet). Wirtualne kanały VPN są ustalane wyłącznie na czas transmisji między węzłami sieci stanowiącymi rutery, przez które informacja z sieci prywatnych jest przesyłana w zaszyfrowanej postaci. Rozwiązanie VPN ma zapewnić kontrolę i filtrowanie z pamięcią stanu całego ruchu w kanałach VPN, a także, poprzez współpracę z

usługami katalogowymi, kontrolę dostępu klientów VPN przez mechanizm kwarantanny pozwalające na zabezpieczenie sieci przed atakami zewnętrznymi przeprowadzanymi przez połączenia VPN.

Rozwiązanie ma zapewnić również możliwość pracy w trybie „web cache" buforując strony internetowe i dostarczając je użytkownikom z kopii lokalnej.

Całość podsystemu ma dostarczyć następujące usługi:

- zabezpieczenie i publikacja usług sieci organizacji dostępnych od strony sieci zewnętrznych,
- zapewnienie kontroli nad dostępem użytkowników do sieci Intranet i Internet,
- zapewnienie wydajnego dostępu do zasobów sieci Intranet i Internet.

3.6. Sieć lokalna (LAN).

Sieć lokalna musi być odpowiednio chroniona przed nieuprawnionym dostępem, przykładowo:

- istotne serwery muszą być odseparowywane od sieci klienckich,
- gniazdka sieciowe dostępne publiczne muszą być nieaktywne,
- goście nie mogą uzyskiwać dostępu do sieci LAN.

Szczegółowe informacje dotyczące przyjętych metod ochrony zostały zawarte w osobnej procedurze.

3.7. Systemy IT / serwery

Systemy IT przechowujące dane poufne (np. dane osobowe) muszą być odpowiednio zabezpieczone. W szczególności należy dbać o poufność, integralność i rozliczalność danych przetwarzanych w systemach.

Szczegółowe informacje dotyczące przyjętych metod ochrony zostały zawarte w osobnej procedurze.

3.8. Publiczne udostępnianie infrastruktury IT

Infrastruktura udostępniona publicznie musi być szczególnie zabezpieczona. Przykładowe środki bezpieczeństwa:

- Separacja od sieci LAN (np. z wykorzystaniem strefy DMZ)

- Wykonanie hardeningu systemu (zwiększenia bezpieczeństwa oferowanego domyślne przez system)
- Wewnętrzna lub zewnętrzna weryfikacja bezpieczeństwa systemu (np. poprzez realizację testów penetracyjnych)

3.9. Kopie zapasowe.

Każde istotne dane (w tym dane poufne) powinny być archiwizowane na wypadek awarii w firmowej infrastrukturze IT.

- Nośniki z kopiami zapasowymi powinny być przechowywane w miejscu uniemożliwiającym dostęp osobom nieupoważnionym.
- Okresowo kopie zapasowe muszą być testowane pod względem rzeczywistej możliwości odtworzenia danych.

3.10. Dostęp do systemów IT po rozwiązaniu umowy o pracę

W przypadku rozwiązania umowy o pracę z pracownikiem, dezaktywowane są wszelakie jego dostępy w systemach IT.

3.11. Weryfikacja przestrzegania polityki bezpieczeństwa.

Zarząd okresowo wykonuje wewnętrzny lub zewnętrzny audyt bezpieczeństwa mający na celu wykrycie ewentualnych uchybień w realizacji założeń polityki bezpieczeństwa.

4. Narzędzia ochrony przed atakami dostępne w ofercie Microsoft

4.1. Azure Monitor

Azure Monitor to zespół usług pomagających zmaksymalizować dostępność i wydajność aplikacji i usług w chmurze hybrydowej. Zapewnia kompleksowe rozwiązanie do zbierania, analizowania i działania na podstawie telemetrii ze środowisk chmurowych i lokalnych. Te informacje pomagają proaktywnie identyfikować problemy, które mają wpływ na aplikacje oraz zasoby, od których są zależne. W ramach Azure Monitor zaimplementowano następujące usługi:

- Wykrywanie i diagnozowanie problemów w aplikacjach i zależnościach za pomocą Application Insights,

- Korelację problemów z infrastrukturą przy pomocy VM insights i Container insights,
- Szczegółową analizę danych monitorowania za pomocą Log Analytics w celu rozwiązywania problemów i szczegółowej diagnostyki,
- Wspieranie skalowania systemów za pomocą automated actions,
- Tworzenie wizualizacji działania platformy Azure za pomocą dashboards i workbooks,
- Zbieranie danych z monitorowanych zasobów za pomocą Azure Monitor Metrics,
- Badanie zmian w danych w celu rutynowego monitorowania lub klasyfikacji incydentów za pomocą Change Analysis.

4.2. Azure Active Directory Identity Protection

Usługa AADIP umożliwia osiągnąć następujące cele:

- Automatyzację wykrywanie i korygowanie zagrożeń związanych z tożsamością,
- Badanie zagrożeń za pomocą danych w portalu,
- Eksportowanie danych wykrywania ryzyka do innych narzędzi,

Sygnały generowane przez ochronę tożsamości przekazywane są do narzędzi takich jak:

- Dostęp warunkowy - w celu podejmowania decyzji dotyczących dostępu,
- SIEM w celu dalszego zbadania.

Usługa AADIP umożliwia dla systemów bazujących na Azure Active Directory:

- Ochronę tożsamości, niezależnie od ich poziomu uprawnień,
- Proaktywne zabezpieczanie użycia skompromitowanych tożsamości.

AADIP oferuje następujące funkcje ochrony tożsamości:

- Udostępnia pulpit nawigacyjny ochrony tożsamości,
- Wykrywa luki w zabezpieczeniach i wskazuje konta wysokiego ryzyka,
- Generuje niestandardowe zalecenia, aby poprawić ogólny stan zabezpieczeń przez wyróżnianie luk w zabezpieczeniach,
- Oblicza poziom ryzyka logowania,
- Oblicza wskaźniki ryzyka dla użytkownika,
- Bada zdarzenia o podwyższonym ryzyku,
- Bada i wysyła powiadomienia dla zdarzeń o podwyższonym ryzyku,

- Zapewnia mechanizmy przepływu pracy wspomagające śledzenie naruszenia bezpieczeństwa tożsamości,
- Zapewnia łatwy dostęp do krytycznych akcji, takich jak resetowanie haseł,
- Wprowadza zasady dostępu warunkowego dla kont uprzywilejowanych na podstawie szacunku ryzyka.

4.3. Azure DDoS Protection

Usługa *Azure DDoS Protection* zapewnia następujące rodzaje funkcji:

Podstawowe: Automatycznie włączone w ramach subskrypcji platformy Azure, zapewniające monitorowanie ruchu, a także ograniczenie w czasie rzeczywistym typowych ataków na poziomie sieci.

Standardowe: Udostępniające dodatkowe zabezpieczenia skierowane na ochronę zasobów usługi Azure Virtual Network. Usługi z tej grupy nie wymagają dodatkowej konfiguracji aplikacji. Za pomocą dedykowanego monitorowania i algorytmów uczenia maszynowego następuje dostosowanie zasad ochrony. Zasady są stosowane do publicznych adresów IP skojarzonych z zasobami wdrożonymi w sieciach wirtualnych, takich jak usługa Azure Load Balancer, Azure Application Gateway i usługi Azure Service Fabric. Ta ochrona nie ma zastosowania do środowiska usługi App Service. Telemetria usług, zarówno on-line jak i danych historycznych, jest dostępna dzięki Azure Monitor.

4.4. Azure Web Application Firewall

Azure Web Application Firewall chroni aplikacje internetowe przed typowymi technikami hakowania sieci Web, takimi jak wstrzykiwanie kodu SQL, oraz lukami w zabezpieczeniach, takimi jak skrypty międzywitrynowe.

Podstawowymi funkcjami Azure WAF są:

- Kompleksowa ochrona dla określonych w Open Web Application Security Project (OWASP) dziesięciu najważniejszych zagrożeń bezpieczeństwa,
- Niestandardowe i zarządzane zestawy reguł zapobiegające złośliwym atakom na brzegu sieci,
- Wgląd w czasie rzeczywistym w środowisko i alerty bezpieczeństwa,

- Pełna obsługa interfejsu API REST w celu automatyzacji procesów DevOps.

4.5. Azure Front Door

Azure Front Door to usługa sieciowa dostarczania zawartości z chmury (CDN), która zapewnia wymaganą wydajność, skalowalność i bezpieczne środowisko użytkownika dla danych i aplikacji. Realizuje ona następujące funkcje:

- Narzędzia i DevOps do automatyzacji i usprawnienia wdrożeń,
- W pełni konfigurowalny silnik reguł dla zaawansowanego routingu,
- Skalowalność dzięki globalnemu równoważeniu obciążenia HTTP i przełączaniu awaryjnemu,
- Dołączanie zapory aplikacji internetowych (WAF), ochronę DDoS i ochrona botów w zakresie ochrony aplikacji i treści.

4.6. Role Based Access Control - Zasada minimalnych uprawnień

Kontrola dostępu oparta na rolach (*Role Based Access Control* – RBAC) jest systemem pozwalającym precyzyjnie zarządzać uprawnieniami do danych i usług na platformie Azure na bazie uprawnień ról zdefiniowanych w systemie, także w kontekście przydziału zadań w zespołach. RBAC wykorzystuje usługę *Azure Resource Manager* zapewniającą spójną warstwę zarządzania, umożliwiającą tworzenie, aktualizowanie i usuwanie zasobów w subskrypcji platformy Azure.

Przykładami użycia RBAC są:

- Zezwolenie jednemu użytkownikowi na zarządzanie maszynami wirtualnymi w ramach subskrypcji, a innemu na zarządzanie sieciami wirtualnymi,
- Zezwolenie grupie administratorów baz danych na zarządzanie bazami danych SQL w ramach subskrypcji,
- Zezwolenie użytkownikowi na zarządzanie wybranymi zasobami w grupie zasobów, w tym maszynami wirtualnymi, witrynami internetowymi i podsieciami,
- Zezwolenie aplikacji na dostęp do wybranych zasobów w grupie zasobów.

4.7. Application Gateway

Usługa Application Gateway (AG) pozwala na równoważenie obciążenia ruchu internetowego z zarządzaniem ruchu do konkretnej aplikacji internetowej w odróżnieniu od tradycyjnych rozwiązań działających w warstwie transportu na podstawie źródłowego adresu IP i portu do docelowego adresu IP i portu.

AG pozwala kierować ruch na podstawie przychodzącego adresu URL. Jeśli w przychodzącym adresie URL jest element /obrazy, można kierować ruch do określonego zestawu serwerów (nazywanego pulą) skonfigurowanego na potrzeby obrazów, a zawierające element /video kierowane są do innej puli, która jest zoptymalizowana pod kątem filmów wideo.

Usługa automatycznie skaluje się w górę lub dół zależności od zmieniających się wzorców obciążenia ruchu.

4.8. VPN Gateway

Usługa VPN Gateway to typ bramy sieci wirtualnej, która służy do wysyłania zaszyfrowanego ruchu sieciowego między siecią wirtualną platformy Azure, a siecią lokalną za pośrednictwem publicznego Internetu. Za pomocą bramy sieci VPN można także wysyłać zaszyfrowany ruch sieciowy między sieciami wirtualnymi platformy Azure za pośrednictwem sieci dedykowanej firmy Microsoft. Każda sieć wirtualna może mieć tylko jedną bramę sieci VPN. Można utworzyć wiele połączeń do tej samej bramy sieci VPN. W przypadku utworzenia wielu połączeń do tej samej bramy sieci VPN wszystkie tunele VPN współdzielą dostępną przepustowość bramy.

