ENGAVE S.A.

Porady i wskazówki techniczne w zakresie zabezpieczeń sprzętowych i programowych

Firma **Engave S.A.**, NIP **5223105508** / KRS: **0000704729** (dalej Partner PWCyber), udziela Ministerstwu Cyfryzacji zgody na wykorzystanie i publikację materiałów przekazanych w ramach Programu PWCyber (zwanych dalej „Materiałami"), w szczególności: tekstów, grafik, diagramów, infografik, prezentacji oraz innych treści edukacyjnych. Partner oświadcza, że materiały nie naruszają praw osób trzecich.

Spis treści

1. Kradzież lub zgubienie urządzenia - jak należy zabezpieczyć przed wyciekiem danych z takich urządzeń

Poziom: **krytyczny**

Dotyczy: **użytkownika**

Najprostszym sposobem zabezpieczenia danych na urządzeniach przenośnych firmowych oraz prywatnych w przypadku kradzieży lub zgubienia jest uruchomienie funkcji szyfrowania.

W zależności od platformy, są to różne mechanizmy szyfrowania. W systemie **Windows** należy wdrożyć w organizacjach politykę GPO Bitlockera na krytycznych stacjach (np. administratorów/księgowych) lub na wszystkich stacjach. Bitlocker jest funkcją wbudowaną w wersje Windows Pro/Enterprise. Należy upewnić się, że notebook posiada zaktualizowany BIOS i sprawdzić czy w opcjach BIOS-u jest włączony TPM oraz SecureBoot. Należy pamiętać, że w czerwcu 2026 wygasa certyfikat Microsoft SecureBoot i należy go uaktualnić, aby nie mieć problemu z uruchomieniem systemu. W celu ułatwienia pracy użytkownikowi można skonfigurować automatyczne odblokowanie TPM przy starcie (mniej bezpieczna opcja) lub zabezpieczyć wymaganiem PIN-u minimalnie 6 znakowego. W przypadku prywatnego komputera również należy uruchomić funkcję bitlockera we własnym zakresie i przechowywać zapasowy klucz najlepiej na dwóch różnych zewnętrznych zasobach aby nie utracić możliwości zalogowania.

W systemie operacyjnym **macOS** należy uruchomić aplikacje FileVault w *Preferencjach systemowych* → *Bezpieczeństwo i prywatność* -> uruchomić funkcję szyfrowana i zapisać klucz odzyskiwania w iCloud lub w bezpiecznym menedżerze haseł.

W systemach **Linux** znajdziemy przydatną aplikacja LUKS (Linux Unified Key Setup) do szyfrowania partycji. Konfiguracji dokonamy przez *cryptsetup*, *luksFormat* i *cryptsetup luksOpen*. Klucz tak jak w innych przypadkach przechowujemy w bezpiecznym miejscu (np. offline, w menedżerze haseł).

W organizacjach możemy zaimplementować płatne rozwiązanie typu MDM np. *Microsoft Intune*, dzięki której będzie możliwe zdalne usuniecie danych, tzw. Wipe. Wymogiem jest podpięcie urządzenia skradzionego/zgubionego do sieci.

2. Zabezpieczenia przed „phishingiem” oraz przed przejęciem tożsamości

Poziom: **krytyczny**

Dotyczy: **użytkownika**

Nie ma póki co złotego środka ochrony przed phishingiem. Mechanizmy AI są coraz sprytniejsze i tworzą maile, które mogą przedostać się przez zapory antyspamowe i zostać zaklasyfikowane jako normalne maile, w których ukryte są niebezpieczne linki oraz załączniki.

Zabezpieczamy się przed takim działaniem kierując się dobrymi praktykami.

Przede wszystkim edukacja i weryfikacja. Należy dokładnie sprawdzać adres i nr nadawcy w mailach, smsach, wiadomościach w komunikatorach internetowych. Nie logować się na linki podane w mailach chyba, że zostały sprawdzone jako wiarygodne źródła. Należy sprawdzać czy strona, na która chcemy się zalogować, posiada aktualny certyfikat. Należy ignorować (nie otwierać i jeżeli dotyczą służbowych kont zgłaszać do działu bezpieczeństwa) prośby o nietypowe pilne logowania.

