Ogólne czynności jakie zostały wprowadzone/obowiązują na każdym serwerze firmy.

Poniższa tabela przedstawia opis ogólnych informacji o czynnościach jakie zostały podjęte na rzecz zabezpieczenia Serwerów (umieszczonych lokalnie w siedzibie firmy) 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-serwer"***
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-serwer"***
Regularne sprawdzenie uprawnień aplikacji (w tym aplikacji zewnętrznych)	Chroni przed wyciekiem danych do niepowołanych osób fizycznych bądź organizacji.	***"Rejestr Czynności IT-serwer"***
Instalacja managera haseł	Chroni przed atakami z sieci WAN przed keyloggerami oraz innymi sposobami przechwytu haseł. Tworzy hasła składające się z wielu losowych znaków dzięki czemu odgadnięcie takiego hasła jest niemal niemożliwe bez odpowiedniej wiedzy oraz odpowiednich narzędzi jakimi są jednostki o olbrzymiej mocy przeliczeniowej.	**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)* ***"Rejestr Czynności IT-serwer"***
Podniesienie bezpieczeństwa przeglądarek internetowych **Regularne czyszczenie przeglądarek z plików cookies oraz cookies Flash** **UWAGA!!** **PRZEGLĄDARKA INTERNETOWA STOSOWANA JEDYNIE W SYTUACJI AWARYJNEJ !**	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-serwer"***
VPN *Łącząc się z nie swoją siecią (Wi-Fi)*	Chroni przed podsłuchiwaniem danych. W przypadku gdy użytkownik łączy się z serwerem przy pomocy 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 dane i hasła. Atakujący może także	**OpenVPN -** według wikipedia: 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

	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 - co za tym idzie dostęp do danych serwera	bez certyfikatu). *(lic. GPL)* ***"Rejestr Czynności IT-serwer"***
Połączenie zdalne *(wykonywane jedynie w wyjątkowej sytuacji)*	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-serwer"***
Konfiguracja zapory *(tzn. Firewall'a)*	Chroni przed zwiększaniem powierzchni ataku poprzez wystawienie "wszystkim" usług z Serwera	Ustawienie odpowiednich blokad zapory na pakiety które są wysyłane i odbierane ***"Rejestr Czynności IT-serwer"***
Ustawienie kont urzytkowników (nie administracyjnych) oraz kont administracyjnych z różnymi uprawnieniami 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 (bez dostępu do "zdalnego pulpitu"). Założenie kont użytkownikom z ograniczonymi prawami administracyjnymi (z możliwością dostępu do "zdalnego pulpitu"). ***"Rejestr Czynności IT-serwer"***
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-serwer"***

Baza Danych SQL *(baza danych oparta na oprogramow. MS SQL Server)*	Zabezpieczenie poufnych **baz danych** aby kradzież danych była niemalże niemożliwa. Jeżeli z jakiegoś powodu nastąpiłby niespodziewany wyciek danych to zabezpieczenia wprowadzone są na tyle silne aby zminimalizować ich odczytanie - bądź nawet uniemożliwić bez dużych nakładów..	Opis niektórych zabezpieczeń można znaleźć na stronie internetowej producenta: https://technet.microsoft.com/pl-pl/library/bb283235(v=sql.105).aspx ***"Rejestr Czynności IT-serwer"***
Udostępnione zasoby dyskowe w sieci lan	Udostępnienie zasobów dyskowych serwera jest narażone na wyciek danych związany z ogólnodostępnym słabo zabezpieczonym oraz niecertyfikowanym udostępnianiem danych w sieci LAN.	Krótka instrukcja wspomagająca oraz pokazująca jakie między innymi zabezpieczenia zostały wprowadzone http://slow7.pl/server-2003-2008/item/108-windows-server-2012-poradnik-administratora-serwer-plikow ***"Rejestr Czynności IT-serwer"***
Macierz RAID 1	Minimalizuje możliwość utraty danych z winy sprzętowej	Polega na replikacji pracy dwóch lub więcej dysków fizycznych. Powstała przestrzeń ma rozmiar najmniejszego nośnika. RAID 1 jest zwany również lustrzanym (ang. *mirroring*).np.: Dwa dyski po 1000 GB zostały połączone w RAID 1. Powstała w ten sposób przestrzeń ma rozmiar 1000 GB. Jeden z dysków w pewnym momencie ulegają uszkodzeniu. Cała macierz nadal działa.

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