Fundamentalne wytyczne

w zakresie ochrony przed cyberatakami

csirt
Centrum e-Zdrowia

cez Centrum e-Zdrowia

Spis treści

Cyberbezpieczeństwo stanowi bezustanny proces, a nie jednorazowe działanie. Regularne wdrażanie najlepszych praktyk w zakresie cyberbezpieczeństwa jest kluczowym elementem skutecznej obrony przed cyberzagrożeniami.

Zapoznaj się z podstawowymi wymaganiami, które pomogą podnieść poziom cyberbezpieczeństwa. Stosowanie się do nich pozwoli zminimalizować ryzyko utraty danych, zakłóceń w działaniu systemów oraz poniesienia strat finansowych.

01. Tworzenie, przechowywanie i testowanie kopii zapasowych

- Sporządź wykaz wszystkich baz danych, repozytoriów plików oraz plików konfiguracyjnych aplikacji, aby mieć pełną świadomość zasobów, które należy regularnie archiwizować.
- Upewnij się, że kopie zapasowe powstają wystarczająco często, aby minimalizować utratę danych. Dobierz częstotliwość ich tworzenia do poziomu krytyczności każdego systemu (np. codziennie, co godzinę).
- Przechowuj kopie w różnych miejscach, np. w chmurze oraz offline na dyskach fizycznie odłączonych od sieci, aby zapewnić wielopoziomową ochronę i uniknąć ryzyka utraty danych w przypadku ataku lub awarii.
- Regularnie sprawdzaj, czy odzyskiwanie danych działa prawidłowo, wykonując testowe przywracanie plików, aby zweryfikować integralność oraz użyteczność kopii zapasowych.
- Zabezpieczaj backupy hasłem lub kluczem, dzięki czemu nieuprawnione osoby nie będą mogły odczytać zawartości archiwizowanych danych.
- Nie korzystaj z tych samych poświadczeń dla kopii oraz innych systemów (np. Active Directory), aby zminimalizować ryzyko przejęcia dostępu do backupów w wyniku naruszeń bezpieczeństwa.
- Ogranicz liczbę osób z prawami do tworzenia, kasowania i odtwarzania kopii zapasowych, przydzielając uprawnienia wyłącznie pracownikom, którzy rzeczywiście powinni zarządzać kopiami.
- Zdefiniuj, jak długo i w jakiej formie przechowywane są kopie. Jest to szczególnie istotne podczas audytów oraz analizowania potencjalnych incydentów bezpieczeństwa.
- Twórz szczegółowy rejestr wszystkich operacji wykonywanych na kopiach zapasowych (kto, kiedy i dlaczego wykonał daną czynność), aby móc wyjaśnić ewentualne nieprawidłowości.

02. Zarządzanie poprawkami systemowymi i aplikacjami

- Korzystaj z systemów automatycznej aktualizacji, aby na bieżąco wykrywać oraz instalować poprawki w systemach i aplikacjach, skracając czas ekspozycji na potencjalne luki.
- Ustalaj priorytet podejmowanych działań ze względu na luki bezpieczeństwa, skupiając się w pierwszej kolejności na tych krytycznych (o wysokim CVSS), które mogą umożliwić zdalne wykonanie kodu lub eskalację uprawnień.
- Weryfikuj wersje oprogramowania na wszystkich urządzeniach, łącznie z IT/OT/IoT czy systemami SCADA, tak aby każde z nich posiadało najnowsze poprawki bezpieczeństwa.
- Określ stałe „okna czasowe" na instalowanie aktualizacji, np. raz w tygodniu lub raz w miesiącu, i sprawdzaj, czy ich wdrożenia przebiegają zgodnie z założeniami.
- Przygotuj procedurę wycofania wadliwych aktualizacji, aby móc szybko powrócić do poprzednich wersji w razie problemów ze stabilnością systemu.
- Utwórz środowisko testowe, gdzie najpierw wdrażane są poprawki i zmiany konfiguracji, aby ocenić ich wpływ na kluczowe systemy przed wprowadzeniem do środowiska produkcyjnego.
- Integruj informacje o lukach i poprawkach z dedykowanych baz (np. CVE, NVD) bezpośrednio w systemie do zarządzania poprawkami, by automatycznie identyfikować istotne aktualizacje.
- Korzystaj z narzędzi do inwentaryzacji oprogramowania (Software Asset Management), aby mieć pewność, że wszystkie urządzenia w organizacji zostały objęte procesem wdrażania poprawek.