Dobrym zwyczajem jest generowanie silnych unikalnych haseł dla każdej usługi, np. złożonych z wielu wyrazów. Należy unikać tego samego hasła w wielu miejscach. Przy obsługiwaniu wielu portali usług należy przemyśleć użycie sprawdzonych rozwiązań menadżerów haseł typu *Bitwarden*, *1Password*, *KeePassXC* - oczywiście z backupem tych haseł na innych zasobach. Dodatkową praktyką jest nie zapisywanie haseł w przeglądarce bez szyfrowania oraz regularne aktualizacje haseł w krytycznych usługach.

Zalecane jest używanie, tam gdzie tylko się da, MFA (Multi-Factor Authentication) w postaci zabezpieczenia autoryzacji na urządzeniu mobilnym. MFA w postaci sms i e-mail mogą być przechwycone przez mechanizmy typu SIM swap lub phishing. Najbezpieczniejszym sposobem MFA jest klucz sprzętowy (FIDO, U2F) który można dodatkowo zabezpieczyć PIN-em. Zawsze należy posiadać dwa takie klucze - jeden z nich powinien być przechowywany w bezpiecznym miejscu typu sejf.

3. Atak przez nieznane urządzenia USB

Poziom: **wysoki**

Dotyczy: **użytkownika**

Ważna jest edukacja pracowników w organizacjach, aby nie podpinać znalezionych pendrive’ów, kabli USB czy też dysków, na których może być ukryte złośliwe

oprogramowanie np. ransomware, keyloggery lub mogą być wykorzystywane ataki typu *BadUSB* (podszywanie się pod klawiaturę i wykonywanie komend).
W organizacjach należy wyłączyć autostart dla zewnętrznych nośników lub w ogóle zablokować możliwość używania pendrivów i zewnętrznych nośników danych - polityka **„Zero Trust dla USB”**. Należy rozważyć zakup dodatkowych mechanizmów:

- **MDM/EDR** (np. Intune, Defender for Endpoint) – blokada nieautoryzowanych urządzeń.
- **DLP (Data Loss Prevention)** – kontrola kopiowania danych na USB.
- **Device Control** w rozwiązaniach antywirusowych (np. ESET, Symantec).

4. Ataki przez publiczne punkty dostępowe (Wi-Fi)

Poziom: średni

Dotyczy: **użytkownika**

W przypadku pracy zdalnej poza miejscem zamieszkania lub pracy, najlepiej używać własnego źródła Internetu w postaci hotspot'u np. z telefonu komórkowego.
W przypadku użycia hotspot'u należy włączyć hasło WPA/WPA3. Należy wyłączyć hotspot, gdy jest nie używany aby nie narazić się na atak. Sieci publiczne np. w kawiarniach lub hotelach, mogą być podsłuchiwane. W celu zwiększenia poziomu bezpieczeństwa powinniśmy zapewnić szyfrowanie transmisji danych uruchomiając VPN przy podłączeniu się do sieci WI-FI. Wskazanie jest używanie sprawdzonych rozwiązań typu *NordVPN*, *ProtonVPN*, *OpenVPN* (dla firm). Zalecamy unikanie darmowych VPN, które często zbierają dane zamiast realnie nas chronić. Dodatkowe zabezpieczenia na stacjach, to obowiązkowo włączone zapory (firewall) na urządzeniu, wyłączenie „*udostępniania plików i drukarek*” w sieciach publicznych. Należy włączyć funkcję „*Public Network*” w Windows (brak wykrywania urządzeń).

5. Atak na kamerę i mikrofon

Poziom: średni

Dotyczy: **użytkownika**

Zagrożenie polega na tym, że złośliwe oprogramowanie lub osoba trzecia może uzyskać dostęp do kamery i mikrofonu w urządzeniu użytkownika, co prowadzi do naruszenia prywatności, podsłuchiwania rozmów, a nawet szpiegowania otoczenia. Kamera i mikrofon są często wykorzystywane w pracy zdalnej, wideokonferencjach i komunikacji głosowej. Atakujący mogą nagrywać obraz i dźwięk bez wiedzy

użytkownika, co może prowadzić do wycieku danych osobowych i informacji firmowych.

Jakiego typu zabezpieczeń możemy użyć?

