Zarządzane bezpieczeństwo w ofercie NetiaNext

Mysłowice, 28 września 2023 r.

NETIA
netianext

FORTINET

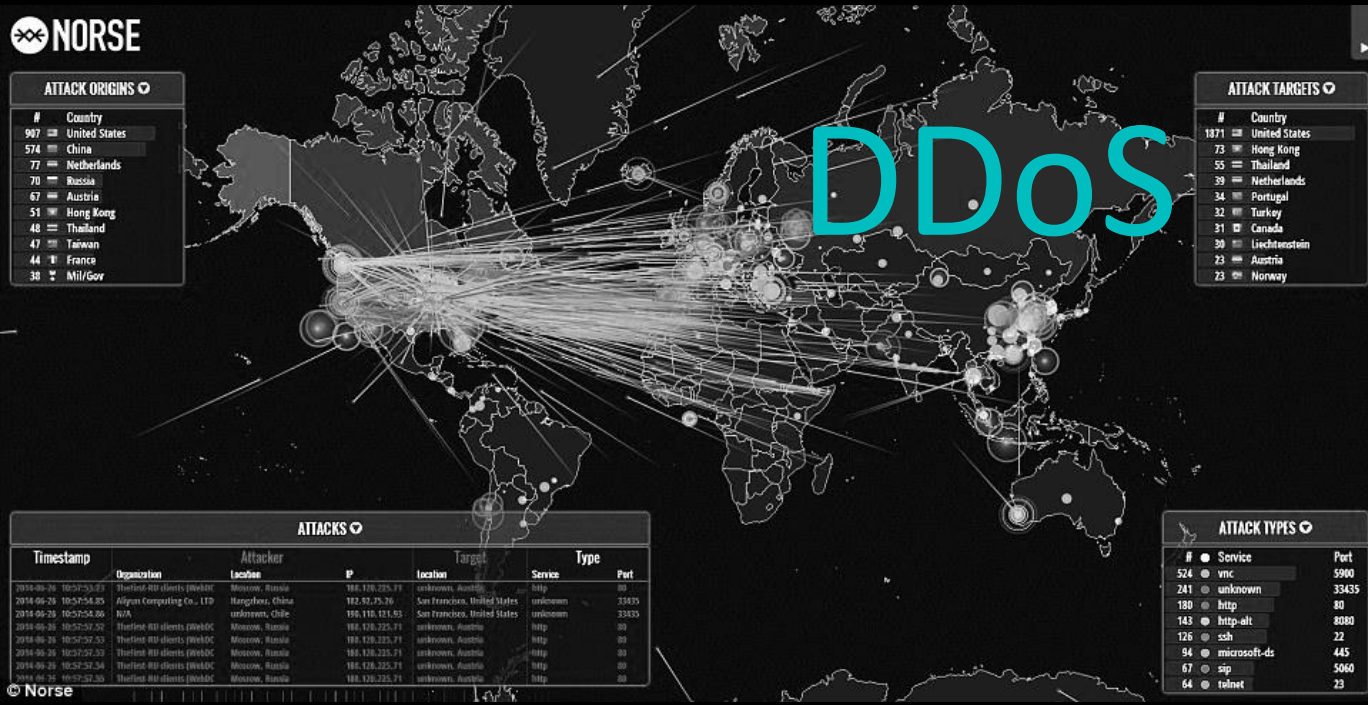
EXCLUSIVE NETWORKS

NETIA netianext

DC & compute

Bezpieczeństwo

Transmisja


NORSE
ATTACK ORIGINS
Country
907 United States
574 China
77 Netherlands
70 Russia
67 Austria
51 Hong Kong
48 Thailand
47 Taiwan
44 France
38 Mil/Gov
DDoS
ATTACK TARGETS
Country
1871 United States
73 Hong Kong
55 Thailand
39 Netherlands
34 Portugal
32 Turkey
31 Canada
30 Liechtenstein
23 Austria
23 Norway
ATTACKS
Timestamp
Attacker
Organization
Location
IP
Target
Location
Type
Service
Port
2014-06-26 10:57:53.23 Theltest RU clients (WebDC Moscow, Russia 188.120.225.71 unknown, Austria http 80
2014-06-26 10:57:54.25 Aligun Computing Co., LTD Hangzhou, China 182.92.75.76 San Francisco, United States unknown 33435
2014-06-26 10:57:54.86 N/A unknown, Chile 190.110.121.93 San Francisco, United States unknown 33435
2014-06-26 10:57:57.52 Theltest RU clients (WebDC Moscow, Russia 188.120.225.71 unknown, Austria http 80
2014-06-26 10:57:57.53 Theltest RU clients (WebDC Moscow, Russia 188.120.225.71 unknown, Austria http 80
2014-06-26 10:57:57.53 Theltest RU clients (WebDC Moscow, Russia 188.120.225.71 unknown, Austria http 80
2014-06-26 10:57:57.54 Theltest RU clients (WebDC Moscow, Russia 188.120.225.71 unknown, Austria http 80
2014-06-26 10:57:57.55 Theltest RU clients (WebDC Moscow, Russia 188.120.225.71 unknown, Austria http 80
ATTACK TYPES
Service Port
524 vnc 5900
241 unknown 33435
180 http 80
143 http-alt 8080
126 ssh 22
94 microsoft-ds 445
67 sip 5060
64 telnet 23
© Norse