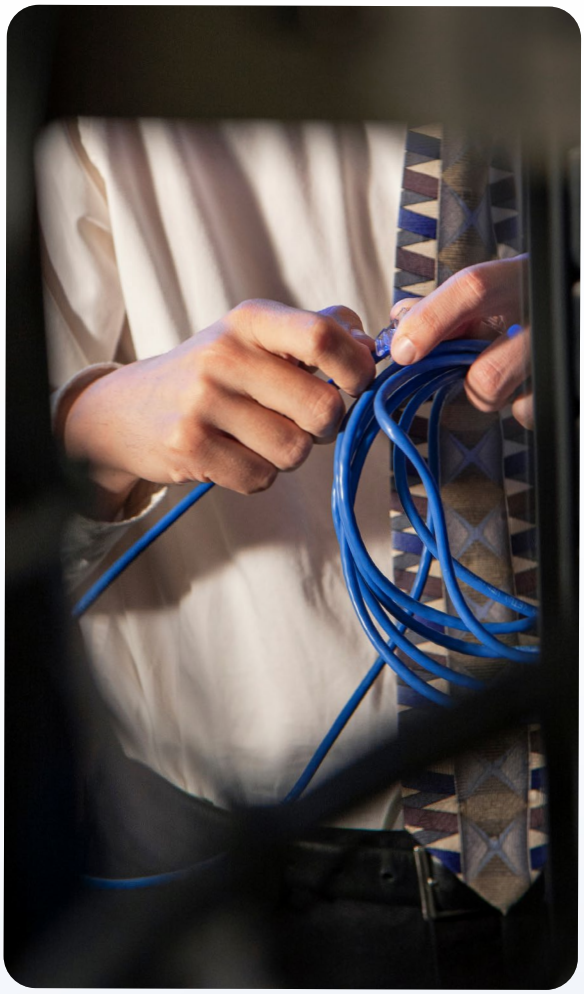
03. Kontrola dostępu i zarządzanie tożsamością

- Stosuj zasadę „najmniejszych uprawnień" (least privilege) oraz strategię Zero Trust, udzielając pracownikom wyłącznie tych uprawnień, które są absolutnie niezbędne do wykonywania ich obowiązków. Za każdym razem weryfikuj żądania, w myśl zasady „nigdy nie ufaj, zawsze weryfikuj".
- Wdrażaj uwierzytelnianie wieloskładnikowe (MFA), np. przez tokeny sprzętowe lub aplikacje mobilne, zwłaszcza w systemach krytycznych.
- Wymuszaj stosowanie silnej polityki haseł, w tym odpowiednią ich długość, złożoność, limity prób logowania i cykliczną rotację haseł w ustalonych odstępach czasu.
- Przeprowadzaj cykliczne rewizje kont i uprawnień, zwłaszcza po odejściu pracownika z organizacji, aby wyeliminować zbędne lub zapomniane konta.

- Monitoruj i rejestruj logowania, zwracając szczególną uwagę na nietypowe pory oraz lokalizacje, aby szybko wykrywać podejrzaną aktywność i na nią reagować.

- Prowadź cykliczne weryfikacje uprawnień, podczas których przełożeni sprawdzają, czy danemu użytkownikowi w dalszym ciągu potrzebne są dotychczasowe poziomy dostępu.

- Stosuj „segregację obowiązków" w przypadku najbardziej krytycznych operacji, tak aby wymagały zgody lub współdziałania co najmniej dwóch uprawnionych osób.



04. Bezpieczeństwo stacji roboczych, serwerów i urządzeń końcowych

- Wdrażaj rozwiązania umożliwiające przygotowywanie, konfigurację i wycofywanie stacji roboczych, co zapewni spójne wdrażanie polityk bezpieczeństwa (np. GPO) od pierwszego uruchomienia systemu.

- Korzystaj z oprogramowania antywirusowego oraz antimalware za pomocą rozwiązań takich jak NGAV (Next-Gen AV) czy EDR (Endpoint Detection and Response).

- Wdrażaj politykę „Application Whitelisting", umożliwiając uruchamianie jedynie zaufanych i podpisanych plików wykonywalnych.

