DNR
GROUP

TWOJE IT
POD
KONTROLĄ

KLUCZOWE ASPEKTY BEZPIECZEŃSTWA IT W BIZNESIE

DNR GROUP

- Miejsce składowania danych
- Kontrola dostępu do urządzeń
- Bezpieczeństwo energetyczne
- Monitoring wizyjny
- Monitoring środowiskowy
- Lokalizacja (onPremis / Cloud)

- Hasła dostępowe
- Dokumentacja Techniczna
- Procedury
- Śledzenie zmian
- Rejestrowanie i analiza incydentów
- Okresowa inwentaryzacja
- Audyt Infrastruktury IT

DNR GROUP

- Oprogramowanie
- Urządzenia warstwy sieciowej
- Urządzenia przetwarzające dane
- Urządzenia przechowujące dane
- Sprzęt odpowiedzialny za backup i archiwizację
- Monitorowanie luk bezpieczeństwa

ZABBIX

Windows 10 BitLocker

Bitdefender

PROXMOX

pf

WORMS

PHISHING

BACKDOOR

PAYLOADS

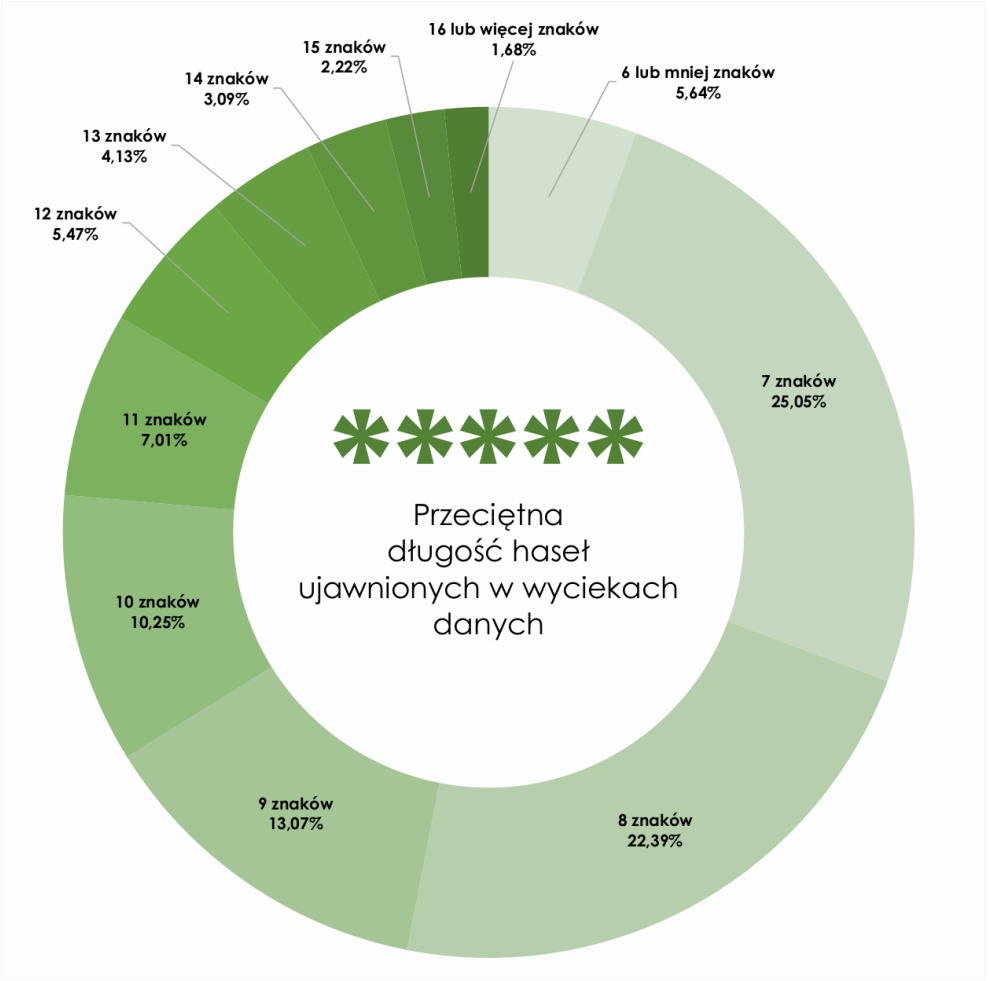
ROOTKITS

- Dostęp zdalny i praca zdalna
- Energia
- Błędy w konfiguracji
- Zabezpieczenie komputerów
- Zabezpieczenie telefonów
- Kopie bezpieczeństwa / Archiwizacja danych
- Brak monitoringu systemów informatycznych
- Hasła
- Każda firma powinna mieć plan **Disaster Recovery**