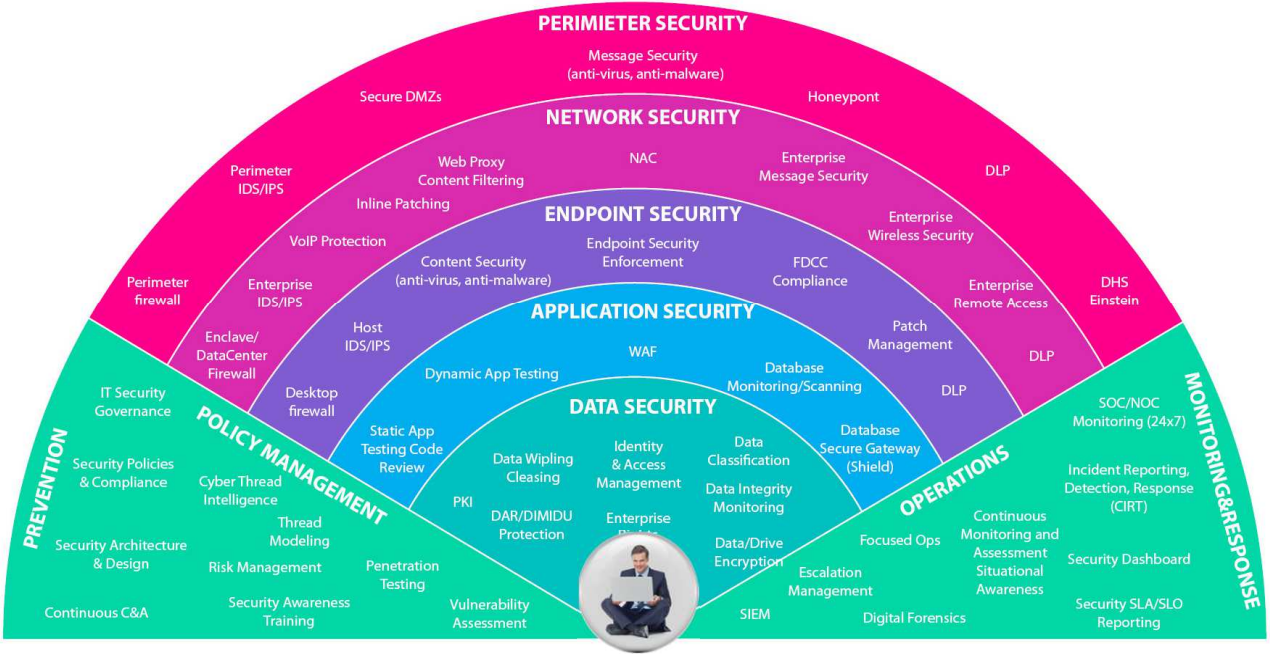
(spear) phishing

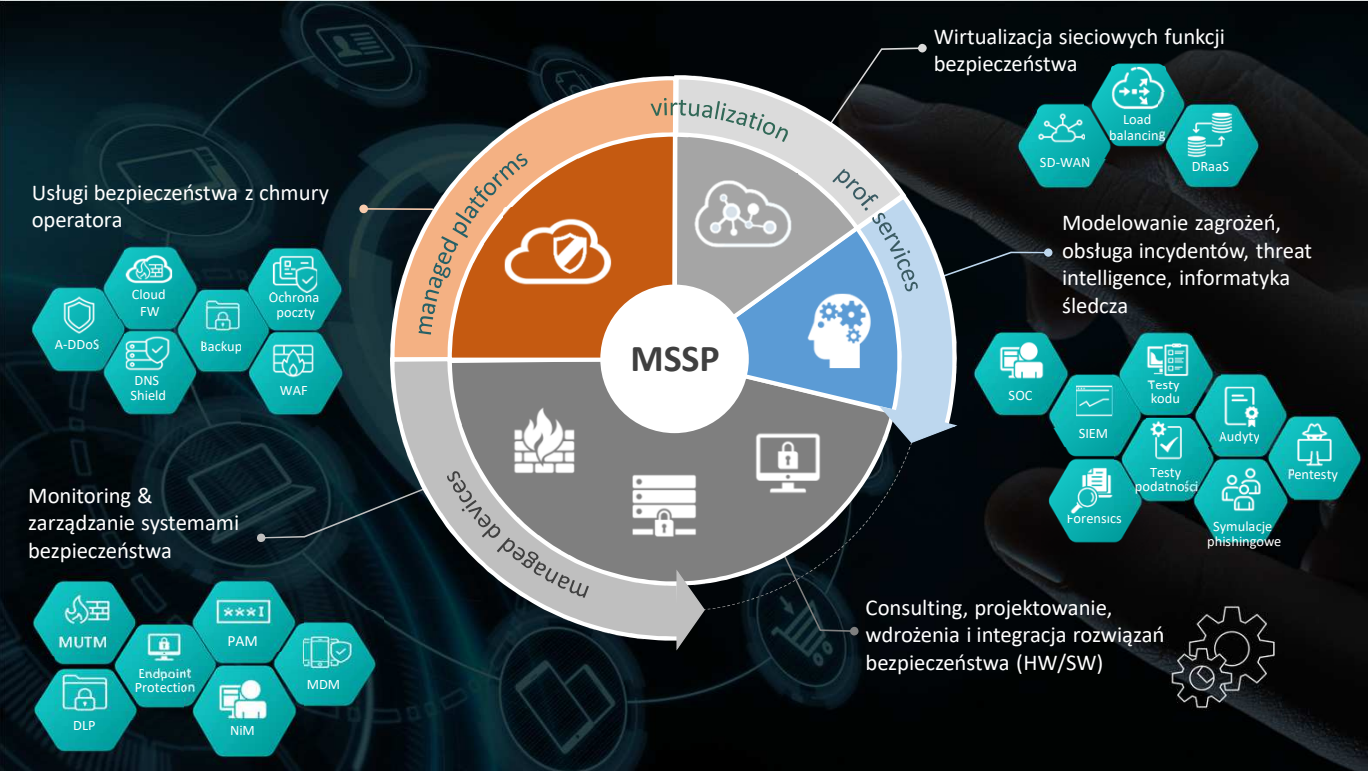
malware
ransomware


NETIA
netianext
APT

NETIA netianext

nie ma bezpiecznych systemów, tylko możliwe do obrony


PERIMIETER SECURITY
Message Security
(anti-virus, anti-malware)
Secure DMZs
Honeypont
NETWORK SECURITY
Perimeter
IDS/IPS
Web Proxy
Content Filtering
NAC
Enterprise
Message Security
DLP
Inline Patching
ENDPOINT SECURITY
VoIP Protection
Endpoint Security
Enforcement
Enterprise
Wireless Security
Content Security
(anti-virus, anti-malware)
FDCC
Compliance
Perimeter
firewall
Enterprise
IDS/IPS
APPLICATION SECURITY
Enterprise
Remote Access
DHS
Einstein
Host
IDS/IPS
WAF
Patch
Management
Enclave/
DataCenter
Firewall
Dynamic App Testing
Database
Monitoring/Scanning
DLP
DLP
Desktop
firewall
DATA SECURITY
Static App
Testing Code
Review
Data Wipling
Cleasing
Identity
& Access
Management
Data
Classification
Database
Secure Gateway
(Shield)
PKI
Data Integrity
Monitoring
DAR/DIMIDU
Protection
Enterprise
Data/Drive
Encryption
PREVENTION
POLICY MANAGEMENT
OPERATIONS
MONITORING&RESPONSE
IT Security
Governance
Security Policies
& Compliance
Cyber Thread
Intelligence
Thread
Modeling