- Zapewniaj regularne oraz cykliczne skanowanie stacji roboczych i serwerów, aby wykrywać ewentualne zagrożenia w możliwie najszybszym czasie.

- Konfiguruj firewalle osobiste (lokalne zapory systemowe), m.in. takie, jak w systemie Windows, i dbaj o ich właściwe ustawienia zgodne z polityką bezpieczeństwa.

- Rozważ zablokowanie portów USB i nośników wymiennych dla stacji roboczych, stosując kontrolę nośników w celu zapobiegania nieautoryzowanemu kopiowaniu danych lub wprowadzaniu złośliwego oprogramowania.

- Dokonuj tzw. twardej konfiguracji (hardeningu), wyłączając zbędne usługi oraz protokoły (np. Telnet, SMBv1).

- Korzystaj z pełnego szyfrowania dysków, np. BitLocker (Windows) lub LUKS (Linux), zwłaszcza na urządzeniach mobilnych i laptopach, aby chronić dane w razie utraty sprzętu.
- Instaluj wyłącznie niezbędne oprogramowanie, minimalizując w ten sposób wektory ataku.
- Wdrażaj regularne restarty systemów, ponieważ niektóre poprawki i zmiany w konfiguracji wymagają ponownego uruchomienia, co należy egzekwować zgodnie z ustalonym harmonogramem.
- Ogranicz dostęp do portów zewnętrznych, np. RDP, SSH czy SMB, jedynie do zaufanych adresów IP, kiedy nie są one potrzebne w szerszym zakresie.

05. Segmentacja sieci

- Wydziel strefy sieciowe, aby krytyczne zasoby (np. serwery bazodanowe, systemy szpitalne) były oddzielone od stref ogólnodostępnych w ramach sieci.
- Umieszczaj usługi publiczne w strefie DMZ, zapewniając izolację ruchu między DMZ a siecią wewnętrzną oraz ograniczając ekspozycję wewnętrznych zasobów.
- Stosuj listy kontroli dostępu (ACL) na routerach i przełącznikach w celu blokowania ruchu między segmentami, który nie jest niezbędny dla działania organizacji.
- Wdrażaj IDS/IPS do monitorowania ruchu sieciowego, aby w czasie rzeczywistym wykrywać i blokować potencjalne ataki.
- Korzystaj z wirtualnych sieci VLAN, gdy tylko jest to możliwe, w celu dodatkowego logicznego podziału ruchu sieciowego na poziomie infrastruktury fizycznej.

06. Ochrona poczty elektronicznej

- Korzystaj z systemów antyspamowych i antyphishingowych, aby skutecznie blokować podejrzane wiadomości oraz szkodliwe załączniki (np. .exe, .js).
- Konfiguruj mechanizmy SPF, DKIM i DMARC, zmniejszając ryzyko podszywania się pod adresy firmowe w korespondencji e-mail.
- Regularnie edukuj użytkowników, przypominając im, by nie otwierali linków i załączników otrzymanych z nieznanych źródeł.
- Wdrażaj „sandboxing” przy analizie załączników, aby przed dostarczeniem do użytkownika sprawdzić, czy plik nie zawiera złośliwego kodu.
- Rozważ wprowadzenie szyfrowania poczty (np. S/MIME, PGP) w przypadku przesyłania danych o podwyższonym poziomie wrażliwości, aby uniemożliwić przechwycenie treści przez osoby nieuprawnione.

- Monitoruj i analizuj raporty logów serwera poczty (np. informacje o odrzuconych i podejrzanych wiadomościach), co pozwoli wykryć nietypowe wzorce ruchu i próby ataku.

- Włącz opcję skanowania załączników w czasie rzeczywistym na bramkach e-mail, aby zapewnić dodatkową warstwę ochrony przed nowym i nieznanym złośliwym oprogramowaniem.

07. Monitoring i gromadzenie logów

- Centralizuj logi za pomocą systemu SIEM, zbierając dane z serwerów, urządzeń sieciowych, aplikacji i systemów operacyjnych w jednym miejscu do korelacji zdarzeń.

- Definiuj alerty na niepokojące zachowania, np. powtarzające się nieudane próby logowania czy gwałtowny wzrost wykorzystania zasobów.