4.9. Purview Information Protection

Microsoft Purview Information Protection to zespół usług bezpieczeństwa w ramach usługi Purview. Główne zadania usługi to:

Rozpoznanie danych w organizacji

Nie jest możliwa ochrona danych organizacji bez ich rozpoznania. Aby zrozumieć strukturę danych, miejsce ich składowania, sposób użycia i zidentyfikować poufne dane w środowisku hybrydowym, należy użyć następujących funkcji:

- Identyfikacji poufnych danych za pomocą wbudowanych lub niestandardowych wyrażeń regularnych albo funkcji,

- Identyfikuje poufne dane, używając przykładów danych, które przeglądamy, zamiast identyfikować elementy poprzez dopasowywanie wzorców. Możliwe jest użycie wbudowanych klasyfikatorów lub budowa klasyfikatorów z własną zawartością,
- Graficznie identyfikuje zasoby w organizacji, które mają etykietę poufności, etykietę przechowywania lub zostały sklasyfikowane w inny sposób. Na podstawie tych informacji można uzyskać wgląd w działania podejmowane przez użytkowników na tych zasobach,

Aby zastosować działania chroniące dane (np. szyfrowanie, ograniczenia dostępu i oznaczenia wizualne, należy użyć następujących funkcji:

- Spójnego etykietowania danych w aplikacjach, usługach i na urządzeniach w celu ochrony danych podczas ich przesyłania wewnątrz i na zewnątrz organizacji,
- Na urządzeniach z systemem Windows rozszerzenie zakresu etykietowania na Eksploratora plików i PowerShell, czy dodatkowych funkcji aplikacji pakietu Office,
- Przy odpowiednich uprawnieniach - odszyfrowania chronionej informacji lub ze względu na wymagania prawne przechowywania kluczy szyfrowania w określonej lokalizacji,
- Szyfrowania wiadomości e-mail i załączonych dokumentów, które są wysyłane do dowolnego użytkownika na dowolnym urządzeniu, dzięki czemu tylko uprawnieni odbiorcy mogą odczytywać informacje wysłane pocztą e-mail,
- Ochrona przed odczytem danych przez nieautoryzowane systemy lub personel,
- Ochrona list i bibliotek programu SharePoint, dzięki czemu, gdy użytkownik wyewidencjonuje dokument, pobrany plik jest chroniony, i tylko upoważnione osoby mogą odczytać plik i używać go zgodnie z zasadami określonymi w organizacji,
- Ochrona dla istniejących wdrożeń lokalnych korzystających z programu Exchange, SharePoint albo serwerów plików z systemem Windows Server i infrastrukturą klasyfikacji plików (FCI),
- Dzięki ujednoliconemu skanerowi etykiet usługi Information Protection odnajdowanie, etykietowanie i ochrona poufnych informacji znajdujących się w lokalnych zasobach danych,
- Dzięki usłudze Defender for Cloud Apps odnajdowanie, etykietowanie i ochrona poufnych informacji znajdujących się w chmurze,

- Identyfikacja poufnych danych i stosowania automatycznego etykietowania do zawartości w zasobach Microsoft Purview Data Map, w tym Azure Data Lake i Azure Files, oraz dane schematyzowane, takie jak kolumny w Azure SQL DB i Cosmos DB,
- Dzięki pakietowi Microsoft Information Protection SDK rozszerzanie zakresu etykietowania na wytwarzane aplikacje i usługi.

Zapobieganie wyciekowi danych

Aby zapobiec celowemu, przypadkowemu lub nadmiarowemu udostępnianiu poufnych informacji, należy użyć następujących funkcji:

- Microsoft Purview Data Loss Prevention (DLP) - zapobiega nieuprawnionemu udostępnianiu poufnych zasobów,
- Endpoint data loss prevention - rozszerza zakres działania DLP na elementy, które są używane i udostępniane na komputerach z systemem Windows 10 i Windows 11,
- Microsoft Compliance Extension - rozszerza zakres działania DLP na przeglądarkę Chrome,
- Microsoft Purview data loss prevention on-premises scanner - rozszerza zakres monitoringu DLP na lokalne udziały plików oraz foldery i biblioteki dokumentów programu SharePoint,
- Rozszerza niektóre funkcje DLP na czaty i wiadomości kanałów Teams.

4.9.1. Information Protection

Usługa Information Protection pozwala na klasyfikację, wyszukiwanie i zabezpieczanie danych przechowywanych i przetwarzanych w Office 365 oraz lokalnych repozytoriach. Jest to kluczowy mechanizm dla ochrony informacji, pozwalający wiedzieć co chroni organizacja, a następnie dobrać odpowiednie metody zabezpieczeń. Jest też wstępem do klasyfikacji stacji roboczej. Etykiety klasyfikujące informację są nadawane z uprzednio przygotowanych szablonów automatycznie (na bazie przeszukiwania zawartości dokumentów czy maili) lub manualnie przez użytkownika. Dotyczy to zarówno już istniejącej, składowanej czy edytowanej informacji, jak i procesu opatrywania nowo tworzonych dokumentów/maili. Nadanie odpowiedniej klasyfikacji powoduje dodanie metadanych do dokumentu, które mogą być wykorzystywane przez różne aplikacje i systemy.

Wdrożone aplikacje klienckie w Office 365 wyposażone są w narzędzie wskazujące jak sklasyfikowana została informacja oraz umożliwiające (po podaniu powodu) zmienić tą klasyfikację.

Zatwierdzone szablony etykiet są przygotowane i dystrybuowane w całej organizacji.

Przewidziane jest stosowanie mechanizmu *Azure Rights Management*, co po wybraniu odpowiedniej etykiety (np. „dane osobowe") spowoduje automatyczne zaszyfrowanie informacji z wybranymi uprawnieniami dostępu.

4.9.2. Communication Compliance

Communication Compliance to rozwiązanie do analizy ryzyka wewnętrznego, które pomaga zminimalizować ryzyko związane z komunikacją, pomagając wykrywać, przechwytywać niezgodne z politykami wiadomości w organizacji i reagować na nie.

Zasady uprawnionego przekazywania informacji komunikacji w organizacji pomagają przezwyciężyć wiele wyzwań związanych ze zgodnością oraz komunikacją wewnętrzną i zewnętrzną, w tym:

- Coraz większej liczby typów kanałów komunikacji,
- Rosnącej liczby danych wiadomościach,
- Egzekwowania przepisów,
- Ryzyka kar.

Wymagany jest rozdział obowiązków między administratorami IT a zespołem zarządzania zgodnością. Zgodność komunikacji ułatwia oddzielenie konfiguracji zasad od badania i przeglądania komunikatów. Na przykład grupa IT w organizacji może być odpowiedzialna za konfigurowanie uprawnień, grup i zasad roli zgodności z komunikacją, a badacze i recenzenci mogą być odpowiedzialni za klasyfikację wiadomości, przegląd i działania ograniczające zagrożenie.

Propozycje dotyczące planowania rozwiązania problemu zgodności i ryzykownych działań w organizacji opisane są w części dotyczącej analizy ryzyka.

4.9.3. Compliance Manager

- Pozwala spełnić wymagania dotyczące zasad zgodności z globalnymi, przemysłowymi lub lokalnymi przepisami i standardami w środowiskach hybrydowych,

- Oferuje kompleksowe funkcje zarządzania zgodnością, takie jak zarządzanie przepływem pracy, wdrażanie kontroli i katalogowanie dowodów,
- Umożliwia korzystanie z gotowych, konfigurowalnych i wielochmurowych szablonów oceny regulacyjnej,
- Zmniejsza ryzyko braku zgodności dzięki funkcjom, takim jak ocena zgodności, mapowanie kontroli, wersjonowanie i raporty kontroli,
- Dostarcza ponad 300 gotowych do użycia i konfigurowalnych szablonów oceny zgodności stosowanych usług z regulacjami.

4.9.4. Data Lifecycle Management

- Klasyfikuje i zarządza danymi na dużą skalę, w celu uzyskania zgodności z prawem, politykami prywatności i regulacyjne obowiązki dotyczące treści,
- Klasyfikuje, przegląda i usuwa dane na platformie Microsoft 365,
- Korzysta z inteligentnych funkcji uczenia maszynowego, aby klasyfikować zawartość i automatycznie stosować odpowiednie zasady,
- Dostarcza informacji o działaniach na danych, dowody usunięcia i udokumentowane ścieżki audytu z zarządzaniem informacjami.

4.9.5. Data Loss Prevention

Automatycznie chroni poufne informacje przed nieautoryzowanym i nieuprawnionym dostępem do aplikacji, usług, punktów końcowych i plików.

Organizacje mają pod swoją kontrolą poufne informacje, takie jak dane finansowe, dane zastrzeżone, numery kart kredytowych, dane osobowe czy medyczne. Aby chronić te poufne dane i zmniejszyć ryzyko ich wycieku, trzeba zapobiegać niewłaściwemu udostępnianiu ich przez użytkowników nieuprawnionym osobom lub organizacjom. Ta praktyka nazywa się zapobieganiem wyciekom danych (DLP) - tych umyślnych jak i przypadkowych.

Dzięki DLP możliwe jest wprowadzenie skutecznych zabezpieczeń przed wyciekiem informacji i dostosowaniem (w tym zakresie) do obowiązującego prawa, regulaminów i polityk bezpieczeństwa.

Po ustaleniu w organizacji zasad DLP można identyfikować, monitorować i automatycznie chronić poufne elementy w następujących systemach:

- Microsoft 365 (Teams, Exchange, SharePoint i OneDrive),
- Aplikacje Office (Word, Excel i PowerPoint),
- Windows 10, Windows 11, MacOS (Catalina 10.15 i wyższe),
- Wybrane usługi SaaS,
- Lokalne zasoby plików i lokalne zasoby SharePoint.

Funkcja DLP wykrywa poufne elementy danych za pomocą analizy treści, a nie tylko prostego skanowania tekstu. Zawartość jest analizowana pod kątem dopasowania danych podstawowych do słów kluczowych, oceny wyrażeń regularnych, sprawdzania poprawności funkcji wewnętrznych oraz dopasowania danych pomocniczych, związanych z danymi podstawowymi. DLP wykorzystuje również algorytmy uczenia maszynowego i inne metody do wykrywania zawartości określonej w zasadach DLP.

W zależności od konfiguracji usługa może zablokować dostęp do informacji osobom nieuprawnionym lub zaszyfrować tą informację. DLP generuje też podpowiedzi dla użytkowników sugerując im odpowiednie działania w zakresie klasyfikacji i ochrony informacji.

Administratorzy bezpieczeństwa mają do dyspozycji kokpit pozwalający na tworzenie polityk ochrony informacji, zarządzanie nimi i raportowanie zgodności ochrony informacji z założeniami.

4.9.6. eDiscovery

eDiscovery Premium opiera się na istniejących funkcjach zbierania elektronicznych materiałów dowodowych i analiz firmy Microsoft. Zbieranie elektronicznych materiałów dowodowych jest wspierane przez kompleksowy przepływ pracy służący do zachowywania, gromadzenia, analizowania, przeglądania i eksportowania zawartości, która wspomaga wewnętrzne i zewnętrzne dochodzenia w organizacji. Umożliwia zespołom prawnym zarządzanie całym przepływem pracy w celu komunikowania się z osobami zaangażowanymi w sprawę.

Przepływami pracy związanymi ze zbieraniem elektronicznych materiałów dowodowych można zarządzać, identyfikując badane w procesie osoby i wykorzystywane przez nie źródła danych. Umożliwia stosowanie blokad w celu zabezpieczenia danych, a następnie zarządzanie procesem komunikacji z zespołem prawnym. Funkcje uczenia maszynowego, wykorzystujące zaawansowane indeksowanie i wyszukiwanie, pomagają również zredukować duże ilości danych do analizy.