Security Architecture
& Design
Risk Management
Penetration
Testing
Continuous C&A
Security Awareness
Training
Vulnerability
Assessment
SIEM
Focused Ops
Continuous
Monitoring and
Assessment
Situational
Awareness
Escalation
Management
Digital Forensics
SOC/NOC
Monitoring (24x7)
Incident Reporting,
Detection, Response
(CIRT)
Security Dashboard
Security SLA/SLO
Reporting


Wirtualizacja sieciowych funkcji bezpieczeństwa
Load balancing
SD-WAN
DRaaS
virtualization
prof. services
managed platforms
managed devices
MSSP
Usługi bezpieczeństwa z chmury operatora
Cloud FW
A-DDoS
Backup
Ochrona poczty
DNS Shield
WAF
Modelowanie zagrożeń, obsługa incydentów, threat intelligence, informatyka śledcza
SOC
SIEM
Testy kodu
Audyty
Testy podatności
Pentesty
Forensics
Symulacje phishingowe
Monitoring & zarządzanie systemami bezpieczeństwa
MUTM
Endpoint Protection
PAM
MDM
DLP
NiM
Consulting, projektowanie, wdrożenia i integracja rozwiązań bezpieczeństwa (HW/SW)

Security Operations Center

NETIA
netianext

Dziękuję.

Jarosław Gwizdoń
Kierownik ds. Klientów Kluczowych
- Rozwiązania Zintegrowane
jaroslaw.gwizdon@netia.pl

FORTINET

EXCLUSIVE NETWORKS

Strategie defensywne w cyberbezpieczeństwie