- Wykorzystuj User and Entity Behavior Analytics (UEBA), aby wykrywać odstępstwa od typowych zachowań użytkowników lub urządzeń i w porę reagować na anomalie.

- Konfiguruj poziom logowania w taki sposób, by obejmował również zdarzenia związane z dostępem do plików czy zmianami w rejestrze systemowym.

- Regularnie przeglądaj starsze zapisy zdarzeń w logach, ponieważ cyberprzestępcy często działają w ukryciu przez dłuższy czas. Wczesne ślady nieautoryzowanej aktywności mogą ujawnić się dopiero po analizie zdarzeń sprzed kilku tygodni czy nawet miesięcy.

08. Procedury reagowania na incydenty

- Stwórz i aktualizuj plan postępowania na wypadek incydentu, który krok po kroku opisze działania konieczne do ograniczenia szkód.
- Określ role i odpowiedzialności w jednostce ds. incydentów, rozdzielając zadania związane z zarządzaniem sytuacją kryzysową, komunikacją z zarządem i organami ścigania.
- Przygotuj gotowe szablony powiadomień, które pozwolą szybko poinformować pracowników, partnerów oraz klientów (zwłaszcza jeśli naruszenie dotyczy danych osobowych).
- Organizuj ćwiczenia scenariuszowe, aby personel dokładnie wiedział, jak zareagować w razie ataku, oraz aby zweryfikować skuteczność przyjętych procedur.
- Opracuj plan odtworzenia kluczowych systemów, określając priorytety przywracania, co skróci przestój i zminimalizuje straty.
- Upewnij się, że procedury zgłaszania nietypowej aktywności są czytelne dla wszystkich pracowników, aby nikt nie miał wątpliwości, do kogo należy się zwrócić w razie podejrzenia incydentu.
- Wprowadź zasadę gwarantującą, że osoba zgłaszająca potencjalne naruszenie nie zostanie ukarana za niedopełnienie obowiązków, co sprzyja otwartej i szybkiej wymianie informacji.
- Zapewnij łatwe kanały zgłaszania incydentów, takie jak dedykowany nr. telefonu czy adres e-mail do SOC lub działu IT.

09. Polityka bezpieczeństwa i zgodność (compliance)

- Wdrażaj i utrzymuj System Zarządzania Bezpieczeństwem Informacji (SZBI), który będzie stanowił formalną podstawę do kompleksowego zarządzania ryzykiem, procedurami oraz wymaganiami prawnymi w obszarze bezpieczeństwa informacji.
- Zapewnij jasne, spisane polityki i regulaminy, które regulują między innymi zasady dostępu do systemów oraz korzystania z urządzeń służbowych.
- Regularnie przeprowadzaj audyty zgodności, by weryfikować, czy organizacja przestrzega RODO, ISO 27001, i innych norm oraz wytycznych.

- Przygotuj plan zgłaszania naruszeń do organów regulacyjnych (np. UODO) w sytuacjach, w których przepisy prawa nakładają taki obowiązek.

- Dokumentuj wszystkie procesy związane z bezpieczeństwem, co ułatwi analizę incydentów, doskonalenie procedur oraz przeprowadzanie audytów.

10. Ograniczanie ryzyka związanego z użyciem makr i skryptów

- Ustal politykę domyślnej blokady makr w Office, np. za pomocą reguł GPO lub Intune dotyczącą plików pobranych z internetu.

- Dopuszczaj wyłącznie skrypty podpisane cyfrowo, aby mieć pewność, że ich źródło jest zweryfikowane i zaufane.

- Regularnie uświadamiaj użytkowników, że makra mogą zawierać złośliwy kod, a otwieranie plików z niezaufanego źródła jest poważnym zagrożeniem.

- Zbieraj logi i analizuj uruchomienia makr, by wiedzieć, który użytkownik, kiedy i w jakim celu uruchomił makro, co może pomóc w wykryciu anomalii.