ZAGROŻENIA

RODZAJE ATAKÓW

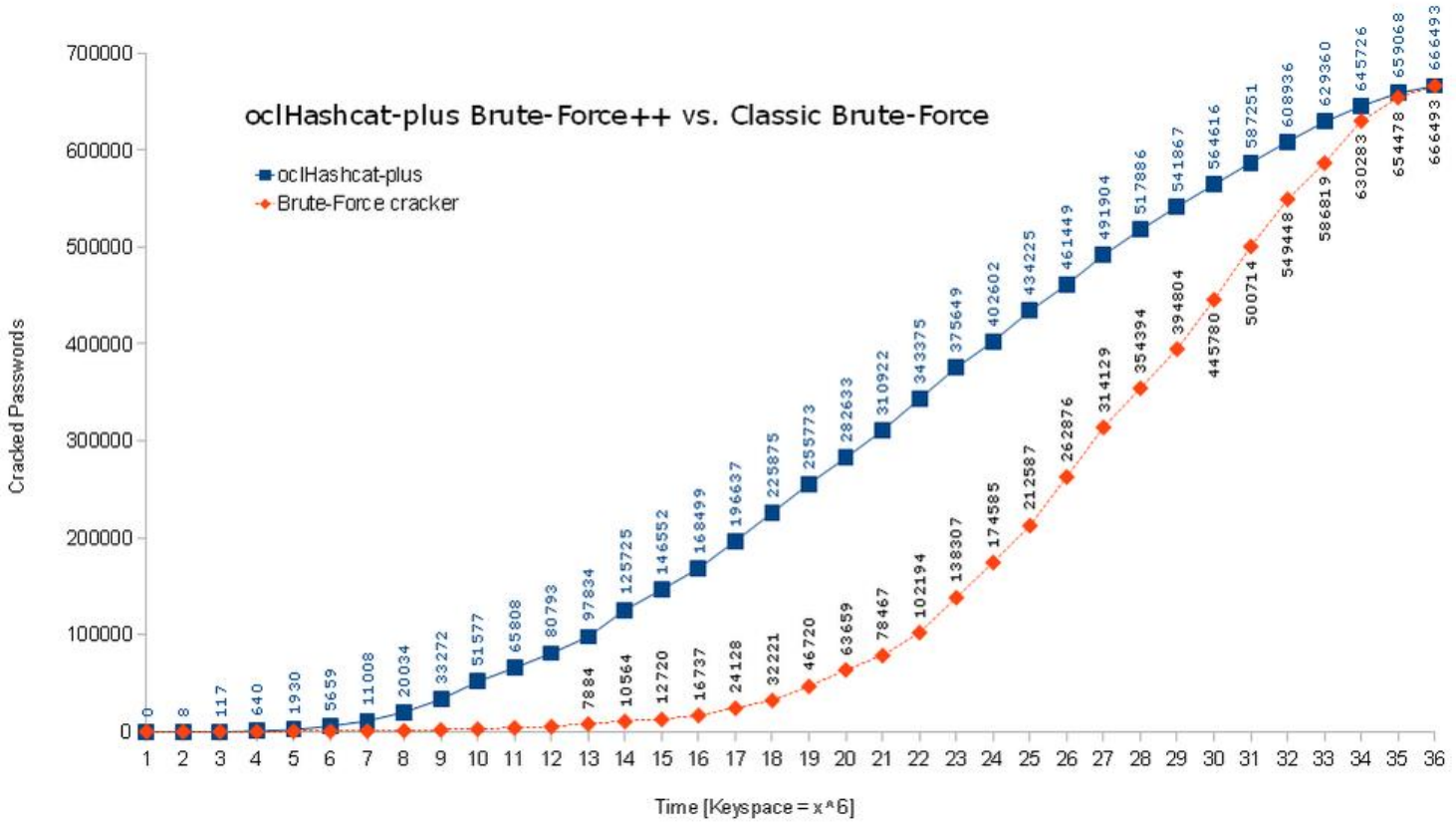
- PHISHING
- PRZEŁAMANIE HASŁA



Przyczyny:

- Przełamanie haseł – atak siłowy
- Ujawnienie hasła – hasło zapisane na kartce
- Jedno hasło do wielu systemów
- Zbyt proste hasło

https://haveibeenpwned.com
https://project-rainbowcrack.com/table.htm
https://cert.pl/



Listing 1. 50 najpopularniejszych haseł w analizowanym zbiorze

1. 123456	18. 1qaz2wsx	35. zxcvbnm
2. qwerty	19. 1234567	36. kasia
3. 12345	20. qwerty123	37. 1q2w3e4r
4. 123456789	21. qwerty1	38. kochanie
5. zaq12wsx	22. 123123	39. lol123
6. 1234	23. 0	40. kasia1
7. 12345678	24. bartek	41. natalia
8. polska	25. damian	42. myszka
9. 111111	26. michal	43. 11111
10. misiek	27. qwe123	44. 1qazxsw2
11. monika	28. polska1	45. lukasz
12. 123	29. password	46. mateusz1
13. marcin	30. karolina	47. komputer
14. mateusz	31. kacper	48. 666666
15. agnieszka	32. maciek	49. qazwsx
16. 123qwe	33. samsung	50. piotrek
17. 1234567890	34. qwertyuiop	

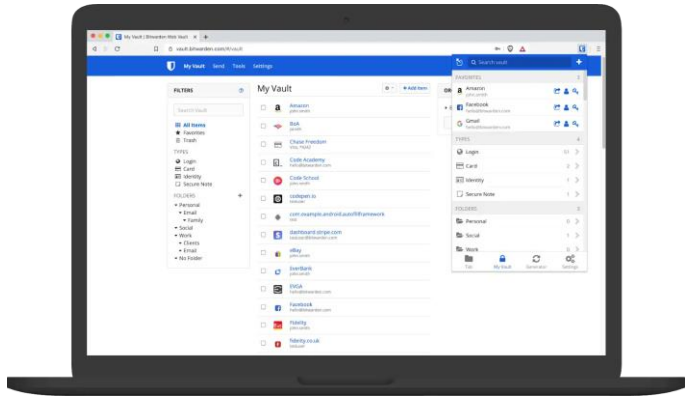
HASŁA

REKOMENDACJE:

- Korzystać z menagera haseł i wdrożyć politykę haseł
- Wszędzie gdzie jest to możliwe wykorzystywać mechanizm uwierzytelniania dwuskładnikowego (2FA)
- Do usług krytycznych wykorzystywać uwierzytelnianie przy pomocy klucza fizycznego np. yubikey