czyli jak chronić swoje zasoby teleinformatyczne

NETIA
netianext

Wybrane ataki w Polsce w 2023

NETIA
netianext

- **Styczeń:** Politechnika Bydgoska, Uniwersytet Artystyczny w Poznaniu, Min. Zdrowia
- **Luty:** podatki.gov.pl / Min. Finansów
- **Marzec**: Służba Kontrwywiadu Wojskowego, T-Mobile
- **Kwiecień:** BLIK, PZU, GPW
- **Maj**: wpolityce.pl, wprost.pl, polityka.pl, se.pl, rp.pl, niezależna, wyborcza.pl
- **Czerwiec:** Zarząd Dróg Zieleni i Transportu w Olsztynie, ePUAP
- **Lipiec**: Alfanet, Landtech, PGZ Stocznia Wojenna
- **Sierpień:** Evercom, Softinet, profil zaufany, COIG, Akademia Sztuki Wojennej, GPW, PKO BP, Credit Agricole, BNP Paribas

Firmy na GPW, ich przychody e-commerce… i potencjalne straty

NETIA
netianext

- Branża motoryzacyjna: przychody 1,7 mld PLN rocznie
  - dziennie – 4,7 mln PLN
  - na godzinę – 195 tys. PLN
- Branża odzieżowa: przychody 4,5 mld PLN rocznie
  - dziennie – 12,3 mln PLN
  - na godzinę – 513 tys. PLN
- Branża elektroniczna: przychody 3 mld rocznie
  - dziennie – 8,2 mln PLN
  - na godzinę – 342 tys. PLN

Która firma w obecnych czasach nie prowadzi działalności biznesowej w Internecie?

Czy stać ją na jakikolwiek przestój w sprzedaży?