4.9.7. Insider Risk Management

Narzędzie zapewniania zgodności, które pomaga zminimalizować ryzyko wewnętrzne, umożliwiając wykrywanie, badanie i działanie na złośliwe i nieumyślne działania w organizacji. Zasady dotyczące ryzyka niejawnego dostępu do informacji umożliwiają zdefiniowanie typów zagrożeń do zidentyfikowania i wykrycia w organizacji, w tym podejmowanie działań w przypadku spraw i eskalowanie spraw do eDiscovery. Analitycy ryzyka w organizacji mogą szybko podjąć odpowiednie działania, aby upewnić się, że użytkownicy są zgodni ze standardami organizacji.

Insider Risk Management

- Wykrywa, bada i umożliwia podejmowanie działań w związku z krytycznymi zagrożeniami w organizacji, w tym kradzieżą danych, wyciekami danych i naruszeniami zasad zabezpieczeń,
- Zarządza ryzykiem związanym z danymi dzięki użyciu pseudonimizacji i kontrolom,
- Identyfikuje ukryte zagrożenia za pomocą konfigurowalnych szablonów uczenia maszynowego, które nie wymagają agentów w punktach końcowych,
- Wspomaga zespoły zajmujące się bezpieczeństwem, zasobami ludzkimi i prawem dzięki zintegrowanym przepływom pracy w dochodzeniach.

4.10. Microsoft 365 Defender

Microsoft 365 Defender to ujednolicony pakiet ochrony organizacji przed i po naruszeniu bezpieczeństwa, który pozwala koordynować wykrywanie, zapobieganie, badanie i reagowanie w punktach końcowych, tożsamościach, poczcie e-mail i aplikacjach, zapewniając zintegrowaną ochronę przed zaawansowanymi atakami.

Dzięki Microsoft 365 Defender specjaliści ds. cyberbezpieczeństwa mogą łączyć sygnały o zagrożeniach odbierane przez każdy z tych produktów oraz określać pełny zakres i wpływ zagrożenia, w jaki sposób wszedł do środowiska, na co ma wpływ i jak obecnie wpływa na organizację. Skonfigurowana usługa Microsoft 365 Defender podejmuje automatyczne działania w celu zapobieżenia atakowi lub jego zatrzymania oraz samoleczenia skrzynek pocztowych, punktów końcowych i tożsamości użytkowników, których dotyczy problem.

4.10.1. Defender for Endpoint

Defender for Endpoint zarządza zasadami ochrony przed złośliwym kodem i zabezpieczeniami zapory systemu Windows dla komputerów klienckich. Jest platformą bezpieczeństwa punktów końcowych zaprojektowaną, aby wspomagać działania w obszarze zapobiegania, wykrywania, badania i reagowania na zaawansowane zagrożenia. Usługa korzysta z mechanizmów Windows i usług, takich jak:

- Czujniki behawioralne punktów końcowych: Czujniki te, osadzone w systemie Windows 11 i Windows 11, zbierają i przetwarzają sygnały behawioralne z systemu operacyjnego i wysyłają te dane z czujników do prywatnej, izolowanej usługi Microsoft Defender for Endpoint,
- Analiza bezpieczeństwa w chmurze: Wykorzystując duże zbiory danych, mechanizmy uczenia się urządzeń, produkty z chmury (takie jak Office 365) i zasoby online, sygnały behawioralne są tłumaczone na szczegółowe informacje, pozwalające wykryć i zalecić reakcje na zaawansowane zagrożenia,
- Analiza zagrożeń: Generowana przez mechanizmy wyszukiwania firmy Microsoft, zespoły ds. zabezpieczeń i wzbogacona o informacje o zagrożeniach dostarczane przez partnerów, analiza zagrożeń umożliwia usłudze Defender for Endpoint identyfikowanie narzędzi, technik i wektorów ataku oraz generowanie alertów.

4.10.2. Defender for 0ffice 365

Defender for 0ffice 365 chroni organizację przed złośliwymi zagrożeniami stwarzanymi przez wiadomości e-mail, łącza (adresy URL) i narzędzia do współpracy. Usługa Defender dla usługi Office 365 realizuje:

- Zasady ochrony przed zagrożeniami: Pozwala zdefiniować zasady ochrony przed zagrożeniami, aby wprowadzić odpowiedni poziom ochrony dla swojej organizacji,
- Raporty: Udostępnia raporty w celu monitorowania wydajności usługi Defender for Office 365.
- Funkcje badania zagrożeń i reagowania na nie: Udostępnia narzędzia do badania, poznania, symulowania i zapobiegania zagrożeniom,
- Zautomatyzowane funkcje dochodzenia i reagowania: Automated investigation and response (AIR) wspomaga działania zespołu SOC w zakresie funkcji dochodzenia i reagowania. Gdy pojawiają się alerty są, do zespołu ds. operacji bezpieczeństwa należy przeglądanie tych alertów, ustalanie priorytetów i reagowanie na nie. Środowisko AIR umożliwia wydajne i skuteczne działanie. Funkcje środowiska AIR obejmują zautomatyzowane procesy dochodzeniowe w odpowiedzi na dobrze znane zagrożenia. Odpowiednie działania naprawcze wymagają zatwierdzenia, umożliwiając zespołowi operacji bezpieczeństwa skuteczne reagowanie na wykryte zagrożenia. Dzięki środowisku AIR można skupić się na zadaniach o wyższym priorytecie, nie tracąc z oczu ważnych alertów.

4.10.3. Defender Vulnerability Management

Wbudowane funkcje zarządzania lukami w zabezpieczeniach wykorzystują oparte na ryzyku podejście do wykrywania, oceny, ustalania priorytetów i korygowania luk w zabezpieczeniach punktów końcowych i błędnych konfiguracji.

4.10.4. Redukcja powierzchni ataku

Zestaw możliwości redukcji powierzchni ataku zapewnia pierwszą linię obrony. Upewniając się, że ustawienia konfiguracji są prawidłowe i stosowane są techniki ograniczania możliwości ataku. Ten zestaw funkcji obejmuje również ochronę sieci, blokując dostęp do złośliwych adresów IP, domen i adresów URL.

4.10.5. Next-generation protection

Defender for Endpoint korzysta z ochrony zaprojektowanej do wykrywania różnych typów pojawiających się zagrożeń wykorzystując:

- Ochronę antywirusową opartą na zachowaniu, heurystyce i czasie rzeczywistym, która obejmuje ciągłe skanowanie przy użyciu monitorowania zachowania plików i procesów oraz innych heurystyk (znanych również jako ochrona w czasie rzeczywistym). Obejmuje to również wykrywanie i blokowanie aplikacji, które są uważane za niebezpieczne, ale mogą nie zostać wykryte jako złośliwe oprogramowanie,
- Ochronę jako serwis, która obejmuje niemal natychmiastowe wykrywanie i blokowanie nowych i pojawiających się zagrożeń,
- Dedykowaną ochronę i aktualizację produktów, które obejmują aktualizacje związane z Microsoft Defender.

4.10.6. Zautomatyzowane dochodzenie i naprawa

W połączeniu z możliwością szybkiego reagowania na zaawansowane ataki usługa *Microsoft Defender for Endpoint* oferuje funkcje automatycznego badania i korygowania, które pomagają zmniejszyć liczbę sygnalizowanych alarmów.

4.10.7. Secure Score for Devices

Usługa Defender for Endpoint zawiera mechanizm Secure Score for Devices, który ułatwia dynamiczną ocenę stanu zabezpieczeń sieci, identyfikowanie niechronionych systemów i podejmowanie zalecanych działań w celu poprawy ogólnego bezpieczeństwa organizacji.

Application Guard

Microsoft Defender Application Guard jest usługą izolującą użytkowników od stron internetowych, usług typu chmurowego i sieci zdefiniowanych jako niezaufane. Umożliwia definiowanie listy zasobów zaufanych, do których użytkownicy mają pełny dostęp. W przypadku, gdy użytkownik chce skorzystać z zasobu nie będącego na takiej liście, jest on otwierany w izolowanym kontenerze, odseparowanym od środowiska systemu operacyjnego. Taki kontener jest anonimowy, a więc atakujący nie tylko nie jest w stanie dostać się do środowisk produkcyjnych, ale też nie może przechwycić tożsamości użytkownika.

4.10.8. Exploit Guard

Windows Defender Exploit Guard jest usługą chroniącą użytkowników systemu operacyjnego Windows w następujących obszarach:

- Chroni aplikacje o znanych podatnościach,
- Zmniejsza powierzchnię ataków na aplikacje,
- Chroni urządzenia klienckie przed zagrożeniami w ruchu sieciowym,
- Chroni pliki w katalogach systemowych.

Zaletami tej usługi są skuteczność, małe obciążenie systemu klienckiego i przezroczystość dla użytkownika.

4.10.9. Microsoft Defender Antivirus

Ważnym składnikiem usług ochrony urządzeń klienckich i serwerów jest Defender Antivirus, który jest instalowany wraz z systemem operacyjnym.

Oprogramowanie antywirusowe i anty-malware jest implementowane na poziomie serwerów i na poziomie stacji klienckich. Usługa Defender Antivirus ma następujące możliwości:

- wykrywanie złośliwego oprogramowania i programów szpiegujących oraz wykonywanie działań korygujących,
- możliwość aktualizacji oraz wdrożenia klienta poprzez infrastrukturę WSUS (klient oraz definicje),
- możliwość aktualizacji/wdrożenia klienta poprzez system dystrybucji oprogramowania (np. System Center),
- możliwość konfigurowania zasad bezpieczeństwa za pomocą polityk,
- możliwość generowania raportów, alertów pozwalających na pełną kontrolę nad zagrożeniami, stanem komputerów, aktualizacjami,
- możliwość wykrywania błędów w konfiguracji systemów operacyjnych, braku krytycznych uaktualnień,
- wsparcie instalacji serwerowej dla maszyn wirtualnych,
- generowanie szczegółowych raportów do poziomu pojedynczego komputera,

- wykorzystanie wbudowanych w systemy operacyjne Windows mechanizmów monitorujących (Windows Filter Manager),
- wykrywanie programów typu rootkit i wykonywanie działań korygujących,
- ocena krytycznych luk w zabezpieczeniach i automatyczne aktualizowanie definicji oraz oprogramowania antymalware,
- wykrywanie luk w zabezpieczeniach sieci przy użyciu systemu Network Inspection System,
- integracja z usługą Cloud Protection w celu zgłaszania złośliwego oprogramowania do firmy Microsoft. Po dołączeniu do tej usługi klient Endpoint Protection lub usługa Windows Defender pobiera najnowsze definicje z Centrum ochrony przed złośliwym oprogramowaniem w przypadku wykrycia niezidentyfikowanego złośliwego oprogramowania na komputerze,
- zarządzanie ustawieniami zapory systemu Windows.

Zapewniona jest ochrona w czasie rzeczywistym przed wirusami i oprogramowaniem szpiegowskim dla środowisk systemów operacyjnych 32- i 64-bitowych.

Serwer zarządzania jest obsługiwany przy użyciu centralnej konsoli. Umożliwia ona wybór ustawień prekonfigurowanych i zmianę ustawień klienckich w celu dostosowania do specyficznych warunków danego środowiska. Ustawienia dotyczą harmonogramu skanowania, aktywacji i dezaktywacji ochrony w czasie rzeczywistym, działań podejmowanych domyślnie w razie wykrycia różnych rodzajów zagrożeń oraz sposobu powiadamiania i raportowania. Aby uprościć dystrybucję ustawień na komputerach klienckich Defender został przystosowany do użycia Zasad Grupy (Group Policy) usługi Active Directory. Klienci mogą również zdecydować się na korzystanie z istniejącego systemu dystrybucji oprogramowania.