https://azure.microsoft.com/

https://www.yubico.com



https://bitwarden.com

https://azure.microsoft.com/pl-pl/pricing/details/active-directory/

DNR GROUP

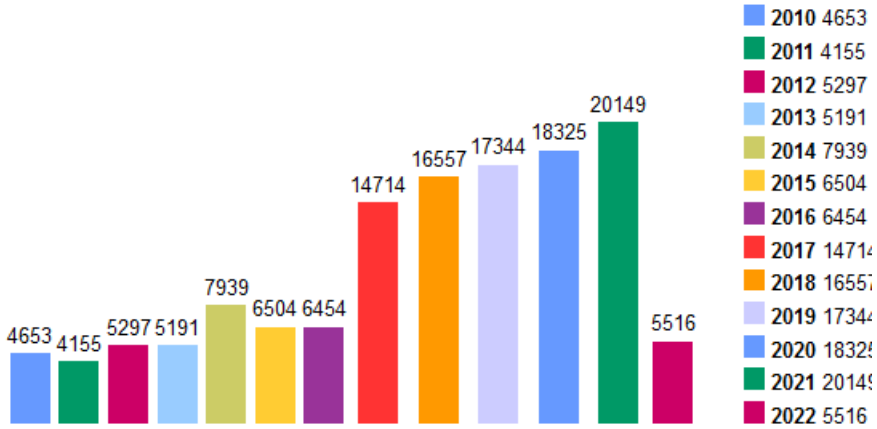
ZAGROŻENIA

BACKDOOR

INTRUSION DETECTION SYSTEM

- Skanowanie portów otwartych na świat z wystawionymi usługami np. Połączenie pulpitu zdalnego (RDP)
- Wykorzystanie podatności (www.cvedetails.com ,) która umożliwi ominięcie zabezpieczeń
- Wykorzystanie socjotechnik do uzyskania zdalnego dostępu do danych

SOCIAL ENGINEERING



Liczba wykrytych podatności w danym roku

SHODAN

https://www.shodan.io/

https://www.greenbone.net

DOSTĘP ZDALNY I PRACA

REKOMENDACJE

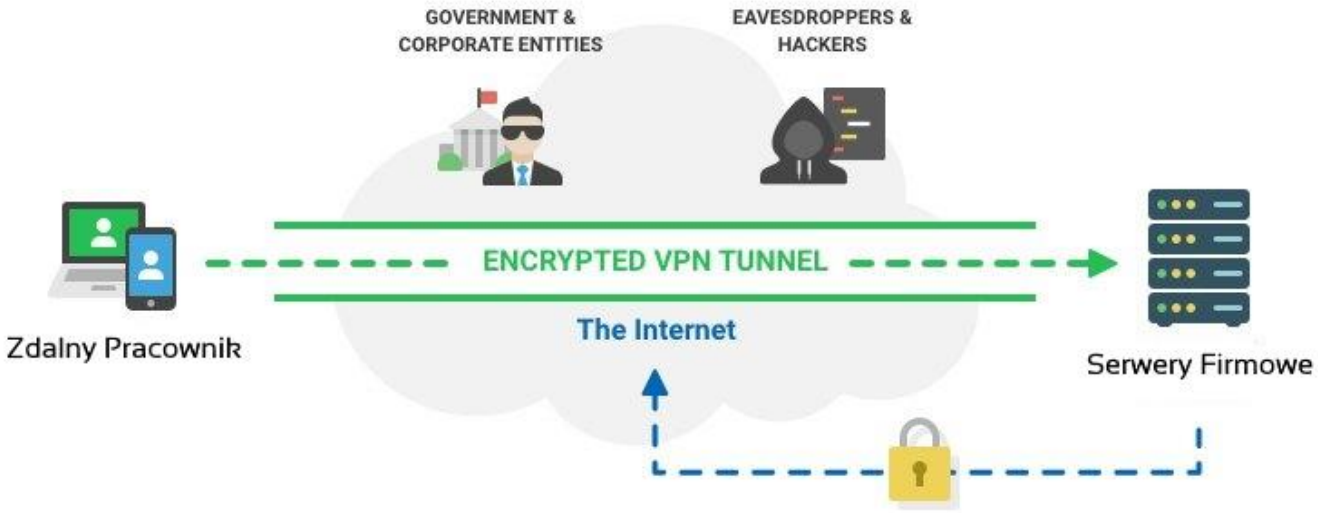
ABY UZYSKAĆ DOSTĘP DO DANYCH FIRMOWYCH UŻYWAJ TYLKO BEZPIECZNEGO POŁACZENIA!

- IPsec
- OpenVPN

- Nadawaj dostęp indywidualnym kontom, przypisanym do konkretnej osoby.

