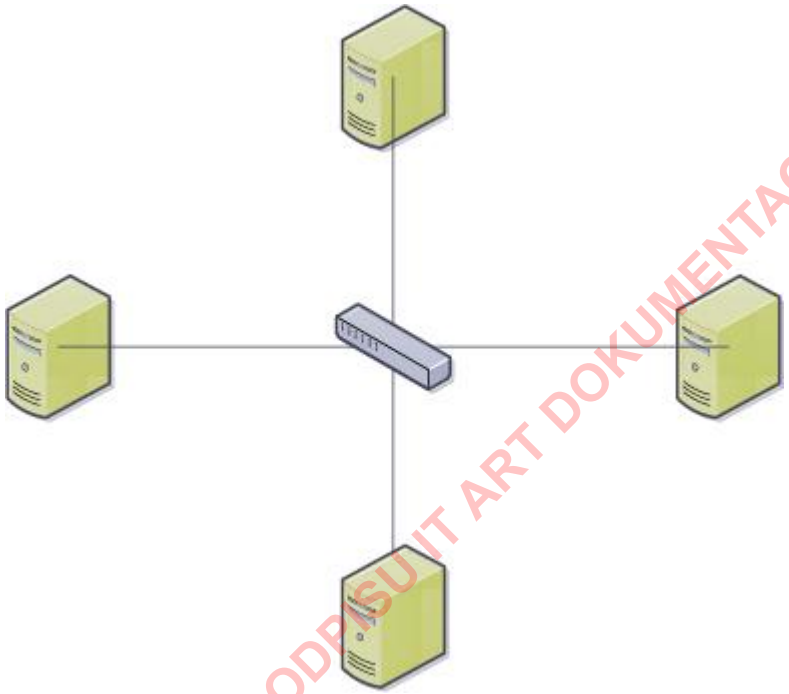
Infrastruktura i zabezpieczenie sieci lokalnej.

Informacje zawarte w tym rozdziale dotyczą infrastruktury sieci wraz z informacjami o zabezpieczeniach jakie zostały wykorzystane do jej zabezpieczenia.
Serwerownia została zabezpieczona metalowymi drzwiami zamkniętymi na klucz.
Pomieszczenie jest klimatyzowana aby zapewnić urządzeniom stałą temperaturę pracy.
W pomieszczeniu znajduje się: Szafa sieciowa, serwer oraz szafka zamykana na klucz między innymi z oprogramowaniem zakupionym na potrzeby firmy.
Urządzenie do wykonywania kopii zapasowych zostało umieszczone w innym miejscu niż w/w lokalizacje.

Sieć: Topologia gwiazdy (terminale + serwery + inne urządzenia sieciowe)



źródło: https://pl.wikipedia.org/wiki/Plik:Topologia_gwiazdy1.svg

Urządzenia wchodzące w skład infrastruktury:

- Stacje robocze - zwane terminalami
- Przełącznik sieciowy (switch) 10/100/1000 Mbps
- Trasownik (router) - nazywany później ”passat”
- Trasownik (router) - nazywany później ”TP”
- Serwer - zwany później “mama” (nie jest to jego prawdziwa nazwa - z wiadomych powodów)
- Serwer NAS-mama - przechowywanie kopii bezpieczeństwa/zapasowych serwera oraz terminali
- Serwer - zwany później “córka” (nie jest to jego prawdziwa nazwa - z wiadomych powodów) - **W trakcie budowy**
- Serwer NAS-córka - przechowywanie kopii bezpieczeństwa/zapasowych danych z serwera córka - **W trakcie budowy**
- Urządzenia peryferyjne (drukarki, skanery, urządzenia wielofunkcyjne itp.)

Poniższa tabela przedstawia opis ogólnych informacji o czynnościach jakie zostały podjęte na rzecz zabezpieczenia infrastruktury sieciowej (w tym urządzeń sieciowych).

Urządzenie	Czynność	Opis minimalizacji ataku	Wykorzystane oprogramowanie / uwagi
Router "passat" Dynamiczny adres IP	Zmiana danych dostępowych	Zmniejsza możliwość dostępu do software urządzenia.	Login i Hasło urządzenia zostały zmienione na niestandardowe, złożone, zawierające znaki z "tablicy ASCII" ***"Rejestr Czynności IT-sieć"***
	Ustawienie VPN	Zmniejsza możliwość przechwycenia danych dzięki tworzeniu "Tuneli" szyfrowanych opartych	Konfiguracja certyfikatów VPN oraz zapisanie listy adresów MAC mogących połączyć się z siecią ***"Rejestr Czynności IT-sieć"***
	Konfiguracja sieci WIFI	Minimalizuje możliwość dostępu do sieci bezprzewodowej	Hasło do sieci zostało zmienione na niestandardowe, złożone, zawierające znaki z "tablicy ASCII" Wyłączenie sieci publicznej "Gość" ***"Rejestr Czynności IT-sieć"***
Router "TP" *(W Budowie - planowane zabezpieczenia)* Stały adres IP	Zmiana danych dostępowych	Zmniejsza możliwość dostępu do software urządzenia.	Hasło urządzenia zostały zmienione na niestandardowe, złożone, zawierające znaki z "tablicy ASCII" ***"Rejestr Czynności IT-sieć"***
	Ustawienie VPN	Zmniejsza możliwość przechwycenia danych dzięki tworzeniu "Tuneli" szyfrowanych opartych	Konfiguracja certyfikatów VPN oraz zapisanie listy adresów MAC mogących połączyć się z siecią ***"Rejestr Czynności IT-sieć"***
	Konfiguracja sieci WIFI	Minimalizuje możliwość dostępu do sieci bezprzewodowej	Hasło do sieci zostało zmienione na niestandardowe, złożone, zawierające znaki z "tablicy ASCII" Wyłączenie sieci publicznej "Gość" ***"Rejestr Czynności IT-sieć"***
Serwer "mama"			***"Rejestr Czynności IT-serwer" - rozdział:*** *"Ogólne czynności jakie zostały wprowadzone/obowiązują na każdym serwerze firmy."*
Serwer NAS "mama"	Zmiana danych dostępowych	Zmniejsza możliwość dostępu do kopii zapasowej "Serwer "mama" oraz kopii stacji roboczych	Hasło urządzenia zostały zmienione na niestandardowe, złożone, zawierające znaki z "tablicy ASCII" ***"Rejestr Czynności IT-sieć"***
	Macierz RAID 1	minimalizuje utracenie	Polega na replikacji pracy dwóch lub więcej

		danych z winy usterki jednego dysku twardego	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. ***"Rejestr Czynności IT-sieć"***
Zasoby udostępnione	Ustawianie poświadczeń użytkowników oraz ich autoryzacja do wyznaczonych zasobów sieciowych	Minimalizuje dostęp nieupoważnionych osób do danej przestrzeni dyskowej	**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)* Dostęp do zasobów za poświadczeniem/autoryzacją Windows (login oraz hasło użytkownika) ***"Rejestr Czynności IT-sieć"***

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