Aktualizacje definicji złośliwego oprogramowania są dostarczane z Microsoft Update. Defender upraszcza dystrybucję aktualizacji definicji na komputerach klienckich dzięki zastosowaniu usług Microsoft Windows Server Update Services (WSUS). Pozwalają one administratorom ustawić automatyczne zatwierdzanie pobierania najnowszych sygnatur lub testować i zatwierdzać poszczególne aktualizacje. Klienci mogą również skorzystać z

dowolnego systemu dystrybucji oprogramowania, używanego w danym środowisku. Konta użytkowników zdalnych mogą pobierać aktualizacje sygnatur z witryny Microsoft Update.

Ponadto Defender posiada następujące certyfikaty:

- Certyfikat vb100
- Certyfikat CESG Claims Tested Mark (CCTM) w kategorii Integrity Protection
- Certyfikat ICSA Labs w kategoriach
  - Anti-Virus Detection
  - Anti-Virus Cleaning
- Certyfikat West Coast Labs' Checkmark w kategoriach:
  - Anti-Malware
  - Anti-Spyware Desktop
  - Anti-Trojan
  - Anti-Virus Desktop
  - Anti-Virus Disinfection
  - Anti-Virus Server
  - CCTM - Checkmark Anti-Spyware Desktop
  - CCTM - Checkmark Anti-Trojan
  - CCTM - Checkmark Anti-Virus Desktop
  - CCTM - Checkmark Anti-Virus Disinfection

4.10.10. Defender for Cloud

Defender for Cloud umożliwia ujednolicone zarządzanie zabezpieczeniami i zaawansowaną ochronę przed zagrożeniami usług z chmury hybrydowej.

Jest to platforma zarządzania stanem zabezpieczeń w chmurze (CSPM) i platforma ochrony obciążeń w chmurze (CWPP) dla wszystkich zasobów platformy Azure, lokalnych i wielochmurowych (Amazon AWS i Google GCP). Defender dla chmury realizuje trzy istotne funkcje:

- Wskaźnika bezpieczeństwa - stale oceniającego stan zabezpieczeń, śledzącego nowe możliwości zabezpieczeń i raportującego postęp działań związanych z zabezpieczeniami,
- Kreowania zaleceń w zakresie akcji chroniących usługi przed znanymi zagrożeniami,
- Dostarczania alertów w czasie rzeczywistym, dzięki czemu można natychmiast reagować i zapobiegać incydentom,
- Przy współdziałaniu z innymi usługami bezpieczeństwa pozwala stosować zasady zabezpieczeń do różnych obciążeń, ograniczać podatność na zagrożenia i wykrywać ataki oraz reagować na nie,
- Ocenia środowisko i pozwala poznać stan zasobów i określić, czy są one bezpieczne,
- Umożliwia ocenę obciążeń i generuje zalecenia dotyczące zapobiegania zagrożeniom oraz alerty związane z wykryciem zagrożeń,
- Zapewnia wytyczne do automatycznego skalowania i ochronę w ramach usług platformy Azure.

Utrzymywanie bezpieczeństwa zasobów to wspólna odpowiedzialność dostawcy usług w chmurze i zarządzającego zasobami lokalnymi. Podczas przechodzenia do chmury trzeba upewnić się, że obciążenia będą bezpieczne w kontekście dostępności systemu. Przejście na model IaaS (infrastruktura jako usługa) to większa odpowiedzialność po stronie klienta niż w przypadku korzystania z modeli PaaS (platforma jako usługa) i SaaS (oprogramowanie jako usługa). Usługa Azure Security Center zapewnia narzędzia potrzebne do zwiększenia bezpieczeństwa sieci, zabezpieczenia usług i zapewnienia maksymalnego poziomu bezpieczeństwa przy utrzymaniu założonej dostępności.

Plany Defender for Cloud oferują ochronę w następujących obszarach:

- Microsoft Defender for Servers
- Microsoft Defender for Storage
- Microsoft Defender for SQL
- Microsoft Defender for Containers
- Microsoft Defender for App Service
- Microsoft Defender for Key Vault

- Microsoft Defender for Resource Manager
- Microsoft Defender for DNS
- Microsoft Defender for open-source relational databases
- Microsoft Defender for Azure Cosmos DB

4.10.11. Threat Experts

Usługa ta udostępnia narzędzia dla Centrum Operacyjne Bezpieczeństwa (SOC) zarządzającego rozwiązywaniem problemów z bezpieczeństwem na poziomach technicznym i organizacyjnym,

Usługa dostarcza między innymi:

- Informacje o atakach, ich celu, użytych metodach, harmonogramie ataku, zasięgu i skutkach.
- Mechanizmy oparte są na monitorowaniu zagrożeń i ich analizie w skali globalnej, uczeniu maszynowym analizującym występowanie znanych i nieznanych zagrożeń, korelacji informacji identyfikacji ryzyk oraz symulacji potencjalnego rozwoju ataku i jego skutków,
- Konsultacje zespołu ekspertów dostępnej na żądanie.

4.10.12. Advanced Threat Analytics

Pozwala analizować, poznawać i identyfikować typowe i nietypowe zachowania użytkowników, urządzeń, aplikacji i wszelkich zasobów.

Dzięki wbudowanej bazie wzorców jest w stanie wykryć typowe efekty ataku na system, a jednocześnie dzięki mechanizmom uczenia się – rozpoznawać nietypowe zachowania i zdarzenia będące odstępstwami od normalnego działania systemów. Najczęściej wykorzystywanym źródłem informacyjnym zasilającym usługę ATA jest System Center Operation Manager – przekazujące dane do Security Information and Event Management (SIEM) - Sentinel.Wykrywane i raportowane są:

- Nietypowe zmiany w DNS,
- Masowe zmiany w prawach dostępu,
- Nieoczekiwane zmiany na poziomie usługi LDAP,
- Dostęp do zasobów bez posiadania uprawnień,

- Posługiwanie tymi samymi uprawnieniami przez wielu użytkowników,
- Wielokrotne nieudane próby dostępu,
- Aktywności na poziomie mechanizmów Honeypot i Honeytoken,
- Nietypowe zachowania użytkowników,
- Masowe kasowanie obiektów czy informacji,
- Ponadto wykrywane są typowe niedociągnięcia w konfiguracji czy procedurach, takie jak brak szyfrowania, przechowywanie haseł w postaci tekstu i tym podobne.

4.10.13. Defender for Cloud Apps

Defender for Cloud Apps to broker zabezpieczeń dostępu do chmury (CASB), który obsługuje różne tryby pracy, w tym zbieranie dzienników, łączniki interfejsu API i zwrotny serwer proxy. Zapewnia widoczność i kontrolę przepływu danych oraz zaawansowaną analitykę w celu identyfikowania i zwalczania cyberzagrożeń we wszystkich usługach w chmurze firmy Microsoft i innych firm.

Usługa Defender for Cloud Apps integruje się z rozwiązaniami firmy Microsoft i została zaprojektowana z myślą o wsparciu administratorów bezpieczeństwa. Zapewnia scentralizowane zarządzanie i możliwości automatyzacji.

4.11. Sentinel

Usługa Sentinel bazująca na usługach platformy Azure pozwala na wykonywanie analiz zabezpieczeń systemów teleinformatycznych dla całej jednostki. Można ją określić jako usługę SIEM nowej generacji. Jest to usługa skalowalna, w której praktycznie nie ma limitów liczby zapytań, korzystająca z zaawansowanych mechanizmów uczenia maszynowego oraz innych usług bezpieczeństwa dostępnych w chmurze Microsoft. Dodatkowo posiada lub pozwala tworzyć konektory do większości dostępnych źródeł danych. Między innymi można wykorzystać wbudowany interfejs REST API.

Podstawowymi funkcjami Sentinel są:

- Zbieranie i agregowanie danych i informacji z całego ekosystemu lokalnego i chmury – użytkowników (i ich zachowań), urządzeń, aplikacji i infrastruktury. Dodatkowym

narzędziem ułatwiającym pracę analityków zabezpieczeń są pulpity nawigacyjne pozwalające na obserwację i analizę tego co dzieje się w trakcie ataku,

- Wykrywanie standardowych oraz nowych, nietypowych zagrożeń dzięki analizie danych i zdarzeń w systemie z wizualizacją rozwoju ataków, przy jednoczesnej minimalizacji ryzyka pojawienia się fałszywych alarmów. Jest to możliwe dzięki wykorzystaniu uczenia maszynowego pozwalającego na analizę i korelację milionów danych oraz porównywanie ich z typowymi schematami zachowań użytkowników i usług,
- Badanie zagrożeń, ich przyczyn i potencjalnych skutków oraz tworzenie modeli skutecznego reagowania,
- Reagowanie na wykryte zagrożenia. Reagowanie to odbywa się na bazie tzw. Playbook – kolekcji procedur reagowania na wykryte zagrożenie. Procedury te mogą być przygotowywane i testowane, a następnie uruchamiane ręcznie lub automatycznie.

Usługa Sentinel jest stale aktualizowana poprzez udoskonalanie modeli wykrywania i reagowania na bazie milionów zdarzeń z całego świata i wymiany doświadczeń użytkowników.

4.12. Purview

Usługa Purview realizuje dla danych organizacji:

- Uzyskanie wglądu w strukturę zasobów danych w całej organizacji,
- Umożliwianie uprawnionego dostępu do danych,
- Klasyfikację danych,
- Ochronę poufnych danych i zarządzanie nimi w chmurach, aplikacjach i punktach końcowych,
- Kompleksowe zarządzanie ryzykiem związanym z ochroną danych oraz zgodnością z przepisami i politykami.

Zastosowanie narzędzi Purview pozwala na:

- optymalizację ogólnej architektury systemów,
- deduplikację danych, ich właściwą ochronę,
- ujednolicenie procesów biznesowych opartych o uprawnienia,
- bezpieczny dostęp do aktualnych i referencyjnych danych,
- definiowanie architektury nowych, jak i modernizowanych systemów i usług,

- Zapewnienie zgodności z większością wymagań w zakresie zasad interoperacyjności i cyberbezpieczeństwa – między innymi rozp. w sprawie Krajowych Ram Interoperacyjności i minimalnych wymagań dla systemów teleinformatycznych, ustawą o cyberbezpieczeństwie czy też RODO.

Głównymi funkcjami Purview są:

- wykrywanie zasobów danych,
- wykrywanie źródeł ich pochodzenia,
- klasyfikacja danych,
- tworzenie mapy naszych zasobów danych z miejscami ich położenia,
- Automatyczne wykrywanie danych.

Purview realizuje funkcje wykrycie miejsca składowania danych, ich źródeł i sposobu ich używania – w tym procesów, które z nich korzystają. Funkcja automatycznego wykrywania danych usługi Purview pozwala zrealizować te zadania zarówno przy inicjalnym mapowaniu danych, jak też w trakcie użytkowania i rozwoju wykorzystywanych systemów.

W trakcie tego procesu następuje:

- wykrycie danych i źródeł ich pochodzenia,
- zautomatyzowanie zarządzania metadanymi w wielu źródłach danych,
- klasyfikacja danych z użyciem wbudowanych lub definiowanych we własnym zakresie schematów klasyfikacji,
- właściwe oznakowanie danych wrażliwych.

4.12.1. Budowa mapy danych

Drugim etapem po wykryciu i klasyfikacji danych jest budowa ich mapy w systemach i usługach dzięki usłudze Purview. Głównymi jej funkcjami są:

- budowa mapy położenia danych, ich źródeł, sposobu użycia oraz zależności między zasobami danych,
- automatyzacja i zarządzanie metadanymi z wielu źródeł,
- ciągła automatyczna lub ręczna klasyfikacja danych wraz z ich odpowiednim oznakowaniem i ujednoliceniem tej klasyfikacji w różnych systemach,
- integracja poprzez API z systemami Apache Atlas.

