Cybersecurity

Wrocław, 8 maja 2017

Bank Zachodni WBK
Grupa Santander

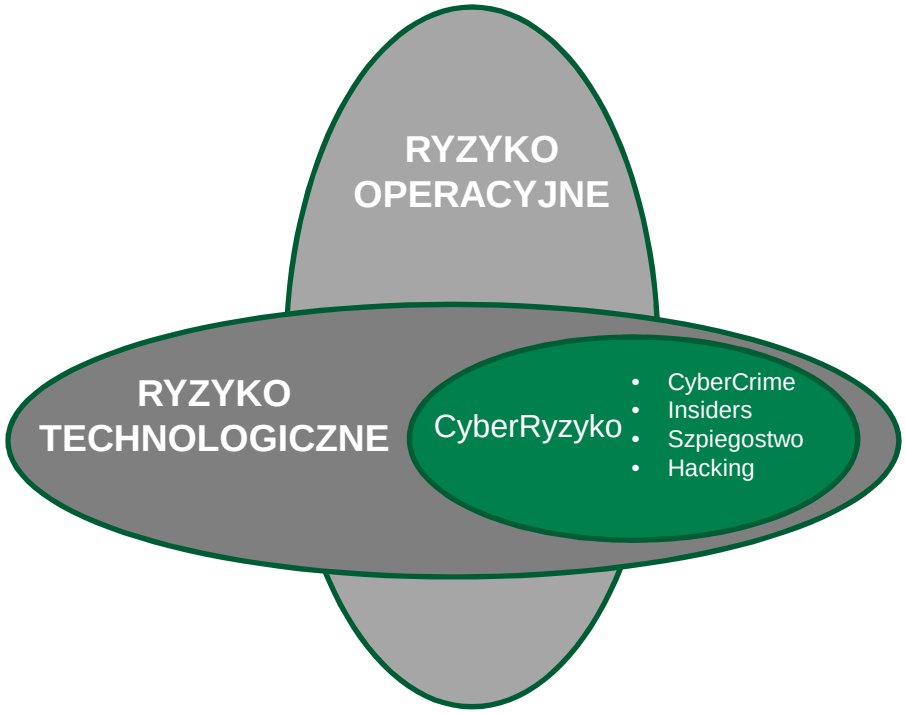
Czym jest cyberryzyko ?

Bank Zachodni WBK

Grupa Santander

Czym jest cyberryzyko?

Cyberryzyko jest częścią globalnego modelu zarządzania ryzykiem technologicznym



Cyberryzyka są częścią Ryzyk Technologicznych. Ich szczególne cechy wymagają opracowania określonego modelu zarządzania.

Czym jest cyberryzyko?

„Cyberryzyko" oznacza ryzyko z jakim wiąże się korzystanie z cyberprzestrzeni, tj. np. sieci komunikacji zewnętrznej.

