Ogólne czynności jakie zostały wprowadzone/obowiązują na każdej stacji roboczej firmy.

Poniższa tabela przedstawia opis ogólnych informacji o czynnościach jakie zostały podjęte na rzecz zabezpieczenia stanowisk roboczych (stacjonarnych/mobilnych) przed niepożądanym wyciekiem danych.

Czynność	Opis minimalizacji ataku	wykorzystane oprogramowanie / uwagi
Szyfrowanie "całego" dysku *(tzw. full disk encryption)* -Szyfrowanie fragmentu dysku na przetrzymywanie poufnych danych	Chroni przed nieuprawnionym dostępem do danych, np. na skutek kradzieży *(tzw. atak Evil Maid).*	**VeraCrypt 1.22 -** jak mówi wikipedia: "otwartoźródłowe narzędzie używane do szyfrowania danych. Pozwala na szyfrowanie całych dysków, partycji, przenośnych dysków USB oraz tworzenie wirtualnych zaszyfrowanych dysków o określonej pojemności… umożliwia szyfrowania za pomocą algorytmów: AES, Camellia, Kuznyechik, Serpent i Twofish, a także szyfrowanie wielokrotne przy pomocy: AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES, Twofish-Serpent *(lic. open source movement)* ***"Rejestr Czynności IT"***
Regularna aktualizacja oprogramowania	Chroni przed większością ataków masowych, typu: - otwarcie złośliwego pliku, - wejście na złośliwą stronę internetową Każde popularne oprogramowanie posiada błędy bezpieczeństwa (tzw. dziury). Są one odnajdywane i łatane na bieżąco. Aby je eliminować należy regularnie wykonywać aktualizację.	***"Rejestr Czynności IT"***
Regularne sprawdzenie uprawnień aplikacji (w tym aplikacji zewnętrznych)	Chroni przed wyciekiem danych do niepowołanych osób fizycznych bądź organizacji.	***"Rejestr Czynności IT"***
Stosowanie unikatowych haseł do każdego serwisu/usługi oraz włączenie dwuskładnikowe uwierzytelnienie *(tzw. 2 factor authentication)* **Instalacja managera haseł**	Chroni przed nieuprawnionym dostępem do danych (kont w serwisach internetowych/oprogramowania). Najczęściej atakujący zdobywają dostęp do twojego konta w serwisie X, dzięki temu, że udało im się włamać na serwis Y, w którym także miałeś zarejestrowane konto na ten sam adres e-mail/login. Ponieważ serwis Y był od dawna zapomniany (np. studenckie forum) i zarządzany przez niekompetentną	Atakujący są w stanie sprawdzać ponad 5 milionów haseł na sekundę. Dlatego aby opóźnić złamanie hasła, hasło powinno być: - niesłownikowe (hasła: qwerty, qazwsx, albo kasia123 lub defibrylator nie są dobre, ponieważ znajdują się w słownikach służących do łamania haseł. Te słowniki zawierają wszystkie poprawne słowa z j. polskiego, angielskiego, itp, oraz popularne kombinacje "123456", a także wersje powyższych słów pisane od tyłu, na przemian małymi i dużymi literami, a także

	osobę, w momencie ataku pracował pod kontrolą nieaktualnego oprogramowania. Dzięki temu, atakując wykorzystując znany od dawna błąd, wykradli z niego bazę danych. W bazie znajdowało się hasła jak w serwisie X. Inną przyczyną włamań na konta jest obejście formularza logowania poprzez formularz "resetu" hasła. Z tego powodu nie ustawiaj pytania "przypominającego hasło" na "Ulubiony kolor" z odpowiedzią "Czarny", gdyż jest to bardzo łatwe do odgadnięcia. Dwuskładnikowe uwierzytelnienie ochroni konto, w przypadku przejęcie hasła atakujący aby mieć dostęp do konta potrzebuje także telefonu	z przyrostkami (ang. suffix): "123", "098", "111", "000", "123!", "1!" itp. na końcu). - nieszablonowe(nie tworzone według szablonu. np. MojeTajneHasloDoAllegro - bo w przypadku wycieku haseł z Allegro, atakujący domyśli się, że hasło do Facebooka to zapewne MojeTajneHasloDoFacebooka) - długie i skomplikowane (im dłuższe hasło i im więcej znaków posiada, tym dłużej zajmie atakującemu jego łamanie). *(te same porady dotyczą także odpowiedzi na pytania "przypominające hasło")* Na każdym możliwym portalu, serwisie bądź oprogramowaniu należy włączyć "Dwuskładnikowe uwierzytelnienie" **KeePass -** to sejf dla haseł. Ustawiamy jedno silne hasło (to należy pamiętać), które broni dostępu do programu, a następnie w programie zapisujemy lub generujemy unikalne hasła dla każdego konta, które posiadamy. Program integruje się z przeglądarką internetową i jest w stanie automatycznie logować nas do serwisów internetowych, wypełniając formularze logowania. Keepas przetrzymuje nasze dane w postaci zaszyfrowanego pliku. Program posiada także wersję na telefony komórkowe, a więc zawsze możemy mieć swoje unikalne hasła pod ręką. *(lic. GNU GPL)* *UWAGA!* *Upewnij się, że wiesz jak się zalogować za pomocą specjalnych kodów awaryjnych, na wypadek gdybyś stracił dostęp do swojego telefonu. Wydrukuj je i przechowuj w bezpiecznym miejscu.* ***"Rejestr Czynności IT"***
Podniesienie bezpieczeństwa przeglądarek internetowych **Regularne czyszczenie przeglądarek z plików cookies oraz cookies Flash**	Podsłuchiwaniem ruchu Internetowego i kradzieżą tożsamości/danych	Korzystanie z przeglądarek internetowych Google Chrome, Firefox (lub z ich zoptymalizowanych odpowiedników) Zaletą Google Chrome jest sandboxing (separacja), minimalizujący skutki ataków, ale wadą przekazywane pewnych statystyk do Google (co można ograniczyć w ustawieniach lub wykorzystać klon przeglądarki Google Chrome zorientowany