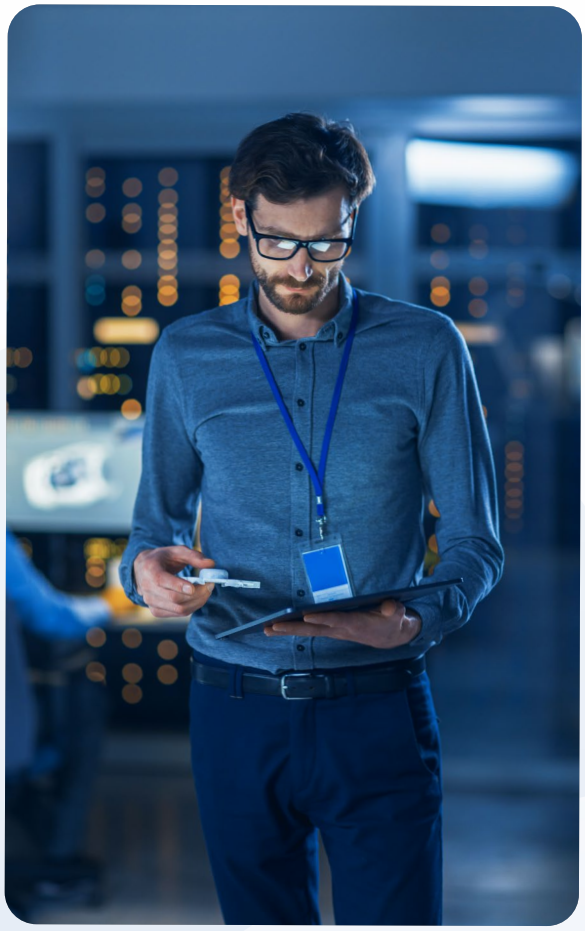
- Wdrażaj narzędzia sandbox w czasie rzeczywistym, które automatycznie uruchamiają i analizują makra w izolowanym środowisku przed ich udostępnieniem użytkownikowi.

- Korzystaj z systemów reputacji plików, które na bieżąco porównują hashe makr i skryptów z bazami znanego złośliwego oprogramowania.

11. Bezpieczeństwo dostępu zdalnego i połączeń VPN

- Wdrażaj wyłącznie szyfrowane połączenia TLS lub IPsec, aby zapewnić ochronę przesyłanych danych przed podsłuchem w internecie.

- Wymagaj uwierzytelniania wieloskładnikowego (MFA) dla sesji VPN i zdalnego pulpitu (RDP), co znacząco podniesie poziom bezpieczeństwa.



- Ogranicz lub całkowicie wyłącz bezpośredni dostęp RDP z internetu, jeśli nie jest on niezbędny, bądź ogranicz go do zaufanych adresów IP, stosując dedykowaną bramę RDP.
- Monitoruj aktywność w kanałach zdalnego dostępu, kontrolując łączny czas sesji i zwracając uwagę na nietypowe próby łączenia w godzinach poza pracą.
- Stosuj segmentację dla zdalnych połączeń, aby także użytkownicy korzystający z VPN mieli dostęp wyłącznie do niezbędnych części sieci.
- Stosuj autoryzację opartą na certyfikatach dla użytkowników i urządzeń, co umożliwia lepszą weryfikację tożsamości.