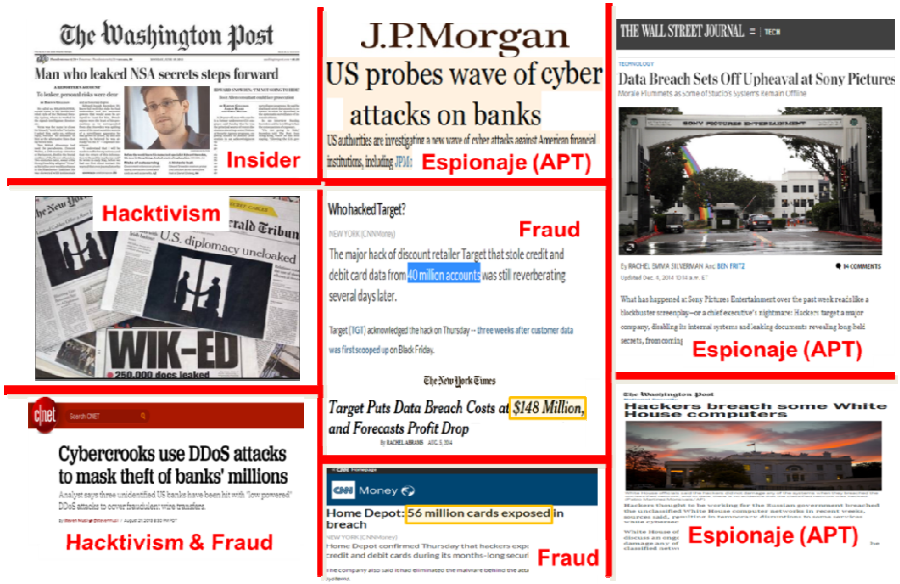
Sabotaż, ataki (haktywizm)	DDoS (rozproszona odmowa usługi), hakerzy, wirusy, złośliwe oprogramowanie Włamania do systemów (hakerzy, manipulacja sprzętu komputerowego) Cyber wymuszenia (sieci społecznościowe, blogi) Ujawnianie informacji poufnych (szkody dot. wizerunku) Usuwanie lub manipulowanie danych
Przestępczość internetowa: przestępstwo gospodarcze	Oszustwo na dużą skalę Szantaże, oszustwa Kradzież informacji Manipulacja/ korzystanie z urządzeń
Szpiegostwo i Wywiad	Kradzież wartości intelektualnej (wyciek informacji) Fałszowanie tożsamości Szpiegostwo cybernetyczne Ataki cybernetyczne na infrastrukturę krytyczną (zaawansowane trwałe zagrożenie (APT), wojna cybernetyczna, itd.)
Insiderzy	Wykorzystywanie informacji poufnych Nadużycia wewnętrzne Publikowanie lub sprzedaż informacji biznesowych

Odporność na ataki cybernetyczne (Cyber Resilience*1) oznacza zdolność otoczenia do obrony i powrotu do stanu sprzed cyberataku.

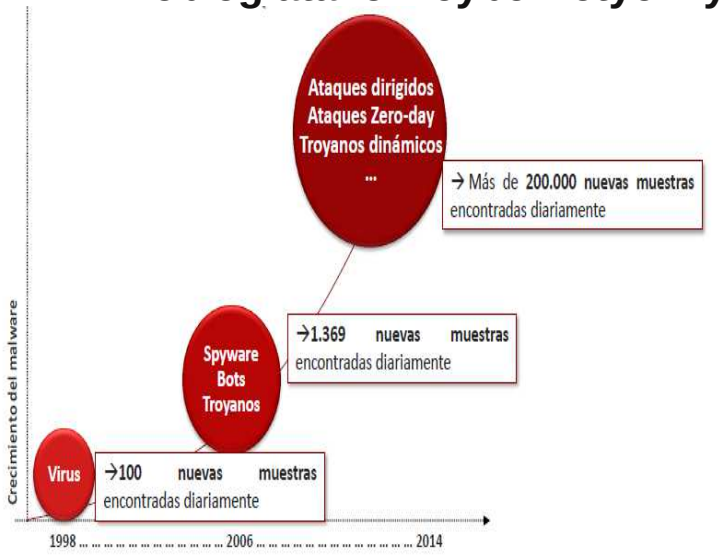
*1 Najnowsza publikacja Banku Rozrachunków Międzynarodowych (BIS) na temat Odporności infrastruktury rynku finansowego (Cyber Resilience in financial Market Infrastructure).

Czym jest cyberryzyko?

Przykłady



Przebieg ataków cybernetycznych



- 2,8 mld osób posiada dostęp do Internetu
- 10 mld urządzeń ma możliwość połączenia z Internetem

W globalnym raporcie ryzyka **Światowego Forum Ekonomicznego** z 2015r. ataki cybernetyczne zostały sklasyfikowane jako istotne zagrożenie o wysokim stopniu prawdopodobieństwa. Cyberprzestępczość pojawiała się na liście **10 najbardziej prawdopodobnych zagrożeń** przez ostatnie 4 lata.