Są na rynku usługi, które tanieją…

NETIA
netianext

DDoS:

- 1 godzina od 10 USD
- 1 dzień od 500 USD

- Malware on demand 45 USD
- Kampania phishingowa 500 USD/miesiąc
- Ransomware 1000 USD/kampania
- Karta kredytowa (numer, CCV) 10 USD
- Hakowanie konta pocztowego, serwisów społecznościowych 200 USD/konto
- Przejęcie urządzenia (komputer, telefon) od 300 USD /urządzenie

Cyberataki to też całkiem dobra inwestycja

NETIA
netianext

- Atak cybernetyczny za 34 USD miesięcznie może przynieść 25 tys. USD zysków, a te za kilka tys. USD – nawet 1 mln USD miesięcznie.

- Obecnie na rynku można kupić KAŻDY składnik potrzebny do stworzenia infrastruktury, narzędzia i treści potrzebnych do tego, aby stworzyć kompletny cyberatak.

Jak radzić sobie z cyberryzykiem?

① REDUKOWANIE RYZYKA

② PRZENIESIENIE RYZYKA

③ UNIKANIE RYZYKA

④ AKCEPTACJA RYZYKA

NETIA
netianext

Przede wszystkim zabezpieczenia

- **STRATEGIE OFENSYWNE**
- **STRATEGIE DEFENSYWNE**

NETIA
netianext

NETIA
netianext

Czym są **strategie ofensywne?**

…działania podejmowane przez organizacje lub państwa w celu aktywnego zwalczania zagrożeń cybernetycznych poprzez działania agresywne lub kontratakujące…

- ataki na infrastrukturę przeciwnika
- ataki na źródła finansowania
- hacking etyczny
- hohneypot’y
- dezinformacja
- hunting
- redteaming

Czym są strategie defensywne?

…są to środki i procedury stosowane przez organizację w celu zapewnienia ochrony danych i zasobów przed zagrożeniami w cyberprzestrzeni

NETIA
netianext

NETIA
netianext

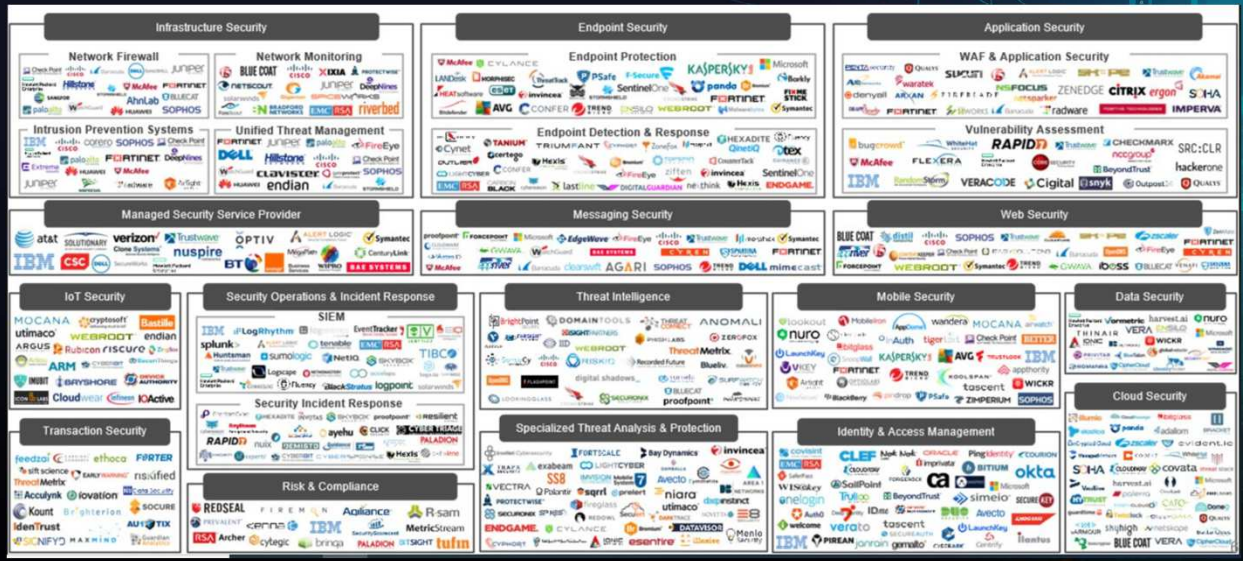
Jaki jest cel **wprowadzania tych strategii?**