		na prywatność, np. SRWare Iron lub Chromium, która domyślnie nie wysyła statystyk i raportów o błędach). Wyłączenie wtyczek Java (oraz inne których nie potrzebujesz, a zapewne nie potrzebujesz niczego poza Flashem) Włączenie funkcji “click-2-play” dla wtyczek. Dzięki temu, żaden aplet Flasha na stronie nie wystartuje sam z siebie (nawet te “niewidzialne” 1x1 px). Aby aktywować np. aplet filmiku na YouTube, będziesz musiał najpierw w niego kliknąć *Dla Chrome:* *Ustawienia → Pokaż ustawienia zaawansowane... → Ustawienia treści → Wtyczki → Kliknij, by uruchomić* Instalacja rozszerzeń: - NoScript(blokada JS dla Fx) - NoScripts(blokada JS dla Chrome) - HTTPS Everywher e(wymusza szyfrowane połączenia, jeśli są możliwe) Ustawienie Cookie oraz Cookie Flash - Google Chrome/Firefox ***“Rejestr Czynności IT”***
VPN *Łącząc się z nie swoją siecią (Wi-Fi)*	Chroni przed podsłuchiwaniem danych. W przypadku darmowych hotspotów (np. McDonalds, itp.) oraz sieci z szyfrowaniem WEP -- każdy inny użytkownik sieci widzi cały ruch internetowy. Jeśli nie korzystasz z szyfrowanych protokołów, będzie możliwy podsłuch tj. przechwycić twoje hasła. Atakujący może także celowo podstawić fałszywą, niezaszyfrowaną sieć o nazwie (SSID) takiej jak sieć, do której wcześniej się łączyłeś. Twój komputer/smartfon połączy się z nią automatycznie, co pozwoli na podsłuch połączenia przez atakującego.	Wszelkie błędy certyfikatów wyskakujące podczas połączenia lub komunikaty informujące o zmianie odcisku/fingerprinta klucza traktuj jako *atak MITM* - **nie akceptuje takiego połączenia.** Dodatkowo warto zdawać sobie sprawę, że ruch jest szyfrowany jedynie do serwera SSH -- jeśli więc ktoś podsłuchuje serwer SSH, na wyjściu będzie w stanie podejrzeć twoje niezaszyfrowane połączenia (dlatego korzystaj tam gdzie to możliwe z szyfrowanych protokołów, tj. np. HTTPS). **OpenVPN -** według wikipedi: używa bibliotek OpenSSL do szyfrowania danych i kanałów kontrolnych. Może również korzystać z HMAC by stworzyć dodatkową warstwę zabezpieczenia połączenia. Pakiet jest w stanie również wykorzystać możliwości sprzętowe, by polepszyć stopień i jakość szyfrowania. *OpenVPN* oferuje kilka metod uwierzytelnienia użytkowników: poprzez klucze, certyfikaty lub nazwę użytkownika i hasło (opcja z nazwą użytkownika i hasłem może być stosowana, w przypadku klienta