4.12.2. Katalogowanie i dostęp do danych

Po utworzeniu dynamicznej mapy danych konieczne jest udostępnienie narzędzi ułatwiających uprawnione ich wykorzystanie przez użytkowników. W tym zakresie Purview umożliwia:

- wyszukiwanie danych w oparciu o metadane, słowa kluczowe i pojęcia,
- rozpoznawanie danych poprzez dołączone metadane i opisy,
- ustalanie poziomu poufności danych,
- ustalanie pochodzenia danych wraz z graficzną wizualizacją źródeł i przepływów,
- właściwy dobór danych do procesów biznesowych oraz analizy,
- monitorowanie wykorzystania danych.

W trakcie wykorzystywania odpowiednio wykrytych, oznakowanych i skatalogowanych danych Purview umożliwia:

- ciągły proces monitoringu wykorzystania – od źródeł surowych danych, poprzez przekształcenia, do ich prezentacji i raportowania,
- użycie mechanizmów platformy Azure w celu pobierania, czyszczenia i integracji danych z różnych źródeł,
- wykrywanie już istniejących analiz i raportów, aby uniknąć ich duplikacji.

4.13. Usługi katalogowe

Usługi katalogowe zaimplementowane są w oparciu o Active Directory i pozwalają opisać, przechowywać i wykorzystywać informacje o zasobach w systemie, użytkownikach i ich grupach oraz relacjach między nimi.

Dla poszczególnych wpisów w katalogu zdefiniowano klasy obiektów, przy czym każdy wpis musi należeć przynajmniej do jednej z klas. W każdej klasie obiektów musi być przynajmniej jeden atrybut. W ten sposób każdy wpis w katalogu X.500 należy do jednej lub wielu klas obiektów oraz zawiera jedną lub wiele wartości poszczególnych typów atrybutów. Szczególnym rodzajem wpisów są aliasy, umożliwiające umieszczenie takiego samego wpisu w różnych miejscach drzewa. Dzięki takiemu rozwiązaniu zmiana dokonana w jednym wpisie powoduje odpowiednie zmiany we wszystkich aliasach.

Funkcjami usług katalogowych są:

- Centralna administracja pozwalająca na zarządzanie zasobami i ich uprawnieniami w całej organizacji.
- Dostarczenie mechanizmów zasad grupowych (Group Policy) pozwalającego na wymuszenie na stacjach roboczych i serwerach centralnie konfigurowanych ustawień systemu, uprawnień i środowiska użytkownika,
- Hierarchiczna budowa katalogu, zgodnie ze specyfikacją X.500,
- Przechodniość stosunków zaufania dzięki zastosowaniu protokołu bezpieczeństwa Kerberos. Zmniejsza to liczbę stosunków zaufania pomiędzy domenami. Stosunek przechodni oznacza, że gdy domena A ufa domenie B i domena C ufa domenie B, wówczas domena A ufa również domenie C,
- Wymuszenie w ramach całości systemu wspólnej polityki haseł określającej parametry i złożoność hasła, jak również warunki i długość blokady kont itp.,
- Wspólne zasady i reguły dla całości usług katalogowych pozwalający na łatwe jego rozszerzanie i możliwość definiowania nowych obiektów i właściwości,
- UK pozwala również na delegację praw do zarządzania określoną grupą komputerów i użytkowników poprzez wbudowane mechanizmy delegacji uprawnień,
- Kontrola i definicja bezpieczeństwa oparta na listach Access Control Lists (ACL) pozwalająca na replikację dozwolonych odwołań w skali całej hierarchii, aż do poziomu obiektu,
- Szerokie możliwości formułowania zapytań i rozbudowany mechanizm zapytań sieciowych dzięki strukturze podobnej do indeksu obsługującego zapytania dotyczące każdego obiektu w katalogu.

W Active Directory zaimplementowano trzy różne elementy logiczne.

- Obiekty

Są to składniki mające wiele atrybutów. Przykładowe obiekty to użytkownicy lub drukarki. Obiekt może być również kontenerem dla innych obiektów.

- Atrybuty obiektu

Wszystkie obiekty w katalogu mają atrybuty lub właściwości. W Microsoft Active Directory oba pojęcia używane są zamiennie. Atrybut to pewna ilość informacji. Obiekty znajdujące się w tym samym kontenerze mają te same atrybuty.

- Klasy obiektów

Active Directory grupuje obiekty według ich atrybutów. Wszystkie obiekty są kategoryzowane właśnie w ten sposób, na przykład jako użytkownicy lub drukarki. Tego rodzaju grupowanie logiczne odpowiada za organizację zasobów w katalogu.

Zaimplementowano następujące kontenery Active Directory:

- Domeny (*Domain*)

Domena zawiera obiekty odpowiadające zasobom sieciowym (komputery, użytkownicy, drukarki itd.), każda z domen przechowuje informacje tylko o obiektach do niej należących. Stanowią granicę bezpieczeństwa w pojedynczej sieci komputerowej. Active Directory składa się z jednej lub wielu domen. W samodzielnej stacji roboczej domeną jest sam komputer. Domena może być czymś więcej niż tylko fizyczną lokalizacją - każda dysponuje własnymi wytycznymi co do bezpieczeństwa w kontaktach z innymi domenami. Jeżeli kilka domen jest połączonych stosunkami zaufania i wykorzystują wspólną konfigurację, mówimy o strukturze domen.

- Jednostki organizacyjne

Stanowią kolejny podział struktury katalogu. Możliwe są dowolne hierarchie w ramach jednej domeny.

Kolejne ważne jednostki podziału struktury określają relacje między domenami. Należą do nich:

- Drzewo (*Tree*)

Jest to zgrupowanie lub hierarchiczne ustawienie jednej lub wielu domen UK, które współdzielą wspólną przestrzeń nazw DNS.

Wiele organizacji utrzymuje kilka domen, choć nie jest to niezbędne z technicznego punktu widzenia. Zastosowanie wielu domen tworzy hierarchię, która ma współzależną przestrzeń nazw i określana jest mianem drzewa. Drzewo tworzy logiczną strukturę wysokiego poziomu, w której domeny są wzajemnie relacyjnie powiązane. W obrębie drzewa domeny są wzajemnie powiązane stosunkami zaufania.

- Las (*Forest*)

Zgrupowanie lub hierarchiczne ustawienie jednego lub wielu drzew domen UK, które tworzą wydzieloną przestrzeń nazw. Wszystkie drzewa w lesie współdzielą schemat katalogu. Microsoft opracował koncepcję "lasu", który umożliwia zachowanie struktur, którymi można nadal zarządzać dzięki współistnieniu dwóch różnych przestrzeni nazw.

- Katalog główny (Global Catalog Server)

Jest to centralny zasób informacyjny usługi katalogowej. Powstaje w wyniku replikacji usługi katalogowej i zawiera kopie wszystkich obiektów drzewa. Tak więc, jest czymś w rodzaju indeksu całej sieci zapisującego kopię każdego obiektu w katalogu.

4.13.1. Usługa AD DS

Umożliwia wdrożenie kontrolerów domeny zarówno we własnej infrastrukturze (*on-premise*) jak i w modelu chmury (*Cloud*). Umożliwia uruchamianie nowych wirtualnych kontrolerów domeny poprzez klonowanie już istniejących.

Udostępnia kreator udostępniania kontrolerów domeny (*domain controller promotion wizard*) pozwalający na bezpieczne i szybkie przygotowanie lasu i domeny wraz z narzędziami zdalnej instalacji AD DS na docelowym serwerze.

Mechanizm dynamicznej kontroli dostępu (*dynamic access control – DAC*) wykorzystujący uwierzytelnienie na bazie oświadczeń (*claims-based authorization*). DAC zawierający centralne polityki dostępu, atrybuty katalogu oraz silnik klasyfikacji plików, pozwala na tworzenie złożonych tożsamości (*compound-identities*), łączących niezaprzeczalnie tożsamość użytkownika z tożsamością urządzenia w postaci jednego identyfikatora.

Zarządzanie Uprzywilejowanym Dostępem (*Privileged Access Management – PAM*) wykorzystującą las (*bastion forest*) izolowany od standardowego lasu pozbawionego możliwości dostępu na prawach administratora. Obniża to ryzyka związane z technika mi kradzieży tożsamości w Active Directory takimi jak *pass-the-hash*, czy *spear phishing.*

Mechanizm *Azure AD Join* dołączania użytkowników do Azure Active Directory, czyli usługi zarządzania tożsamością i dostępem w chmurze Microsoft. Obecnie nie jest wymagane już posiadanie konta Microsoft Account do wykorzystania tej usługi.

Paszport Microsoft jest to metoda uwierzytelniania bazująca na mechanizmach kluczy prywatnego/publicznego lub certyfikatu odporna na wiele form ataków na tożsamość

użytkowników uwierzytelniających się w AD, Azure AD, Microsoft Account czy też w usługach wspierających tzw. Fast ID (FIDO). Po wstępnej dwustopniowej weryfikacji w procedurze wystawiania paszportu Microsoft, jest on konfigurowany na urządzeniu. Użytkownik loguje się do urządzenia poprzez PIN lub cechy biometryczne, a następnie uruchamiany jest proces uwierzytelnienia wykorzystujący link do certyfikatu lub pary asymetrycznych kluczy generowanych przez TPM. Dostawcy tożsamości wykorzystują klucz publiczny, zarejestrowany w usłudze katalogowej do walidacji użytkownika poprzez jego mapowanie do klucza prywatnego i dostarczenie hasła jednorazowego (OTP) lub inny mechanizm, jak np. telefon do użytkownika z żądaniem PINu.

4.13.2. Usługa AD FS

Usługa ta zapewnia kontrolę nad realizacją uprawnień dostępu do systemów i informacji dla użytkowników oraz umożliwia wykorzystanie pojedynczego logowania (*single sign-on*) zasobów i usług.

AD FS generuje tokeny dla aplikacji klienckich w odpowiedzi na uprawnione żądanie dostępu, Przechowuje i przekazuje poświadczenia tożsamości użytkowników pochodzące z aplikacji sieciowej (*web application*).

Pozwala wykorzystać uwierzytelnienia oparte na oświadczeniach generowanych przez AD DS zawartych w biletach Kerberos po uwierzytelnieniu się do domeny.

4.13.3. Usługa AD CS

Usługa ta umożliwia wydawanie cyfrowych certyfikatów oraz zarządzanie nimi w systemach wykorzystujących infrastrukturę klucza publicznego.

Certyfikaty wydane przez usługę AD CS mogą być wykorzystane do uwierzytelniania użytkowników i urządzeń, szyfrowania oraz podpisywania dokumentów i wiadomości poczty elektronicznej. Te dwie ostanie funkcje, oprócz niezaprzeczalnego potwierdzenia tożsamości podpisującego, dają możliwość monitorowania niezmienności dokumentu czy wiadomości, bo w przypadku zmiany podpisanej treści – podpis traci ważność.

Zastosowano możliwość rejestracji certyfikatów dla komputerów niepodłączonych do domeny lub nawet dla komputerów, które nie są członkami domeny.

4.13.4. Usługa AD RMS

Usługa AD RMS jest narzędziem pozwalającym na spójne wprowadzenie polityk ochrony informacji poprzez zabezpieczanie samej informacji, a nie miejsca przechowywania czy warstwy transportowej.