WDROŻENIE IDS/IPS
System który identyfikuje i zapobiega włamaniom.
Systemy które oferują takie rozwiązania to np..:

- Fortigate
- Sophos
- Watchguard
- bezpłatny pfSense / OPNSense



W Przypadku braku infrastruktury IT umożliwiającej dostęp VPN rozważ jego wdrożenie lub skorzystaj z rozwiązania które umożliwi pracownikowi autoryzację dwuskładnikową do zasobów. Przykładem takiego rozwiązania jest OwnCloud.

https://owncloud.com/

ZAGROŻENIA

- UTRATA DANYCH POPRZEZ NAGŁE PRZERWANIE ZASILANIA
- USZKODZENIE SPRZĘTU

REKOMENDACJE

- STOSOWANIE ZASILACZY UPS
- MONITOROWANIE ZASILANIA

ZAGROŻENIA

- CZĘSTE PROBLEMY Z DOSTĘPNOŚCIĄ USŁUG
- NARAŻENIE NA STRATY FINANSOWE / WIZERUNKOWE W WYNIKU INCYDENTU RODO

REKOMENDACJE

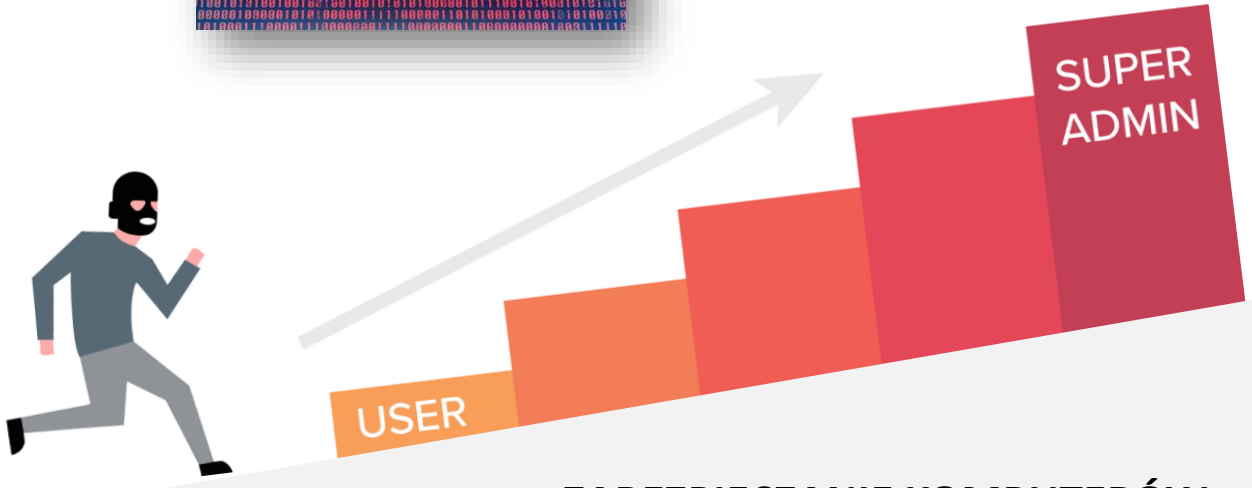
- ŚLEDZENIE ZMIAN W SYSTEMACH INFORMATYCZNYCH
- WDROŻENIE SYSTEMU DEVELOPERSKIEGO I TESTOWANIE ZMIAN PRZED WSTAWIENIEM ICH NA PRODUKCJĘ
- REGULARNY AUDYT KONFIGURACJI
- WDROŻENIE SYSTEMU CENTRALNEGO SYSTEMU LOGÓW
- WDROŻENIE SYSTEMU MONITORUJĄCEGO DZIAŁANIE SYSTEMÓW INFORMATYCZNYCH

DNR GROUP

ZAGROŻENIA

- UTRATA DANYCH, ORAZ MOŻLIWOŚĆ ICH UJAWNIENIA W PRZYPADKU KRADZIEŻY LUB ZGUBIENIA
- POTENCJALNE ŹRÓDŁO ATAKTU MALWARE

VeraCrypt



DNR GROUP

REKOMENDACJE

ZAGROŻENIA

- WYCIEK DANYCH Z KONT SŁUŻBOWYCH
- ROZPOWSZECHNIENIE ZAGROŻENIA WEWNATRZ SIECI FIRMOWEJ

REKOMENDACJE

- WDROŻENIE MOBILE DEVICE MANAGEMENT
- KONTROLA NAD WSZYSTKIMI URZĄDZENIAMI FIRMY
- KONTROLA CYKU ŻYCIA URZĄDZENIA (POZWALA CHRONIĆ URZĄDZENIE I DANE)
- USTANDARYZOWANIE KONFIGURACJI URZĄDZEŃ
- SZYFROWANIE URZADZENIA