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

Bank Zachodni WBK
Grupa Santander

Czym jest cyberryzyko ? - Raportowanie

CYBER-RISK REPORT

Cyber-Incidents

- Cyber-attack objective
- Cyber-incident type
- Cyber-attack length
- Time to identify cyber-attack
- Sophistication of the tactics used
- Cyber-attack impact
- Economic magnitude
- Threat source
- Tolls used
- Who identified the cyber-attack
- Files compromised during cyber-attack
- Data compromised during cyber-attack
- Privileges level used

Maturity Level - Measures Control and Deployment

- DDoS platform implementation level
- Anti-malware platform implementation level
- Information protection platform implementation level
- Internet security and connection with third parties platform implementation level
- Data Leak Prevention, platform implementation level
- Risk analysis-derived measures implementation level
- SOC deployment
- Processes and procedures implementation level

CyberRisk Indicators

- % services with a bad response time due to DDoS
- % updates in systems/ stations
- % virus updates
- % active system vulnerabilities
- % active application vulnerabilities
- % security event managed
- % encrypted laptops
- % profiles & users reviewed
- % activity review systems
- % alerts or events violating policies
- % risk analysis on assets
- % events resolution time

Czym jest cyberryzyko ? – Cyberrisk Program

DEFINED AT CORPORATE LEVEL.

Goal Profile Definition

Define a model with security measures, operational and procedural, related to CyberRisk, considering minimum measures, recommended depending the risk level.

Assessment

Units assessment, on each measure and process defined in the base model.

Gap Analysis

Compliance analysis, from the defined base level identifying the actual gap.

Action Plan Setting

Set an action plan based on the proposed actions analysis.

Action Plan Execution

Assure the proper implementation of each measure defined in the agreed action plan in order to reach the goal level.

Monitoring & Control

Local action plan advance level regular monitoring and control processes.

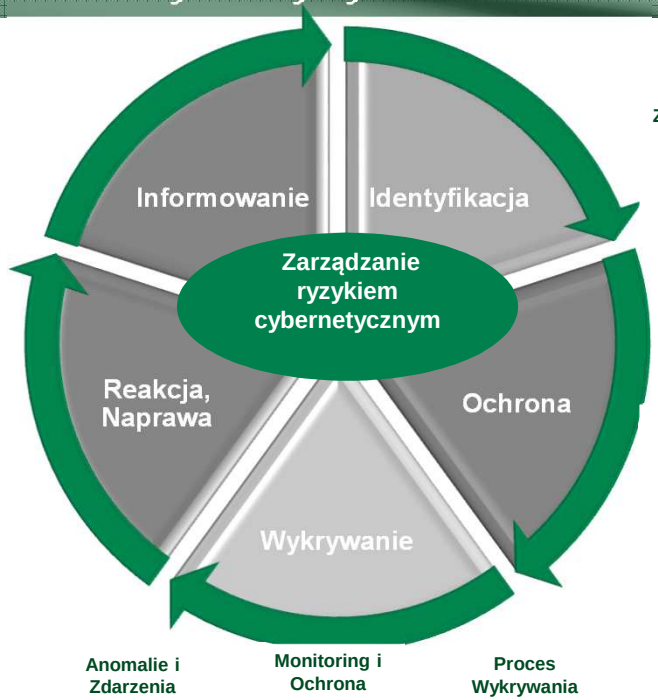
Aktualna sytuacja Grupy
Wprowadzone standardy

Bank Zachodni WBK
Grupa Santander

Model zarządzania cyberryzykiem

- Raport Wskaźników Cybernetycznych
- Raport Incydentów Cybernetycznych
- Nadzór i kontrola nad projektami

- Zasady komunikacji w wypadku incydentów
- Security Operations Center SOC (Centrum Operacji Bezpieczeństwa)
- Analiza incydentów
- Rozwiązywanie incydentów
- Plan Usprawnień
- Plan Naprawczy



- Analiza Ryzyka
- Mapa zagrożeń cybernetycznych
- Pomiar poziomu narażenia na ryzyko
- Spis aktywów i aplikacji

- Platforma Anti- DDoS - System Ochrony Informacji
- Platforma zwalczania złośliwego oprogramowania
- Infrastruktura Ochrony Obwodowej
- Bezpieczeństwo Systemów i Sieci
- Bezpieczeństwo Aplikacji
- Bezpieczeństwo Użytkowników
- Procesy i procedury kontrolne
- Plan zapobiegania oszustwom
- Szkolenia