Zarządzanie polityką dostępu do informacji z wykorzystaniem AD RMS pozwala szyfrować dokumenty oraz wiadomości poczty elektronicznej wraz mechanizmami nadawania odpowiednich praw dostępu zarówno pojedynczym osobom jak i ich grupom. Zastosowanie tej usługi skutecznie chroni informację, nawet gdy zostanie ona przeniesiona w miejsce fizycznie dostępne nieuprawnionym osobom.

4.14. Azure Active Directory

Obecnie większość procesu zarządzanie tożsamością dla komponentów w chmurze realizowane jest w oparciu o funkcje Azure Active Directory (AAD).

AAD nie jest ograniczona do platformy Azure ale jest podstawą nadawania, weryfikacji i wykorzystania tożsamości cyfrowej użytkowników we wszystkich usługach „chmurowych". Zdefiniowane są:

- role administratorów i użytkowników usług,
- ich cyfrowe poświadczenia (login, hasło, certyfikat, token),
- uprawnienia personalne lub grupowe.

Dla wszystkich usług z chmury użyta jest ta sama nazwa domenowa i te same definicje użytkowników, aby uzyskać jednolitą tożsamość użytkownika we wszystkich usługach.

Zaimplementowane scenariusze to:

- Udostępnianie usług i danych użytkownikom zewnętrznym, zwykle za pośrednictwem sieci Internet. Musimy zapewnić niezaprzeczalność i bezpieczeństwo takiego dostępu na bazie usługi katalogowej i zarządzania prawami dostępu użytkowników. Stosowane jest wyizolowanie takiej usługi od usługi obsługującej użytkowników wewnętrznych,
- Budowa systemu na bazie usługi platformowej Azure, gdzie najprościej jest wykorzystać usługę zarządzania tożsamością dostarczaną z platformą,

- Izolacja użytkowników mobilnych dostających się do zasobów wewnętrznych poprzez Internet. Użycie usługi AAD daje możliwość niezaprzeczalnego dostępu do takich zasobów, weryfikowanego poza systemami wewnętrznymi,
- Projekty krótkotrwałe, w których trzeba zapewnić niezaprzeczalność praw dostępu do danych i usług, a nie opłaca się na krótki okres czasu budować specjalnej, wydzielonej infrastruktury,
- Uwierzytelnianie użytkowników do zewnętrznej usługi lub pomiędzy różnymi systemami w modelu pojedynczego logowania (single sign-on).

AAD posiada funkcje pozwalające na posługiwanie się tożsamością cyfrową. Jest podstawą tworzenia bezpiecznych środowisk hybrydowych, w których bazując na uwierzytelnieniu użytkownika poprzez własną usługę katalogową, uwierzytelniamy się do systemów bazujących na AAD zawierającego profil tego samego użytkownika.

Wykorzystane jest stworzenie relacji wzajemnego zaufania pomiędzy AD i AAD.

W przypadku gdy organizacja korzysta z jednego konta w dowolnej zewnętrznej usłudze (np. Twitter), realizowane jest uwierzytelnienie każdego uprawnionego użytkownika poprzez własne, organizacyjne poświadczenia, które w AAD są mapowane na zdefiniowane uprzednio poświadczenia do zewnętrznej usługi, eliminując konieczność przekazywania użytkownikom tego samego loginu i hasła.

Wykorzystywane są wbudowane w AAD mechanizmy samoobsługi użytkowników:

- zmiana hasła,
- reset hasła,
- tworzenie grup użytkowników na bazie udzielonych uprawnień.

AAD posiada wbudowane, definiowalne mechanizmy uwierzytelniania wieloskładnikowego, wykorzystane w scenariuszach dla ochrony danych wrażliwych lub obsługi użytkowników zdalnych.

Mechanizmy zarządzania tożsamością w AAD stosowane są w połączeniu z środowiskami własnymi czy aplikacjami dzięki zastosowaniu standardowych protokołów takich jak SAML 2.0, WS-Federation i OpenID Connect. Poprzez wsparcie dla OAuth 2.0 możliwe jest wykorzystanie własnych aplikacji i interfejsów komunikacyjnych wykorzystujących AAD.

Dzięki wbudowanym mechanizmom, AAD realizuje funkcje:

- Utworzenie pojedynczego katalogu obiektów uwierzytelnianych jednostki w usłudze Azure AD,
- Niezaprzeczalne uwierzytelnienie w AAD,
- Uwierzytelnienie i autoryzację w usługach opartych o AAD,
- Uwierzytelnienie wieloskładnikowe z wykorzystaniem telefonicznych komunikatów głosowych, sms lub aplikacji typu aplikacji Authenticator,
- Uwierzytelnianie bez haseł, w tym przy pomocy Windows Hello, aplikacji Microsoft Authenticator czy kluczy zabezpieczeń FIDO2,
- Dostęp warunkowy, w którym Azure AD ocenia warunki logowania użytkownika i używa zasad dostępu warunkowego, które tworzy się w celu umożliwienia uprawnionego dostępu,
- Samoobsługa w zakresie odnawiania poświadczeń, sposobu ich potwierdzania lub ich resetu dla uprawnionych użytkowników,
- Synchronizację kont i uprawnień z lokalną usługą Active Directory,
- Pojedyncze logowanie (single-sign on) do nieskończonej liczby systemów poprzez bezpieczne przechowywanie poświadczeń użytkownika i powiązanie ich z kontem w AAD,
- Wykrywanie potencjalnych luk w zabezpieczeniach tożsamości organizacji i konfigurowanie zasad automatycznego rozwiązywania problemów ryzyka związanego z nieuprawnionym logowaniem,
- Zarządzanie kontami, poświadczeniami użytkowników i urządzeń oraz ich grupami wraz z cyklem ich życia.

AAD umożliwia skalowanie, pozwalające na obsługę wykorzystywanych obiektów tożsamości, posiadających reprezentację w zarządzanych źródłach danych połączonych z systemem, mając możliwość skalowania stanowisk wydających certyfikaty. Istnieje też możliwość zarządzania życiem certyfikatów w usługach katalogowych składających się z wielu lasów.

AAD wykorzystywane jest dla wielu systemów w środowiskach heterogenicznych. Współpraca ta jest realizowana z użyciem standardowych dla źródeł danych protokołów dostępu oraz przy minimalnej ingerencji w mechanizmy działania źródła danych połączonego z systemem. Zapewnia

też możliwość realizacji dwukierunkowej wymiany informacji z połączonymi źródłami danych udostępniając standardowe interfejsy umożliwiające komunikację dwustronną (np. wymianę danych o użytkownikach) z innymi systemami informatycznymi.

Ponadto AAD zapewnia agregację i synchronizację danych poprzez:

- Zapewnienie możliwości odczytu i zapisu danych pomiędzy źródłami danych działającymi w heterogenicznym środowisku systemów połączonych siecią lokalną lub rozległą,
- Zapewnienie możliwości integracji rozwiązania zarządzania tożsamością z następującymi źródłami danych:
  - Pliki tekstowe CSV, AVP, LDIF,
  - Relacyjne bazy danych
  - Usługi zarządzania tożsamością i dostępem Active Directory, Novell eDirectory, OpenLDAP.
- Zapewnienie komunikacji z użyciem standardowych dla każdego ze źródeł danych mechanizmów i protokołów oraz dwustronną wymianę danych w zakresie informacji o obiektach zarządzanych w ramach każdego ze źródeł danych,
- Umożliwienie tworzenia, uaktualniania oraz usuwania obiektów z połączonych źródeł danych,
- Definiowanie zakresu informacji odczytywanych z każdego ze źródeł danych oraz możliwość filtrowania danych o obiektach pochodzących ze źródeł danych na podstawie zadanych kryteriów,
- Definiowanie zasad przepływu danych pomiędzy systemami oraz rozszerzenia przepływu danych o możliwość zdefiniowania reguł transformacji danych w ramach realizowanego przepływu.

4.15. Zatwierdzanie i podpisywanie decyzji

Zatwierdzanie i podpisywanie decyzji odbywa się dzięki wykorzystaniu certyfikatów kwalifikowanych od zewnętrznego dostawcy.

5. Podstawowe obowiązki pracownika

Bezpieczeństwo teleinformatyczne jest kluczową częścią pracy i obowiązkiem każdego pracownika. Ochrona personelu, informacji, systemów, obiektów i klientów jest kluczowym elementem budowania zaufania i zgodności z prawem. Polityki bezpieczeństwa zapewniają stan, w którym wszystkie aspekty informacji zastrzeżonych pozostaną poufne, że integralność danych jest zachowana, że funkcje statutowe organizacji działają skutecznie i są odporne na ataki.

Niniejsze zasady zawierają szczegółowe informacje na temat wymagań dotyczących zabezpieczeń dotyczących personelu organizacji, zdefiniowanego zarówno jako personel wewnętrzny (pracownicy zatrudnieni w pełnym i niepełnym wymiarze godzin oraz stażyści), jak i personel zewnętrzny (wykonawcy, zewnętrzni, goście biznesowi i pracownicy tymczasowi). Wymagania te koncentrują się na osobistej odpowiedzialności za:

- Ochronę pracowników, klientów i gości,
- Ochronę aktywów fizycznych i niematerialnych,
- Kontrolę dostępu fizycznego i logicznego,
- Spełnieniu wymagań w zakresie szkoleń,
- Zgłaszanie naruszeń zabezpieczeń,
- Ujawnianie luk w zabezpieczeniach,
- Przestrzeganie obowiązujących przepisów prawa oraz zasad i procedur organizacji.

5.1. Szkolenie z zakresu cyberbezpieczeństwa

Organizacja dba o cykliczną edukację pracowników w zakresie bezpieczeństwa informacji. Pracownicy w zależności od zajmowanego stanowiska mogą uczestniczyć w szkoleniach z zakresu:

- ochrony Danych Osobowych,
- świadomości istnienia problemów bezpieczeństwa,
- szczegółowych aspektów bezpieczeństwa.

Aby uzyskać dostęp do systemów informatycznych oraz danych jednostki, pracownik musi przejść szkolenie z podstaw cyberbezpieczeństwa. Szkolenie dostępne jest w formie stacjonarnej/online. Po ukończeniu szkolenia i podpisaniu zobowiązania do przestrzegania regulaminu cyberbezpieczeństwa pracownik uzyskuje dostęp do zestawu narzędzi, usług i danych

niezbędnych do realizacji swoich obowiązków. Wymagane jest przechodzenie szkolenia przynajmniej raz do roku.

5.2. Dbałość o powierzony sprzęt i oprogramowanie

Pracownik zobowiązany jest dbać o powierzony sprzęt i stosować się do instrukcji obsługi producenta sprzętu. Ponadto pracownik nie może pozostawiać sprzętu bez zabezpieczeń uniemożliwiających jego kradzież lub w warunkach powodujących możliwość jego uszkodzenia. Uruchomiony sprzęt (telefon, laptop, komputer) nie może być pozostawiany w stanie zalogowania – umożliwiającym dowolnej osobie na dostęp.

W przypadku utraty sprzętu pracownik musi natychmiast zgłosić ten przypadek na ustalony i opublikowany w organizacji adres, za pośrednictwem maila lub numeru telefonu.

Dokonywanie napraw sprzętu we własnym zakresie jest niedozwolone. Uszkodzony sprzęt należy zgłaszać do osób odpowiedzialnych w organizacji.

Po zakończeniu eksploatacji sprzętu (zużycie, rozwiązanie umowy o pracę), pracownik niezwłocznie zdaje kompletny sprzęt do osób odpowiedzialnych w organizacji.

5.3. Wykorzystywanie sprzętu prywatnego do pracy

Realizacja modelu, w którym pracownik wykorzystuje prywatny sprzęt do realizacji zadań służbowych stacjonarnie lub zdalnie, wymaga dostosowania zasad bezpieczeństwa na tym sprzęcie do wymogów ustalonych w politykach bezpieczeństwa.