- **Fizyczna zasuwka na kamerę** – najprostsze i najskuteczniejsze rozwiązanie. Nawet jeśli urządzenie zostanie zainfekowane, kamera nie zarejestruje obrazu.
- **Wyłączanie mikrofonu, gdy nie jest używany** – w ustawieniach systemu lub poprzez dedykowane przyciski w laptopie.
- **Kontrola uprawnień aplikacji** – sprawdzaj, które aplikacje mają dostęp do kamery oraz mikrofonu i ograniczaj to do niezbędnych.
- **Aktualizacje systemu i oprogramowania** – zmniejszają ryzyko wykorzystania luk w zabezpieczeniach.
- **Używanie Antywirusa i EDR** – wykrywanie prób nieautoryzowanego dostępu.
- **Monitorowanie aktywności** – np. powiadomienia o włączonej kamerze / mikrofonie.

6. Ransomware i utrata danych

Poziom: **krytyczny**

Dotyczy: **administratora**

Ransomware to złośliwe oprogramowanie, które szyfruje dane i żąda okupu za ich odszyfrowanie. Skutkiem ataku może być całkowita utrata danych, przestój w pracy, a nawet poważne straty finansowe i reputacyjne. Nowoczesne podejście do backupu, które minimalizuje ryzyko utraty danych w wyniku ataku ransomware, awarii sprzętu czy błędu ludzkiego to strategia **3-2-1-1-0.**

- **3** – trzy kopie danych (1 produkcyjna + 2 kopie zapasowe);
- **2** – na dwóch różnych nośnikach (np. dysk lokalny + taśma lub chmura);
- **1** – jedna kopia poza lokalizacją (off-site, np. w chmurze);
- **1** – jedna kopia w „cyfrowym bunkrze” (air-gapped), odłączona od sieci, np. taśma lub WORM storage *(Write Once, Read Many)* - to technologia przechowywania danych, w której pliki można zapisać tylko raz, a następnie wielokrotnie odczytywać, bez możliwości ich modyfikacji lub usunięcia;
- **0** – zero błędów w backupie (regularne testy odtwarzania i weryfikacja integralności).

Wdrażając odpowiednie zabezpieczenie najpierw trzeba określić krytyczne dane: systemy które chcemy objąć ochroną, wybrane bazy, pliki użytkowników. Następnie wybieramy technologie backupu z wielu dostępnych na rynku np. Veeam, Commvault lub natywne rozwiązania chmurowe. W celu dodatkowego zabezpieczenia rekomendujemy zbudować „cyfrowy bunkier" – fizycznie odłączony nośnik lub logicznie izolowana strefa (Immutable Storage). Staramy się zautomatyzować backupy ustawiając harmonogram + szyfrowanie + wersjonowanie. W celu weryfikacji działania należy testować otworzenie backupu - minimum raz w miesiącu. Monitorujemy codziennie raporty backupu i alerty z nimi związane – wykrywanie anomalii w backupach (np. nagły wzrost zmian w plikach).

7. Ataki na firmware i bootkit

Poziom: **krytyczny**

Dotyczy: **administratora**

Secure Boot zapewnia, że podczas startu systemu uruchamiane są tylko podpisane i zaufane komponenty. Należy sprawdzić w UEFI/BIOS, czy Secure Boot jest włączony, oraz upewnić się, że mamy najnowsze klucze platformy (*PK*, *KEK*, *db*, *dbx*). Skonfiguruj także hasło do BIOS/UEFI - ustaw hasło administratora (Supervisor Password), aby uniemożliwić nieautoryzowane zmiany w ustawieniach firmware. Opcjonalnie: hasło użytkownika do blokowania startu systemu. Zmień kolejność bootowania - usuń lub przenieś na koniec opcje bootowania z: USB, DVD/CD, sieci (PXE), pozostaw tylko dysk systemowy jako główny nośnik.

TPM (*Trusted Platform Module*) umożliwia pomiar integralności komponentów podczas rozruchu (*PCR – Platform Configuration Registers*). Wykorzystuj funkcje Measured Boot i BitLocker do ochrony danych. Włącz w BIOS opcję TPM i skonfiguruj w systemie (np. Windows: tpm.msc).

8. Ataki na sieć

Poziom: **wysoki**

Dotyczy: **administratora**

Podstawowe zabezpieczenia organizacji przed próbami ataku poprzez router brzegowy poza systematycznymi aktualizacjami firmware, antywirusa, IPS (*Intrusion Prevention System*) i samych urządzeń polegają na wdrożeniu segmentacji VLAN, czyli stworzeniu osobnych VLAN-ów dla: drukarek i urządzeń IoT (Internet of Things np. kamery, urządzenia przemysłowe), stacji roboczych i serwerów. Należy włączyć ACL (*Access Control Lists*) na switch'ach/router'ach, aby kontrolować ruch między VLAN-ami.