Zgodnie z krajowymi i międzynarodowym i standardami (NIST, COBIT i ISO) oraz dyrektywami regulatorów (Strategia Bezpieczeństwa Cybernetycznego) (1)

- Usługi nadzoru cybernetycznego
- Usługi monitoringu infrastruktury
- Współpraca z organami rządowymi (np. CNPIC – Narodowe Centrum Ochrony Infrastruktury Krytycznej, itp.)
- Usługi wykrywania incydentów: Etyczne Hakerstwo i Zapobieganie Phishingowi

NIST: National Institute of Standards and Technology (Narodowy Instytut Standaryzacji i Technologii)

(1) Zgodnie z krajowymi i międzynarodo-wymi standardami (NIST, COBIT i ISO) oraz dyrektywami regulatorów (Strategia Bezpieczeństwa Cybernetycznego) (1)

Bank Zachodni WBK
Grupa Santander

Model zarządzania cyberryzykiem

CYBER-RISK MEASURES			
Function	**Category**	**Line**	**MEASURES**
Identify	**Risk Analysis**	**Risk Assessment**	Risk identification process Risk analysis Mitigation or acceptation proposals Risk levels monitoring
	Business environment	**Business environment**	Missions, goals, business activities Dependencies & functions – critical services development Availability requests – business point of view
	Asset Management	**Assets inventory**	Assets inventory
Protect	**Protection Technology**	**Perimeter security infrastructures**	Firewalls Proxies IPS WAF Layer architecture (Front, Back, DB) Navigation antivirus AntiSPAM Secure Remote Access platforms (VPN)
		Anti-DDoS platform	Traffic filtering/cleaning services Contents checking services (CDNs) Selective Routing Advertisement Blackhole Routing Geo-location and Geo-protection Events monitoring and identification (anomalous traffic)
		Anti malware platform	Internet Malware Infection Physical Malware Infection External Exploitation

Ryzyko cybernetyczne

CYBER-RISK MEASURES			
Function	**Category**	**Line**	**MEASURES**
Protect	**Protection Technology**	**Systems & Networks Security**	Vulnerabilities management Devices Secure Configuration (Hardening) Infrastructures, devices and authorized & non-authorized software inventory Internal network protection (NAC) Third parties connection protection
		Users Security	Workstation End Point solution (FW, disk encryption, Antivirus, IDS, USB ports restriction) e-mail encryption Devices secure configuration
	Data Security	**Data Security**	Data Security (encryption, information classification)
		Applications Security	Secure development Vulnerabilities management SSDLC Development Security Testing Security Coding and processes Data Base Security ERP / Application Control
	Information Protection	**Information Protection System**	IRM (Identity Rights Management) DLP (Data Loss Prevention) Users & profiles review and adaptation Activity log Information leaking policy
	Processes	**Control Processes & Procedures**	Communication procedures Management procedures Reporting procedure

Ryzyko cybernetyczne

CYBER-RISK MEASURES			
Function	**Category**	**Line**	**MEASURES**
Protect	**Access Control**	**Access Control**	Profiles & users review and activity control User Provisioning Privileged User management Role Based Access Control Management User Certification
	Training	**Training Programs**	Staff training and awareness
Detect	**Continuous Security Monitoring**	**Infrastructure Monitoring Services**	Monitoring service (SOC) Vulnerability Assessment
	Detection Process	**Detection Services**	Vulnerabilities detection service Trademark theft (Anti-phishing)
		Cyber-vigilance services	Intelligence services (APT networks , Botsnet, fraudulent IPs)
	Anomalies & Events	**Intelligence**	Events correlation and management – SIEM
Respond / Recover	**Communication**	**Communication protocols for incidents**	Unit communication and coordination protocols
	Analysis	**Incidents Analysis**	Cyber Crisis Management Cyber Incident Management & Response SOC
	Mitigation	**Incidents Solving**	Internal procedures of actions against threats Problem Management Service Level Management Capacity Management Availability Management
	Improvements	**Improvement Plan**	Best practices, improvement plans in recovery plans
	Recovery	**Recovery Plans**	Recovery plans
Report	**Indicators**	**Indicators Report**	Indicators report
	Incidents	**Cyber-Incidents Report**	Incidents report
	Management & Control	**Projects Monitoring**	Projects monitoring and control