Pracownik chcący korzystać ze sprzętu prywatnego musi wyrazić zgodę na dokonanie zmian konfiguracyjnych na urządzeniu, zapewniających wymagany poziom bezpieczeństwa.

Dodatkowo pracownik zobowiązuje się do:

- Używania silnych haseł lub/i biometrycznych metod odblokowania urządzenia,
- Aktualizowania systemu operacyjnego i aplikacji do najnowszych wersji,
- Unikania łączenia się z niezaufanymi sieciami Wi-Fi lub Bluetooth,
- Nieotwierania nieznanych (podejrzanych) linków lub załączników,
- Korzystania z szyfrowania danych i kopii zapasowych, w tym dysków w urządzeniach,
- Zgłaszania utraty lub kradzieży urządzenia odpowiednim osobom.

5.4. Wykorzystywanie wyłącznie zaakceptowanej listy oprogramowania i usług

Dział IT określa listę oprogramowania i usług (w tym zewnętrznych) dopuszczonych do wykorzystywania przez konkretną rolę w organizacji. Użytkownik może zgłaszać konieczność modyfikacji tej listy poprzez wniosek do działu IT.

5.5. Instalowanie aktualizacji

Instalowanie aktualizacji jest obowiązkiem pracownika. Opóźnianie instalacji poprawek dystrybuowanych przez dział IT ponad 24 godziny jest niedozwolone.

5.6. Oznaczanie danych

Pracownik, kreując lub modyfikując dane obowiązany jest do ich klasyfikacji.

Jako dane podlegające szczególnej ochronie (informacje poufne) rozumie się:

- informacje o realizowanych kontraktach (zarówno planowane, bieżące jak i historyczne),
- informacje finansowe Firmy,
- informacje organizacyjne,
- dane dostępowe do systemów IT,
- dane osobowe,
- informacje stanowiące o przewadze konkurencyjnej organizacji,
- inne informacje oznaczone jako „informacji poufne” lub „dane poufne”.

5.7. Odpowiedzialność pracowników za dane dostępowe do systemów

Każdy pracownik zobowiązany jest do ochrony swoich danych dostępowych do systemów informatycznych. Dane dostępowe obejmują między innymi takie elementy jak:

- hasła dostępowe,
- klucze softwareowe (pliki umożliwiające dostęp – np. certyfikaty do VPN) oraz sprzętowe,
- inne mechanizmy umożliwiające dostęp do systemów IT.

Przykłady ochrony danych dostępowych:

- nieprzekazywanie dostępów do systemów IT innym osobom (np. przekazywanie swojego hasła dostępowego osobom trzecim),
- nieprzechowywanie danych w miejscach publicznych (np. zapisywanie haseł dostępowych w łatwo dostępnych miejscach),

- Ochrona danych dostępowych przed kradzieżą przez osoby trzecie.

5.8. Transport danych poufnych przez pracowników

Zabrania się przenoszenia niezabezpieczonych danych poufnych poza teren Firmy. W szczególności zabrania się przenoszenia danych poufnych na nośnikach elektronicznych (np.: pendrive, nośniki CD) poza teren organizacji.

5.9. Korzystanie z firmowej infrastruktury IT w celach prywatnych

Zabrania się korzystania z firmowej infrastruktury IT w celach prywatnych.

5.10. Naruszenie bezpieczeństwa

Wszelakie podejrzenia naruszenia bezpieczeństwa danych w Firmie należy zgłaszać w formie ustnej lub za pośrednictwem poczty elektronicznej do Zarządu Spółki.

Każdy incydent jest odnotowywany w stosownej bazie danych, a Zarząd Firmy podejmuje stosowne kroki zaradcze.

5.11. Podsumowanie obowiązków pracownika

5.11.1. Bezpieczeństwo informacji

1. Przestrzegaj Polityki dotyczącej informacji poufnych
2. Nie zapewniaj dostępu do informacji organizacji ani informacji o klientach bez uzasadnionej potrzeby biznesowej i zgody odpowiedzialnego właściciela. Postępuj zgodnie z wymaganiami i wytycznymi standardu klasyfikacji danych, aby zapewnić odpowiednią klasyfikację i ochronę danych.
3. Nie omijaj zabezpieczeń, ograniczeń ani żadnych innych środków bezpieczeństwa.
4. Nie udostępniaj poświadczeń konta użytkownika ani zalogowanych sesji innym osobom i zawsze uwierzytelniaj się przy użyciu przypisanych poświadczeń konta użytkownika. Nie należy zmieniać przeznaczenia ani synchronizować poświadczeń organizacji z kontami w witrynach innych firm.
5. Zachowaj bezpośrednią kontrolę nad urządzeniami firmowymi i osobistymi oraz blokuj lub zabezpieczaj urządzenia przez cały czas, gdy nie są używane. Postępuj zgodnie z wymaganiami dotyczącymi zapobiegania kradzieży, aby zapobiec kradzieży.

6. Zgłaszaj wszelkie podejrzane incydenty związane z danymi klientów organizacji (wewnętrznie, za pośrednictwem partnera lub dostawcy) tak szybko, jak to możliwe, postępując zgodnie z instrukcjami podanymi w sekcji Zgłoś teraz.
7. Upewnij się, że wszyscy niebędący pracownikami, tacy jak personel zewnętrzny (w tym wykonawcy, osoby zewnętrzne, goście służbowi i tymczasowi pracownicy agencji) są świadomi i przestrzegają wymagań niniejszej polityki.

5.11.2. Bezpieczeństwo fizyczne

1. Jeśli zasób lub urządzenie osobiste organizacji zawierające dane biznesowe organizacji zostanie zgubione lub skradzione, postępuj zgodnie z instrukcjami w sekcji Zgłoś to teraz tak szybko, jak to możliwe.
2. Zawsze wyświetlaj kartę dostępu w widoczny sposób przez cały czas przebywania w placówce organizacji. Upewnij się, że odwiedzający są zarejestrowani w recepcji organizacji. Zabroń wstępu każdemu, kto nie pokazuje karty dostępu, i odprowadź ją do najbliższego punktu kontaktowego - recepcji / ochrony.

5.11.3. Bezpieczeństwo cyfrowe

1. Aktualizuj oprogramowanie komputerowe. Postępuj zgodnie z wymaganiami polityk bezpieczeństwa, aby zachować bezpieczeństwo komputera.
2. Nie należy pobierać ani instalować niezaufanego, nielicencjonowanego, zabronionego lub nielegalnego oprogramowania na żadnym urządzeniu lub systemie, który uzyskuje dostęp do danych biznesowych lub usług organizacji.
3. Upewnij się, że urządzenia osobiste, które są używane do prowadzenia działalności organizacji, są aktualne i są zarejestrowane w systemie zarządzania urządzeniami.

5.11.4. Szkolenia i podnoszenie świadomości

1. Ukończ kursy wymagane dla pracowników w konkretnej roli i inne odpowiednie szkolenia jako nowy pracownik w terminie określonym przez zespół wdrażający.
2. Przeprowadzaj coroczne szkolenia w zakresie bezpieczeństwa, zatwierdzone kursy szkoleniowe oparte na rolach — zgodnie z zaleceniami i terminami określonymi przez

organizację. Kompletne szkolenie techniczne w zakresie bezpieczeństwa, zgodnie z wymaganiami organizacji.

5.11.5. Powiązane zasady

1. Oprócz tej polityki należy przestrzegać wymagań bezpieczeństwa i ochrony życia określonych przez grupę bezpieczeństwa odpowiedniej organizacji.
2. Pracownicy organizacji pełniący między innymi funkcje programistyczne, operacyjne, związane z zabezpieczeniami, zgodnością i inspekcją podczas tworzenia, konserwacji i/lub obsługi produktów muszą również przestrzegać odpowiednich zasad, standardów i wymagań inżynierskich.

5.11.6. Wyjątki

Zasady muszą być przestrzegane, a tam, gdzie nie są możliwe, należy dążyć do wyjątku i zatwierdzić go przez odpowiednią jednostkę zarządzającą. W zależności od zakresu wyjątku i potencjalnego ryzyka, jakie stanowi, wyjątki należy uzyskać od odpowiedniego kierownika.

5.11.7. Egzekwowanie przepisów

Naruszenie tej polityki może skutkować podjęciem działań dyscyplinarnych, włącznie z rozwiązaniem stosunku pracy lub umowy, stosownie do przypadku. Organizacja może przekazywać organom ścigania informacje dotyczące naruszenia zasad zabezpieczeń, które jest równoznaczne z potencjalnym przestępstwem.

6. Dokumentowanie bezpieczeństwa

Firma prowadzi dokumentacje w zakresie:

- obecnie wykorzystywanych metod zabezpieczeń systemów IT,
- budowy sieci IT,
- ewentualnych naruszeń bezpieczeństwa systemów IT,
- dostępów do zbiorów danych / systemów udzielonych pracownikom.

Wszelkie zmiany w obszarach objętych dokumentacją, uwzględniane są w tejże dokumentacji.

7. Dane osobowe

Szczegółowe wytyczne dotyczące przetwarzania danych osobowych powinny być zawarte w odrębnym dokumencie dotyczącym polityki ochrony danych osobowych w jednostce.

8. Załącznik 1 – Metodyki analizy ryzyka

8.1. Ogólne metodyki

Brak ustalonych metodyk. Rekomendowane oparcie się na:

- ISO/IEC 27005:2018 - Information technology - Security techniques - Information security risk management
- NIST SP 800-30 Rev. 1 - Guide for Conducting Risk Assessments
- OCTAVE Allegro - Operationally Critical Threat, Asset and Vulnerability Evaluation
- NSC 800-30 Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne

Dodatkowe informacje znajdują się na stronie https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber

8.2. Metodyki dla usług z chmury publicznej

W związku z brakiem możliwości wykorzystania audytów w centach przetwarzania wykorzystywanych usług chmury publicznej, analizę ryzyka oparto o wyniki audytów uznanych podmiotów niezależnych oraz posiadane aktualne certyfikacje dostawcy komponentów chmury publicznej.

1. Przyjęto konieczność posiadania dla komponentów chmury publicznej posiadanie powszechnie uznanych i rozpowszechnionych standardów i norm potwierdzonych aktualnymi wynikami niezależnych audytów, oraz list kontrolnych w szczególności:
   a) PN-ISO/IEC
      i. 27001,
      ii. 27002,
      iii. 27017,
      iv. 27018,
      v. 20000-1:2011,
      vi. 22301,
   b) SOC 1, SOC 2, SOC 3,
   c) Open Authentication Standard – OAuth,

d) CIS Benchmark.