ZAGROŻENIA

- BŁĘDNIE WYKONANA KOPIA ZAPASOWA, KTÓRA UNIEMOŻLIWA ODZYSKANIE DANYCH
- DŁUGI CZAS ODTWORZENIE DANYCH

REKOMENDACJE

- PRZYGOTOWANIE POLITYKI WYKONYWANIA KOPII BEZPIECZEŃSTWA
- PRZYGOTOWANIE POLITYKI ARCHIWIZACJI DANYCH
- KONTROLA OKRESOWA KOPII BEZPIECZNIKA
- PODEJŚCIE DO KOPII BEZPIECZEŃSTWA W SYSTEMIE 3,2,1

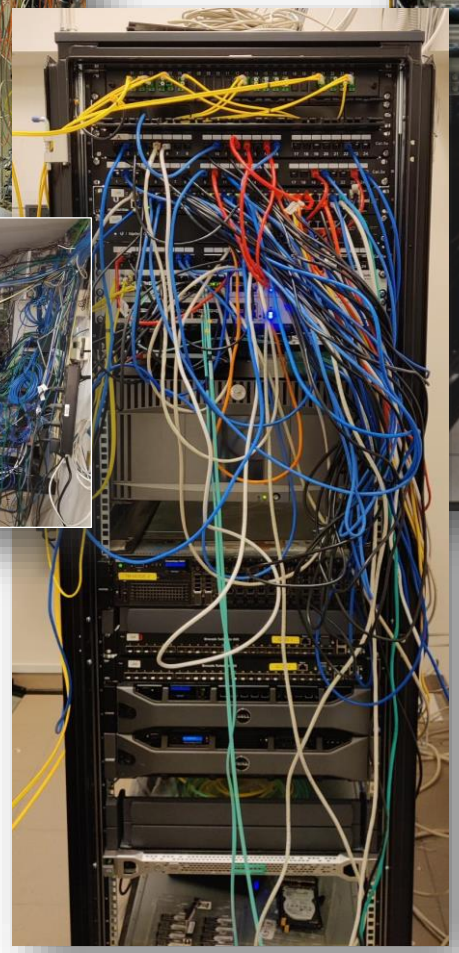
ZAGROŻENIA

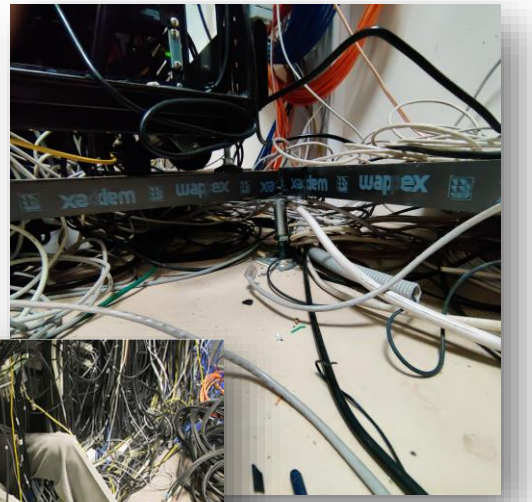
- BRAK WIEDZY O POWSTAJĄCYCH PROBLEMACH IT
- WOLNIEJSZY CZAS REAKCJI
- BRAK WIEDZY O ATAKACH

REKOMENDACJE

- WDROŻENIE SYSTEMU MONITOROWANIA SIECI I SERWERÓW
- WDROŻENIE IDS/IPS
- WDROŻENIE SYSTEMU ANALIZY LOGÓW
- KONFIGURACJA POWIADOMIEŃ EMAIL, SMS ITP

DNR GROUP





DISASTER RECOVERY

QUESTION AND ANSWER

Dziękuję za uwagę!

DNR Group Sp. z o.o.
ul. Chełmżyńska 180 p. 118, 04-464 Warszawa
tel. +48 (22) 230 21 31
email: biuro@dnrgroup.pl

Damian Rokicki
tel. +48 730 732 730
e-mail: rokicki.d@dnrgroup.pl

TWOJE IT
POD
KONTROLĄ

www.dnrgroup.pl