Ryzyko cybernetyczne

CYBER-RISK MEASURES			
Function	**Category**	**Line**	**MEASURES**
Protect	**Information Protection / Processes & Performance / Data Security / Protection Technology**	**Antifraud Plan**	Robust authentication Sites cloning detection Operations limits Operations logs & auditing Transactions Scoring Operations timing Data entrance checking Anti-malware PC identification Adaptive authentication Out-of-the channel operations alert Strong code review in development Adaptive authentication evolution IVR identification Operation risk adapted authentication IVR system (Complete callings recording, register, distribution, recording) Customers voice recognition Hidden numbers blocking Previous record of operation numbers Call-Centre fraud records Fraudster voice recognition (black lists) Holiday flag ATMs securitization EMV adoption 3DSecure with dynamic code ATMs with Anti-skimming Do not store magnetic band Encrypt information with third parties Auto-fraud prevention controls Cards data tables monitoring Anti-phishing service (phishing detection/closing) Ethical Hacking (vulnerabilities detection) Cards Geo-location Admission secure procedures Personal data modification secure procedures Customer training and awareness Money recovery procedures Fraud victims assistance procedures Authentication failures management procedures Agents training and awareness Compromised or non-active users disposal procedures Card & PIN sent separately Cards activation procedure Fraud information DB Compromise points detection procedure Card theft/lost action procedure Contact-less cards controls

Cyber ubezpieczenia

Bank Zachodni WBK

Grupa Santander

CYBER UBEZPIECZENIA

Wymogi regulacyjne

Dotkliwość/ wzrost ilości zagrożeń

Rozwój Rynku Cyberubezpieczeń

ZAKRES CYBERUBEZPIECZENIA

- ✓ Utrata zysków wynikająca z błędu zabezpieczeń/systemów.
- ✓ Koszty powiadomień i obsługi klientów.
- ✓ Koszty ekspertyzy sądowej (kryminalistycznej) i rekonstrukcja danych / oprogramowania.
- ✓ Odpowiedzialność za kradzież informacji lub błędy zabezpieczeń
- ✓ Koszty opinii prawnych w związku z procedurą regulacyjną w zakresie ochrony danych i sankcje
- ✓ Wymuszenia za pośrednictwem sieci i systemów
- ✓ Koszty doradztwa dot. sytuacji kryzysowych/ publikacji związanych z wydarzeniem medialnym dotyczącym kryzysu bezpieczeństwa/danych.
- ✓ Odpowiedzialność za treści publikowane w mediach cyfrowych

KLUCZOWE ASPEKTY

- ✓ Wymogi regulacyjne stosowane w każdym z krajów
- ✓ Dotkliwość/ wzrost ilości zagrożeń
- ✓ Rozwój Rynku Cyberubezpieczeń

Plan cyberbezpieczeństwa jednostek

Bank Zachodni WBK

Grupa Santander

Plan cyberbezpieczeństwa jednostek

Zwiększenie świadomości Grupy na temat zagrożeń cybernetycznych

- Komitety Bezpieczeństwa Cybernetycznego
- Kwestie dot. bezpieczeństwa cybernetycznego na poziomie Dyrekcji

ZARZĄDZANIE

Zwiększanie świadomości i kultury ryzyka cybernetycznego wśród kadry zarządzającej

ZWIĘKSZANIE ŚWIADOMOŚCI

- Uczestnictwo w ćwiczeniach cybernetycznych
- Kursy i szkolenia z zakresu ochrony cybernetycznej
- Cybernetyczne Doradztwo Strategiczne

Przygotowanie organizacji do zarządzania ryzykami cybernetycznymi

Unowocześnienie procesów Zarządzania Cyberbezpieczeństwem

- Zarządzanie incydentami cybernetycznymi
- Dashboard dot. incydentów cybernetycznych

ZARZĄDZANIE PROCESAMI

- Wzmocnienie / rozwinięcie zdolności w zakresie cyberbezpieczeństwa Wsparcie zespołów zarządzających alertami bezpieczeństwa