12. Testy penetracyjne i audyty bezpieczeństwa

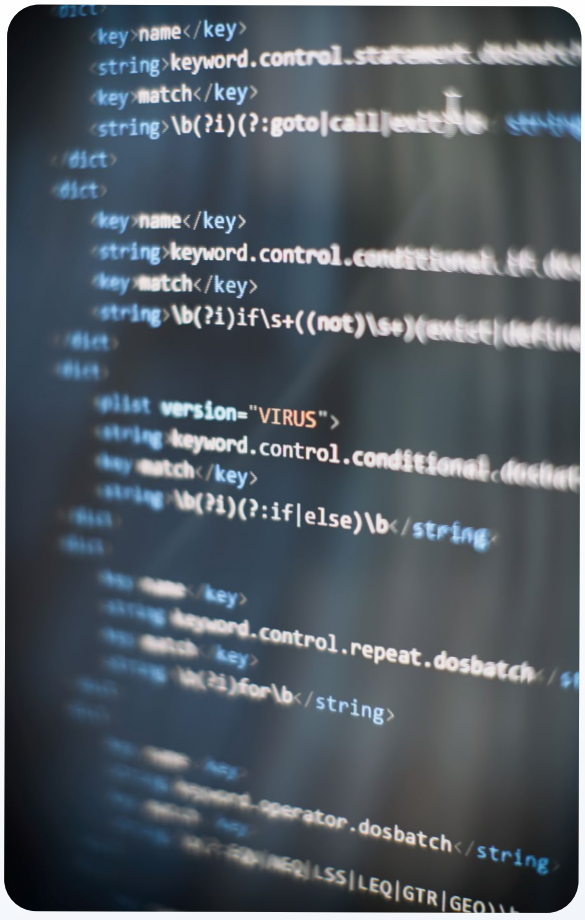
- Zlecaj testy penetracyjne zarówno wewnętrzne, jak i zewnętrzne, by sprawdzić możliwość ataku z perspektywy internetu oraz osoby znajdującej się w sieci lokalnej.
- Precyzyjnie określ zakres testów, uwzględniając w nim kluczowe systemy i usługi narażone na ataki.
- Realizuj testy co najmniej raz w roku lub po znaczących zmianach w infrastrukturze, aby zapewnić aktualną ocenę stanu bezpieczeństwa.
- Opracowuj raporty z wynikami oraz wdrażaj zalecane poprawki, wyznaczając konkretne terminy dla poszczególnych działań.
- Regularnie przeprowadzaj audyty konfiguracji urządzeń sieciowych, serwerów i narzędzi bezpieczeństwa, aby potwierdzić, że działają one zgodnie z założeniami i najnowszymi praktykami.

13. Zarządzanie urządzeniami mobilnymi (MDM)

- Konfiguruj profile bezpieczeństwa, wprowadzając wymóg silnych haseł, blokady ekranu czy szyfrowania, aby chronić dane przechowywane na urządzeniach mobilnych.
- Zapewnij możliwość zdalnego wymazania danych, aby w razie kradzieży lub zgubienia urządzenia mieć możliwość natychmiastowego usunięcia danych służbowych.
- Kontroluj instalację aplikacji, dopuszczając wyłącznie wcześniej zatwierdzone rozwiązania.
- Rozdziel dane prywatne i firmowe, by ograniczyć ryzyko wycieku informacji służbowych.
- Monitoruj, czy urządzenia mobilne mają zainstalowane aktualne poprawki bezpieczeństwa, by ograniczyć podatność na złośliwe oprogramowanie i ataki sieciowe.
- Blokuj możliwość rootowania/jailbreaku na urządzeniach służbowych i wykrywaj próby takiej modyfikacji, co pozwoli uniknąć obejścia krytycznych zabezpieczeń.

14. Kontrola wymiany danych z podmiotami trzecimi

- Wydziel strefę do wymiany danych (np. w osobnej sieci), by zminimalizować ryzyko rozprzestrzenienia się ataku w głównej infrastrukturze.
- Stosuj wyłącznie szyfrowane kanały komunikacji, takie jak SFTP czy HTTPS, przy przesyłaniu wrażliwych informacji na zewnątrz organizacji.
- Regularnie audytuj dostawców i partnerów, sprawdzając, jakie zabezpieczenia stosują, zwłaszcza jeśli mają dostęp do zasobów o krytycznym znaczeniu.



- Ustal standardy i procedury bezpieczeństwa w umowach (SLA), wyraźnie określając zasady zgłaszania incydentów oraz zakres odpowiedzialności stron.
- Udostępniaj tylko niezbędny zakres informacji, ograniczając się do niezbędnych danych dla danej współpracy.
- Precyzyjnie określ w umowach zakres uprawnień dostępu (np. rodzaj i czas obowiązywania) do zasobów, ograniczając sytuacje, w których partnerzy czy dostawcy posiadają więcej uprawnień, niż to konieczne.

15. System zarządzania ryzykiem

- Włącz do strategii zarządzania ryzykiem regularne prenumerowanie alertów i raportów (np. z CERT Polska), aby na bieżąco uzyskiwać informacje o pojawiających się zagrożeniach i metodach ataku.
- Współpracuj z zewnętrznymi organizacjami specjalizującymi się w analizie zagrożeń cybernetycznych, aby stale uzupełniać ocenę ryzyka o wiedzę na temat najnowszych wektorów ataków.
- Aktualizuj zasady i procedury bezpieczeństwa, takie jak reguły filtrów pocztowych, konfiguracja IDS/IPS czy definicje antywirusa, w oparciu o zidentyfikowane zagrożenia i podatności.