Celem strategii defensywnych jest:

- minimalizowanie ryzyka wystąpienia ataków cybernetycznych,
- ochrona poufności, integralności i dostępności danych,
- reagowanie na ewentualne incydenty w sposób skuteczny i kontrolowany,
- ograniczenie szkód w przypadku cyberataku.

Dostępne na rynku **rozwiązania cybersecurity**

NETIA
netianext



Zarządzanie uprawnieniami | Backup danych | Testy penetracyjne | Kontrola dostępu (PIM, PAM, PUM, NAC)

Analiza podejrzanych plików (sandboxing) | Zarządzanie ryzykiem | Szkolenia | Aktualizacje | Symulacje ataków phishingowych

Reagowanie na incydentyc | Monitorowanie bezpieczeństwa | Uwierzytelnianie wieloskładnikowe (MFA) | Audyty bezpieczeństwa

OCHRONA X-ORGANIZACYJNA

OCHRONA KOŃCÓWEK

- Antywirus
- Detekcja podejrzanych aktywności (EDR)
- Ochrona przed phishingiem
- Ochrona przed złośliwym oprogramowaniem
- Ochrona przed wyciekiem danych (DLP)
- Wirtualna sieć prywatna (VPN)
- Ochrona urządzeń mobilnych (MDM)

OCHRONA SIECI

- Ochrona przed atakami DoS / DDoS
- Ochrona przed wyciekiem danych (DLP)
- Ochrona punktu styku z Internetem
- Ochrona poczty e-mail
- Skany sieci
- Wirtualna sieć prywatna (VPN)
- Ochrona przed złośliwym oprogramowaniem
- Ochrona przed phishingiem

OCHRONA APLIKACJI

- Ochrona aplikacji internetowych
- Ochrona przed atakami DoS/DDoS
- Skany webaplikacji
- Ochrona przed botami
- Ochrona API

OCHRONY (Z) CHMURY

- Ochrona przed atakami DDoS
- Ochrona aplikacji internetowych

NETIA
netianext

2 podstawowe **pytania**:

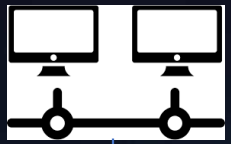
1. Czy potrzebujesz wszystkich tych rozwiązań?

- ponad 2/3 wszystkich ataków i zagrożeń ma związek z phishingiem i złośliwym oprogramowanie
- do 90% ataków wykorzystuje się pocztę elektroniczną
- Jaki jest poziom ekspozycji na ryzyko cyberataków w Twojej firmie?
- Jaki jest poziom dojrzałości strategii cyberbezpieczeństwa w Twojej firmie?

2. W jakiej kolejności należy je wdrażać?

Optymalna droga do kompletnego systemu bezpieczeństwa ICT?

1. Stacje robocze



oprogramowanie end-point protection FORTINET

+ regularne aktualizacje!!!

PODSTAWA OCHRONY W KAŻDEJ FIRMIE

2. Punkt styku z Internetem

firewall sieciowy:
- Cloud Firewall FORTINET
- Managed UTM FORTINET

3. Serwery aplikacyjne

ochrona przed DDoS:
- Netia DDoS Protection

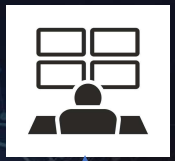
oraz

ochrona webaplikacji:
- Managed WAF FORTINET

4. Serwery pocztowe

ochrona @:
- Netia Ochrona Poczty

5. Cała infrastruktura ICT



monitoring bezpieczeństwa i reagowanie na incydenty:
- Netia Incident Monitoring FORTINET
- Netia SOC/SIEM