ZDOLNOŚCI I TALENT

ĆWICZENIA CYBERNETYCZNE

Wdrożenie rozwiązań zapobiegających atakom cybernetycznym

Zwalczanie złośliwego oprogramowania:

- **Stanowiska pracy i sieć pracownika**
- **Stacja robocza klienta**

ZŁOŚLIWE OPROGRAMOWANIE

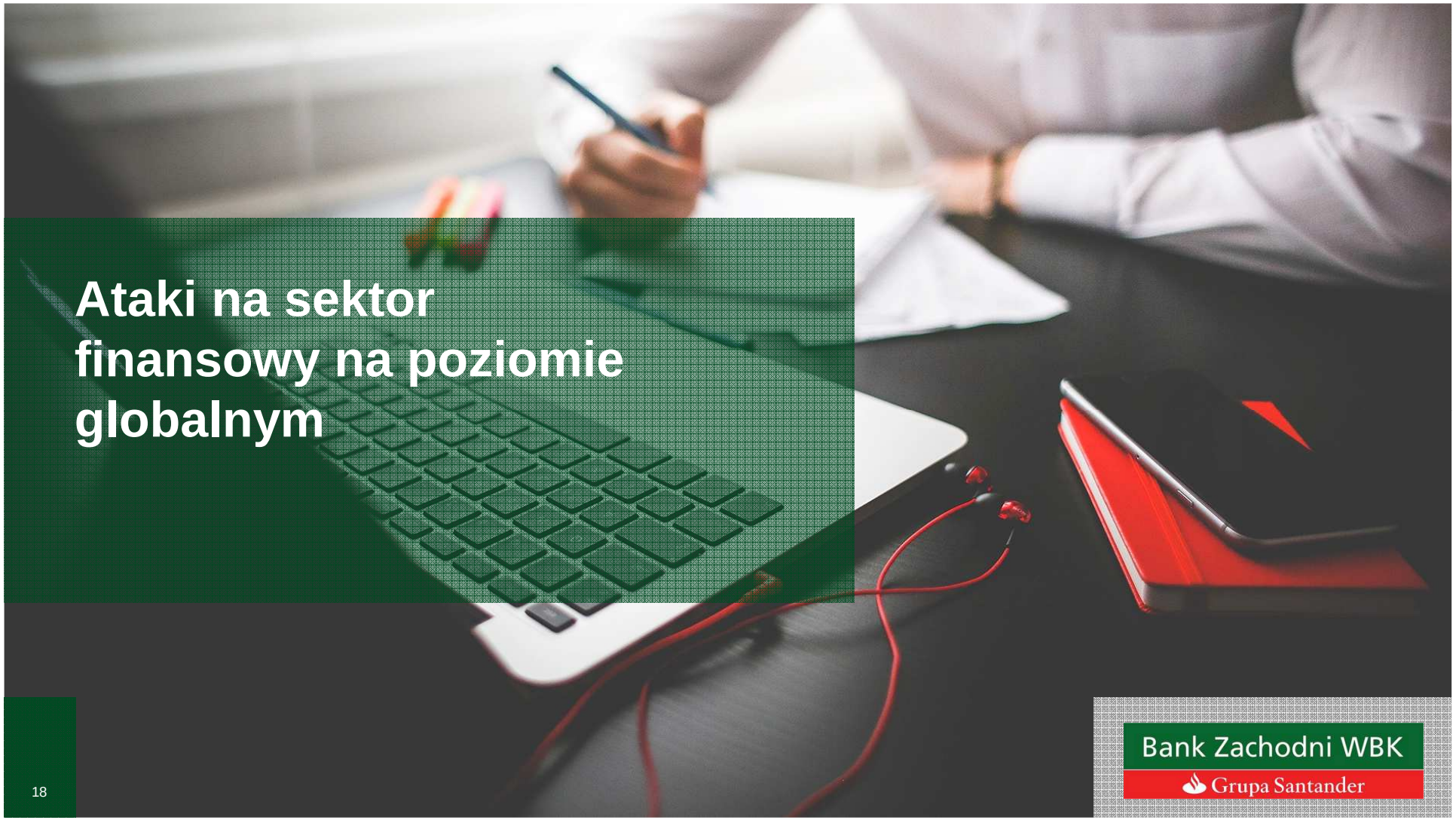
- **Zwiększenie liczby Centrum Operacji Bezpieczeństwa i analityków**
- **Wdrożenie rozwiązań w zakresie ochrony przed wyciekami danych (DLP)**