		bez certyfikatu). *(lic. GPL)* ***"Rejestr Czynności IT"***
Połączenie zdalne	Pozwala przy pomocy szyfrowanego połączenia zdalnie ("z biura") połączyć się z daną stacją roboczą znajdującą się w obiekcie klienta firmy IT ART. Dzięki czemu możliwe jest szybkie usunięcie problemu, usterki lub zatrzymanie wycieku/przesyłania pakietów danych	**TightVNC -** pakiet oprogramowania do zdalnego sterowania komputerem klienta. Dzięki TightVNC możesz zobaczyć pulpit zdalnego komputera i sterować nim za pomocą lokalnej myszy i klawiatury, tak jak było by to robione siedząc przed komputerem w siedzibie klienta. *(lic. GNU GPL)* ***"Rejestr Czynności IT"***
Konfiguracja zapory *(tzn. Firewall'a)*	Chroni przed zwiększaniem powierzchni ataku poprzez wystawienie "wszystkim" usług z Twojego komputera (np. domyślnie włączonego w Windows udostępniania plików przez protokół SMB)	Ustawiono blokadę wszystkich połączeń przychodzących do komputera. Nie utrudnia to korzystania z komputera, pod warunkiem, że nie jesteś serwerem WWW, lub nie udostępniasz innej usługi innym internautom - gdy jest to wykonywane została założona odpowiednia reguła na firewall'u ***"Rejestr Czynności IT"***
Ustawienie kont urzytkowników (nie administracyjnych) wraz z konfiguracją ochrony antywirusowej	Antywirus chroni przed znanymi wirusami, a korzystanie z konta bez przywilejów administratorskich nie pozwoli złośliwemu oprogramowaniu na całkowite przejęcie systemu.	**ESET -** Oprogramowanie antywirusowe *(więcej informacji www.eset.pl)* **EMET** (ang. Enhanced Mitigation Experience Toolkit) - darmowy program autorstwa Microsoftu, który pozwala podnieść bezpieczeństwo danej aplikacji poprzez nałożenie na nią "ograniczeń" takich jak m.in. DEP czy ASLR Założenie kont użytkownikom z ograniczonymi prawami użytkowania. Utworzenie konta z częściowymi uprawnieniami administracyjnymi do poświadczenia niezbędnych certyfikatów/działań zostały podane pracownikom ***"Rejestr Czynności IT"***
Przeszkolenie pracowników o ryzyku umieszczania w sieci różnych danych	Chroni przed kompromitacją, wyciekiem poufnych danych	Wszystko co umieszczasz w internecie lub wysyłasz e-mailem nawet do 1 wybranej osoby, traktuj jako publicznie dostępne. Zawsze. Dla wszystkich. Skrzynka e-mail twojego zaufanego odbiorcy może zostać upubliczniona na skutek ataku lub czasowego błędu w serwisie Wszystko co umieszczasz w internecie,

		ma dużą szansę zostać tam na zawsze, czy tego chcesz, czy nie. ***"Rejestr Czynności IT"***
Hasło BIOS	Chroni przed kradzieżą sprzętu/danych. Atakujący nie odpali Twojego komputera z LiveCD/USB i nie uzyska dostępu do zaszyfrowanych części dysku, obchodząc uwierzytelnienie (utrudni mu to także nadpisanie MBR dysku z poziomu zewnętrznego systemu)	Pamiętaj! Hasło BIOS można zresetować (np. zworką, wyciągnięciem lub uszkodzeniem baterii podtrzymującej pamięć) lub podać domyślne hasło producenta, jeśli ma się dostęp fizyczny do płyty głównej. O ile nie da się przed dostępem fizycznym zabezpieczyć skutecznie, to warto to zastosować. ***"Rejestr Czynności IT"***
Instalacja ukrytego Trojana *(tzw. przyjaznego trojana)*	Zwiększa prawdopodobieństwo odzyskania sprzętu oraz minimalizuje wyciek danych.	**PREY -** oprogramowanie umożliwiające lokalizację sprzętu, przechwyt pulpitu, wykonanie zdjęcia złodziejowi (o ile są kamery podłączone do sprzętu) to wszystko pod warunkiem że jest on podłączony do sieci WAN. ***"Rejestr Czynności IT"***
Poczta elektroniczna *(tzw. poczta e-mail)*	Usługi serwerowe poczty mailowej świadczy firma: **NAZWA PL SP Z O O** Domena: Certyfikat wiarygodności: **SSL** Szyfrowanie wiadomości przy pomocy programuu outlook.	**Outlook -** **https://www.microsoft.com/pl-pl** Konfiguracja oprogramowania mailowego używanego na urządzeniach stacjonarnych oraz mobilnych. ***"Rejestr Czynności IT"***

PAMIĘTAJ!

Nic nie chroni cię w 100% w przypadku kradzieży między innymi przed:
- wyciekiem poufnych danych (nie tylko "Twoich"),
- kradzieżą tożsamości (nie tylko "Twojej"),
- Upublicznieniem danych oraz informacji itp.
-Przekazane Loginy, Hasła, oraz dostęp do danych poufnych należą tylko i wyłącznie do osoby upoważnionej do danych zasobów (ujawnienie tych danych osobom trzecim jest ***ZAKAZANE***)
-Dane dostępowe posiada również administrator oraz przedstawiciel firmy IT ART Łukasz Padula.

W razie jakiegokolwiek podejrzenia o wycieku danych bądź o jego możliwości niezwłocznie poinformuj o tym firmę

W razie niebezpieczeństwa kontakt 24/7
Oraz odpowiednie organy w tym PUODO

"Rejestr Czynności IT"
Szczegółowe informację o wykonywanych czynnościach znajdują się w pliku ***"Rejestr Czynności IT.xlsx"*** którego dokładną lokalizację zna tylko administrator.