+ usługi dodatkowe

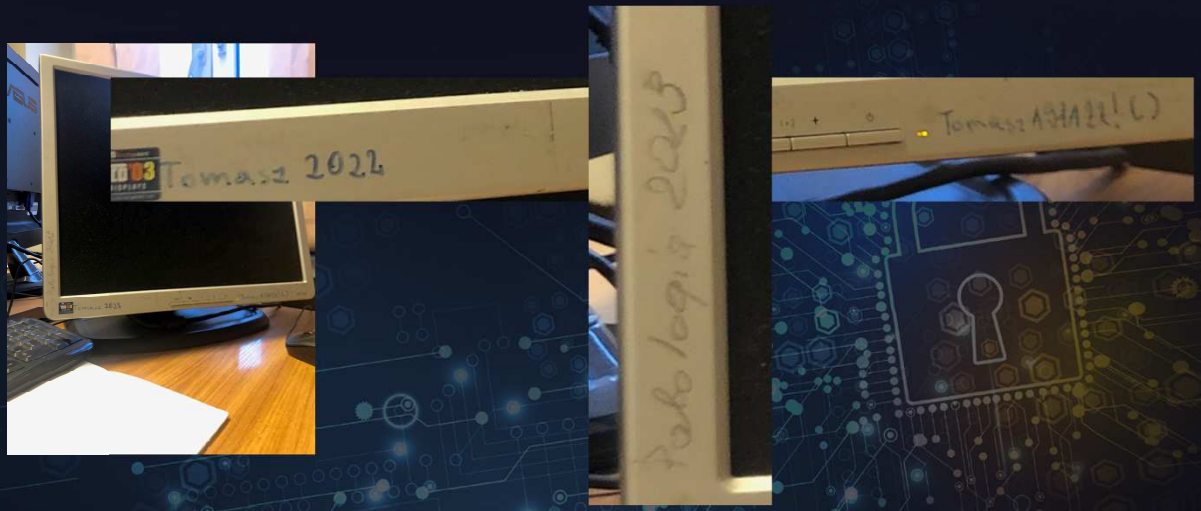
- Symulacje ataków phishingowych:
  - Phishing on Demand
- Backup danych:
  - Netia Data Protection
- Skany sieci: Testy podatności
- Skany webaplikacji: Testy podatności
- Usługi profesjonalne:
  - Testy penetracyjne
  - Audyty bezpieczeństwa,
  - Szkolenia security awareness
- Ochrona urządzeń mobilnych (MDM)
  - Netia End-Point Management

+ rozwiązania integratorskie

- Zarządzanie uprawnieniami
- Kontrola dostępu (PIM, PAM, PUM, NAC)
- Uwierzytelnianie wieloskładnik. (MFA)
- Ochrona przed wyciekiem danych (DLP)
- Ochrona przed wyciekiem danych (DLP)

NETIA
netianext

Dlaczego ważne jest 2FA/MFA?



NETIA
netianext

Cyberbezpieczeństwo to **ciągły proces!**

Aby skutecznie kontrolować zagrożenia i zapobiegać im, organizacja powinna regularnie:

- uaktualniać swoją strategię cyberbezpieczeństwa,
- monitorować dostępne nowe technologie,
- weryfikować i aktualizować procesy i procedury wewnętrzne,
- inwestować w szkolenia,
- testować poziom cyberbezpieczeństwa.

NETIA
netianext

Dziękuję.

Tomasz Łużak

Kierownik Produktu Cyberbezpieczeństwo
tomasz.luzak@netia.pl

FORTINET

EXCLUSIVE NETWORKS

Wykorzystane źródła:
https://cybersecurity.att.com/blogs/security-essentials/understanding-malware-as-a-service-maas-the-future-of-cyber-attack-accessibility
https://www.csoonline.com/article/566901/how-much-does-it-cost-to-launch-a-cyberattack.html
https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-black-market-ecosystem.pdf
https://antyweb.pl/atak-ddos-cena
https://www.computerworld.pl/news/Haker-z-darknetu-ile-kosztuje-jego-zatrudnienie-To-jak-szukanie-freelancera,432835.html
bankier.pl, sekurak.pl, telko.in, pap.pl, gazeta.pl, rp.pl, google.pl, masergy.com