Podstawowa zasada komunikacji między VLAN-ami zakłada dopuszczanie ruchu tylko przez firewall lub router z regułami. Na firewallu skonfiguruj reguły:

- Blokuj niepotrzebny ruch między stacjami roboczymi a serwerami.
- Zezwalaj tylko na wymagane porty/protokół (np. RDP, SMB, HTTP/HTTPS).
- Włącz IDS/IPS lub monitorowanie NetFlow/SFlow, aby wykrywać anomalie.

Jeśli to możliwe to wdróż NAC (*Network Access Control*) czyli system bezpieczeństwa sieci, który kontroluje, jacy użytkownicy i urządzenia mogą uzyskać dostęp do sieci, na jakich zasadach oraz do jakich zasobów, weryfikując tożsamość, stan urządzenia i zgodność z politykami bezpieczeństwa, aby chronić zasoby i zapewnić widoczność w sieci.

Włącz *Port Security* czyli limit liczby MAC na porcie (np. 1 lub 2) oraz Blokadę portu przy wykryciu nieautoryzowanego MAC. Zablokuj nieużywane porty (*shutdown* w konfiguracji switch'a).

9. Ataki na konta

Poziom: **wysoki**

Dotyczy: **administratora**

Ograniczanie pracy na kontach administracyjnych to jeden z najważniejszych elementów strategii bezpieczeństwa. Należy wdrożyć zasadę **Least Privilege** i podejście **Zero Trust**.

Zasady **Least Privilege**:

- Przyznawaj uprawnienia tylko wtedy, gdy są potrzebne – użytkownik powinien mieć minimalny dostęp wymagany do wykonania swoich zadań.
- Oddziel konta administracyjne od kont użytkowników. Administratorzy powinni mieć dwa konta: jedno do codziennej pracy (bez uprawnień admina) i drugie do zadań administracyjnych.
- Używaj mechanizmów Just-In-Time (JIT) - Tymczasowe podnoszenie uprawnień tylko na czas wykonania zadania.

Zasady **Zero Trust:**

- Nie ufaj domyślnie żadnemu urządzeniu ani użytkownikowi – każda próba dostępu musi być weryfikowana.
- Wdrażaj MFA (Multi-Factor Authentication) dla wszystkich kont.

- Wdrażaj kontrolę dostępu opartą na kontekście (lokalizacja, urządzenie, czas).
- Monitoruj aktywność kont administratora w SIEM i reaguj na anomalie.

Techniczne środki ochrony:

- Blokuj logowanie na kontach admina do stacji roboczych użytkowników (tylko serwery lub jump hosty).
- Audytuj grupy uprzywilejowane (np. *Domain Admins*, *Enterprise Admins*).
- Włącz logowanie i alerty dla: zmian w uprawnieniach, tworzenia nowych kont z wysokimi uprawnieniami.

10. Nieaktualne oprogramowanie

Poziom: średni

Dotyczy: **administratora**

Automatyzacja aktualizacji to świetny sposób na minimalizowanie ryzyka związanego z przestarzałym oprogramowaniem. Automatyzację aktualizacji systemów operacyjnych Windows można wdrożyć poprzez włączenie Windows Update for Business lub użycie WSUS (Windows Server Update Services) i skonfigurowanie Group Policy do wymuszania instalacji aktualizacji. W systemach Linux można użyć pakietu unattended-upgrades dla dystrybucji (Debian/Ubuntu) lub dnf-automatic dla (RHEL/Fedora). Można też skonfigurować cron'a do regularnych aktualizacji.

Poza samymi poprawkami do systemów należy stale przeprowadzać aktualizacje aplikacji i sterowników. Pomocny jest do tego SCCM / Microsoft Endpoint Configuration Manager lub Intune do zarządzania aktualizacjami aplikacji lub też zewnętrzne narzędzia takie jak np. Endpoint Central. Należy monitorować stan aktualizacji poprzez włączenie raportowania w WSUS/SCCM lub użyciu zewnętrznych narzędzi typu Qualys, Nessus, OpenVAS do skanowania podatności.

Dodatkowe zalecenia:

- Testuj aktualizacje w środowisku staging przed wdrożeniem do produkcji.
- Wprowadź politykę Patch Management z harmonogramem (np. Patch Tuesday).
- Automatyzuj restart po aktualizacji tam, gdzie to możliwe.