- Gromadź i analizuj wskaźniki kompromitacji (IOC), w tym adresy IP, domeny czy sumy kontrolne złośliwych plików, aby móc uwzględniać w analizie ryzyka konkretne kampanie i ataki.

16. Ograniczanie nieautoryzowanych rozwiązań IT (Shadow IT)

- Monitoruj ruch sieciowy, aby wykryć korzystanie z aplikacji SaaS lub narzędzi, które nie zostały oficjalnie zatwierdzone przez dział IT.
- Wdrażaj politykę instalowania oprogramowania wyłącznie z zaufanych źródeł, takich jak: centralne repozytoria lub oficjalne sklepy.
- Blokuj instalacje oprogramowania z zewnętrznych źródeł, spoza firmowego repozytorium czy oficjalnych sklepów, co znacznie ograniczy ryzyko pobierania niezweryfikowanych aplikacji.
- Utwórz transparentny proces zatwierdzania nowych narzędzi, by pracownicy mogli łatwo zgłosić potrzebę korzystania z dodatkowych rozwiązań i uzyskać ocenę ryzyka.
- Edukuj zespół, uświadamiając, że niezautoryzowane aplikacje stanowią istotne zagrożenie dla bezpieczeństwa infrastruktury oraz informacji.

17. Bezpieczna konfiguracja usług chmurowych

- Stosuj zasadę najmniejszych uprawnień w ramach ról i polityk IAM (np. w AWS, Azure), tak by przyznawany dostęp był jak najwęższy.
- Wymuś szyfrowanie danych w spoczynku i w trakcie przesyłania, aby zabezpieczyć je przed nieautoryzowanym odczytem.
- Monitoruj usługi chmurowe, korzystając z takich narzędzi jak AWS CloudTrail, Azure Monitor czy Google Cloud Logging, i analizuj logi pod kątem potencjalnych anomalii.
- Przeprowadzaj regularne audyty konfiguracji (np. AWS Config, Azure Security Center), aby wykryć nieprawidłową konfigurację oraz otwarte porty.
- Rozważ wdrożenie rozwiązań CSPM (Cloud Security Posture Management), które automatycznie identyfikują i korygują niebezpieczne konfiguracje w środowisku chmurowym.

18. Zabezpieczenia fizyczne

- Stosuj kontrolę dostępu do serwerowni, opartą na systemach kart, monitoringu CCTV oraz rejestrze wejść i wyjść, aby ograniczyć ryzyko nieuprawnionego dostępu.

- Zapewnij odpowiednie warunki środowiskowe, takie jak klimatyzacja, czujniki dymu czy instalacje gaśnicze, aby chronić sprzęt przed czynnikami zewnętrznymi.

- Wdrażaj zasilanie awaryjne (UPS, generatory), co pozwoli uniknąć nagłego wyłączenia systemów w przypadku braku prądu.

- Stosuj blokady antykradzieżowe, szczególnie w strefach ogólnodostępnych, by uniemożliwić łatwą kradzież urządzeń takich jak laptopy czy stacje robocze.

19. Szkolenia pracowników i budowanie świadomości

- Organizuj regularne szkolenia, podczas których pracownicy będą poznawać aktualne zagrożenia (w tym phishing, ransomware i inne ataki socjotechniczne) oraz dobre praktyki bezpieczeństwa.

- Przeprowadzaj testowe kampanie phishingowe, aby sprawdzić w praktyce czujność i reakcje użytkowników, a następnie omawiaj wyniki, wskazując, co można poprawić.

- Udostępniaj materiały edukacyjne, takie jak krótkie poradniki, checklisty czy plakaty, w miejscach łatwo dostępnych dla personelu (intranet, tablice informacyjne).

- Zachęcaj pracowników do natychmiastowego zgłaszania podejrzanych maili i incydentów, zapewniając, że żadne z pytań czy obaw nie zostaną zlekceważone ani ukarane.

- Unikaj domyślnych ustawień zaufania, szczególnie dla linków, załączników oraz urządzeń zewnętrznych. Powinny być one traktowane jako potencjalnie niebezpieczne. Dobrą praktyką jest oznaczanie m.in zewnętrznej korespondencji jako wymagającej szczególnej ostrożności.