2. Zgodność algorytmów zabezpieczających dane usług platformy hostowanej Dostawcy z FIPS 140.
3. Komponenty chmury publicznej muszą zapewniać lub umożliwiać zapewnienie:
   a) Dostępność usług na poziomie 99,9% (lub wyższym),
   b) Dostępność mechanizmów pełnej rozliczalności działań użytkowników w usługach,
   c) Dostępność na żądanie wyników aktualnych audytów, w tym audytów bezpieczeństwa, dla usług i centrów przetwarzania danych oferujących te usługi i audytów związanych z certyfikatami ISO posiadanymi przez Dostawcę,
   d) Możliwość automatycznej, niewpływającej na ciągłość pracy systemów instalacji poprawek dla wybranych składników pakietów usług,
   e) Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego,
   f) Możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi zarządzania tożsamością będącej składową pakietów usług oferowanych przez Dostawcę,
   g) Możliwość realizacji bezpiecznego uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory,
   h) Dostępność mechanizmu uwierzytelnienia wieloskładnikowego,
   i) Dostępność logów informujących o wszystkich zdarzeniach uwierzytelnienia do usług i danych Zamawiającego, zakończonych powodzeniem lub niepowodzeniem oraz prób uwierzytelnienia przy pomocy tożsamości będących na listach „wykradzione”,
   j) Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych,
   k) Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN),
   l) Możliwość zestawienia dedykowanego połączenia pomiędzy lokalną infrastrukturą sprzętową Zamawiającego, a Centrami przetwarzania Dostawcy,

m) Możliwość korzystania w ramach pakietów usług Dostawcy z dedykowanych urządzeń typu HSM zgodnych z FIPS 140-2 poziomu 3,
n) Wbudowane w platformę Dostawcy mechanizmy zabezpieczające przez atakami DDoS,
o) Możliwość zastrzeżenia miejsca uruchomienia usług i składowania danych w usłudze do terytorium krajów Europejskiego Obszaru Gospodarczego (EOG),
p) Możliwość korzystania z przynajmniej dwóch równorzędnych centrów przetwarzania danych Dostawcy, składających się z przynajmniej trzech redundantnych ośrodków przetwarzania i położonych na obszarze EOG,
q) Dostępność zapisów umownych Dostawcy zawierających tzw. Klauzule Umowne opublikowane przez Komisję Europejską w zakresie ochrony danych osobowych,
r) Zobowiązania umowne Dostawcy potwierdzające zgodność z rozp. RODO i potwierdzające rolę Dostawcy jako przetwarzającego dane,
s) Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego,
t) Gwarancję usunięcia danych Zamawiającego z usług i centrów przetwarzania Dostawcy po zakończeniu umowy,
u) Gwarancję braku dostępu do danych Zamawiającego przez Dostawcę, z wyłączeniem działań serwisowych i wykonywanych wyłącznie przez uprawnione osoby z organizacji Dostawcy.

4. Wykorzystanie wspólnych i jednolitych procedur masowej instalacji, aktywacji, uaktualniania, zarządzania, monitorowania i wsparcia technicznego oraz jednolitych mechanizmów wykorzystania tożsamości cyfrowej, zapewnionych przez Dostawcę.
5. Możliwość wyłączenia konta organizacji na spersonalizowanej stronie Dostawcy i usunięcie danych Zamawiającego z centrów przetwarzania Dostawcy.
6. Obronę organizacji z tytułu roszczeń strony trzeciej o naruszenie przez oferowany Produkt prawa autorskiego w przypadku niezwłocznego powiadomienia Dostawcy o roszczeniu odszkodowawczym.

8.3. Metodyki dla informacji niejawnych

- DBBT-811.2 – Metodologia szacowania ryzyka dla systemów teleinformatycznych przetwarzających informacje niejawne[1]
- ZIBT-818A – Zalecenia w zakresie zarządzania ryzykiem bezpieczeństwa teleinformatycznego[1]

9. Załącznik 2 – Lista aktów prawnych

A. Obwieszczenie Prezesa Rady Ministrów z dnia 9 listopada 2017 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017 poz. 2247).

B. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony danych osobowych (RODO).

C. Dyrektywa Parlamentu Europejskiego I Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (NIS)

D. Wymagania dotyczące bezpieczeństwa zawarte w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (eIDAS).

E. Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 10 marca 2023 r. w sprawie ogłoszenia jednolitego tekstu ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U. 2023 poz. 913) – na dzień publikacji poradnika jest procedowana nowelizacja ustawy, której projekt został przyjęty przez Radę Ministrów 7 czerwca 2023 roku.

F. Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. poz. 2180).

G. Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. poz. 2080).

H. Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie wzoru formularza do przekazywania informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych, które miało istotny wpływ na funkcjonowanie sieci lub usług (Dz. U. poz. 1831)

I. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024.
J. Akt o cyberbezpieczeństwie (Cybersecurity Act), który jest ogólnoeuropejską regulacją w zakresie cyberbezpieczeństwa i reguluje m.in. obszar certyfikacji cyberbezpieczeństwa.

Dodatkowo należy uwzględnić wdrożenie zasad zgodnych z dyrektywą NIS2, czyli:

1. Rozszerzenie zakresu podmiotów objętych dyrektywą na nowe sektory i usługi cyfrowe, takie jak chmura obliczeniowa, platformy społecznościowe czy usługi streamingowe,
2. Podział podmiotów na kluczowe i ważne, które podlegają tym samym wymogom zarządzania cyberbezpieczeństwem i obowiązkowi zgłaszania incydentów,
3. Zwiększenie kar za naruszenie przepisów dyrektywy do 10 milionów euro lub 2% rocznego obrotu,
4. Wprowadzenie minimalnych standardów bezpieczeństwa dla produktów i usług cyfrowych oraz systemu certyfikacji cyberbezpieczeństwa.

10. Załącznik 3 - Procedura zgłaszania incydentów do CSIRT

W przypadku wykrycia incydentu należy:

- zarejestrować incydent,
- przeanalizować incydent,
- dokonać klasyfikacji incydentu,
- dokonać zgłoszenia incydentu,
- podjąć działania eliminujące przyczyny i skutki incydentu.

10.1. Klasyfikacja incydentu

W celu klasyfikacji incydentu, należy zastosować procedury określone w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 poz. 1560).
https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20230000913
Jak również określone w Rozporządzeniu Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny: https://www.dziennikustaw.gov.pl/D2018000218001.pdf

10.2. Zgłoszenie incydentu

Aby zgodnie z obowiązującym prawem zgłosić incydent należy:

1. Ustalić właściwy CSIRT (Computer Security Incident Response Team, czyli Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego) dla organizacji,
2. Zgłosić osobę kontaktową organizacji do CSIRT,
3. Używać szyfrowania przesyłek w kontaktach mailowych z CSIRT,
4. Zgłaszać niezwłocznie incydenty do CSIRT za pośrednictwem podanego przez CSIRT serwisu - wypełnić formularz zgłoszenia incydentu poważnego i przesłać go na adres odpowiedniego CSIRT.

Aby skontaktować się z CSIRT GOV, można:

1. Wysłać e-mail na incydent@csirt.gov.pl z użyciem klucza publicznego PGP dostępnego na stronie www.csirt.gov.pl w zakładce „Klucz PGP”,
2. Zadzwonić do Dyżurnego CSIRT GOV pod numerem: +48 22 58 59 373,
3. Wypełnić formularz zgłoszenia incydentu dostępny na stronie www.csirt.gov.pl w zakładce „Zgłoszenie incydentu do CSIRT GOV”.

Aby skontaktować się z CSIRT NASK, można:

1. Wysłać e-mail na adres cert@cert.pl z użyciem klucza publicznego PGP dostępnego na stronie https://cert.pl/kontakt/pl po naciśnięciu przycisku „Przejdź” pod napisem „Obowiązujące klucze publiczne PGP CERT Polska:”,
2. Zadzwonić do Dyżurnego w CSIRT NASK pod numerem: +48 22 380 82 74,
3. Wypełnić formularz zgłoszenia incydentu dostępny na stronie https://incydent.cert.pl.

Aby skontaktować się z CSIRT MON, można:

1. Wysłać e-mail na adres csirt-mon@ron.mil.pl z użyciem klucza publicznego PGP dostępnego na stronie https://csirt-mon.wp.mil.pl/pl/pages/klucz-pgp-csirt-mon/
2. Zadzwonić do Dyżurnego w CSIRT MON pod numerem: +48 261 865 333,

10.3. Lista CSIRT i podmiotów zgłaszających incydenty

CSIRT NASK:

- jednostki samorządu terytorialnego
- jednostki podległe organom administracji rządowej (poza jednostkami podległymi Prezesowi Rady Ministrów)
- jednostki budżetowe, samorządowe zakłady budżetowe
- agencje wykonawcze, instytucje gospodarki budżetowej
- uczelnie publiczne i Polska Akademia Nauk

- Urząd Dozoru Technicznego, Polską Agencję Żeglugi Powietrznej, Polskie Centrum Akredytacji
- Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej
- spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej, których celem jest bieżące i nieprzerwane zaspokajanie zbiorowych potrzeb obywateli
- obywatele.

CSIRT GOV:

- organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały (poza samorządami
- jednostki podległe Prezesowi Rady Ministrów lub przez niego nadzorowane
- ZUS, KRUS, NFZ
- Narodowy Bank Polski, Bank Gospodarstwa Krajowego
- Infrastruktura Krytyczna.

CSIRT MON:

- podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej
- przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, w stosunku do których organem organizującym wykonywanie zadań na rzecz obronności państwa jest Minister Obrony Narodowej.
- podmioty świadczące usługi opisane w art 648. Ustawy z dnia 11 marca 2022 r. o obronie ojczyzny (Dz. U. poz. 655) na rzecz Sił Zbrojnych

11. Załącznik 4 - Definicje

Anonimizacja - działanie uniemożliwiające identyfikację osoby fizycznej.

Atak DDoS (Distributed Denial of Service) – atak poprzez przeciążenie serwera docelowy ogromną liczbą żądań wysyłanych z wielu urządzeń, przez co niemożliwe jest korzystanie z usługi przez uzytkowników.

Atak na DNS – zmiana adresacji pozwalająca na użycie nazwy dowolnej popularnej witryny internetowej w celu przekierowania ruchu na inny adres IP.

Backdoor - luka w budowie oprogramowania pozwalająca na nieuprawnione działania.

Backup - kopia zapasowa danych lub systemów umożliwiająca odtworzenie utraconych lub uszkodzonych danych lub systemów.

Botnet - grupa kontrolowanych zdalnie urządzeń, które zainfekowano szkodliwym oprogramowaniem.

Brute-force attack – atak polegający na losowym wprowadzaniu danych logowania tak długo, aż złamie zabezpieczenia.

Doxing - gromadzenie i analiza danych oraz śladów pozostawionych przez użytkownika w sieci w celu udostępnienia pozyskanych informacji.

Exploit zero-day - oprogramowanie, które pojawia się przed naniesieniem poprawek przez producenta oprogramowania lub sprzętu.

Hacking - próba włamania się do urządzenia lub sieci, której celem są nieuprawnione działania.

Honeypot - pułapka przygotowana z myślą o cyberprzestępcach.

Incydent bezpieczeństwa - jest to pojedyncze zdarzenie lub seria zdarzeń, związanych z bezpieczeństwem informacji, które zagrażają ich poufności, dostępności, integralności lub dostępności.

Keylogger - oprogramowanie rejestrujące ruchy myszką oraz naciśnięcia klawiszy na klawiaturze lub ekranie.

Konie trojańskie - oprogramowanie, które w tle wykonują działania szkodliwe z punktu widzenia użytkownika lub organizacji.

Malicious software (Malware) - złośliwe oprogramowanie, dzięki któremu możliwy jest dostęp do urządzenia bez wiedzy użytkownika.

Phishing - nakłonienie użytkownika do dobrowolnego podania poufnych danych.

Ransomware - złośliwe oprogramowanie, przejmujące kontrolę nad urządzeniem, blokujące dostęp do niego lub szyfrujące dane.

Shadow IT – korzystanie z zasobów IT organizacji w celach prywatnych, lub wykorzystywanie oprogramowania czy usług niezatwierdzonych przez dział IT lub pracodawcę.

VPN - wirtualna sieć prywatna zabezpieczająca przed przechwyceniem danych w trakcie ich transmisji.

Wyciek danych - celowe lub przypadkowe udostępnienie wrażliwych informacji osobom nieuprawnionym wewnątrz i na zewnątrz organizacji.

Zero trust - koncepcja Zero Trust opiera się na założeniu, że w kwestii bezpieczeństwa IT nie ma bezpiecznych rozwiązań, procesów i zaufanych użytkowników.