MONITORING I KONTROLA

- **Umiejętność zapobiegania DDoS**
- **Wzmocnienie zabezpieczeń telefonów i tabletów (Hardening)**
- **Bezpieczeństwo systemów**

KONFIGURACJA ZABEZPIECZEŃ

Bank Zachodni WBK
Grupa Santander



Ataki na sektor finansowy na poziomie globalnym

Bank Zachodni WBK
Grupa Santander

ATAKI NA SEKTOR FINANSOWY NA POZIOMIE GLOBALNYM

Data	Instytucja	Rodzaj
Styczeń 15	Banque Cantonale de Geneve	Kradzież/ wyciek danych
Styczeń 15	Banki niemieckie	Złośliwe oprogr. klientów
Styczeń 15	Jyske bank	Ataki typu phishing
Styczeń 15	OP Pohjola	Brak dostępu (DDoS)
Styczeń 15	Morgan Stanley	Insiders
Styczeń 15	Xoom	Złośliwe oprogr. klientów
Styczeń 15	Bitstamp (BitCoin Exchange)	Hacking
Styczeń 15	Danske Bank	Brak dostępu (DDoS)
Styczeń 15	OP Bank	Brak dostępu (DDoS)
Styczeń 15	Nordea	Hacking
Grudzień 14	Lokai Holdings	Kradzież/ wyciek danych
Grudzień 14	Co-operative Bank	Ataki typu phishing
Grudzień 14	Banki rosyjskie (Anunak)	Hacking
Grudzień 14	Banki na całym świecie (Chtonic)	Złośliwe oprogr. klientów
Grudzień 14	Citibank	Hacking
Grudzień 14	Charge Anywhere	Kradzież/ wyciek danych
Grudzień 14	Redstone Credit Union	Kradzież/ wyciek danych
Grudzień 14	TD Bank	Kradzież/ wyciek danych
Grudzień 14	PayPal	Hacking
Grudzień 14	Banki amerykańskie (FIN4)	Hacking
Grudzień 14	Bank japoński (niezidentyfikowany)	Ataki typu phishing
Październik 14	New Beginning	Kradzież/ wyciek danych
Październik 14	Bancos en Islas Vírgenes (FirstBank, Banco Popular, Scotiabank)	Kradzież/ wyciek danych
Listopad 14	UK Clearing House	Brak dostępu (DDoS)
Listopad 14	Credit Union	Kradzież/ wyciek danych
Listopad 14	TD Bank	Kradzież/ wyciek danych
Listopad 14	Goldman Sachs	Kradzież/ wyciek danych
Listopad 14	Leumi	Hacking
Listopad 14	Banki brazylijskie	Hacking
Listopad 14	HSBC Turquía	Kradzież/ wyciek danych
Listopad 14	TSB Bank	Hacking
Listopad 14	Palm Springs Federal Credit Union	Utrata sprzętu komputerowego
Październik 14	MoneyPak	Ataki typu phishing
Październik 14	Banki szwajcarskie (Dyre)	Złośliwe oprogr. klientów
Październik 14	Fidelity National Financial	Ataki typu phishing
Październik 14	Capital One	Insiders
Październik 14	GPW	Hacking
Październik 14	UK Real Time Gross Settlement	Brak dostępu (DDoS)
Październik 14	Nationwide	Brak dostępu (DDoS)
Październik 14	First National Bank	Kradzież/ wyciek danych
Październik 14	Banki amerykańskie(Qbot)	Złośliwe oprogr. klientów
Październik 14	BBVA	Insiders

● Duża dotkliwość

ATAKI NA SEKTOR FINANSOWY NA POZIOMIE GLOBALNYM

Data	Instytucja	Rodzaj	
Październik 14	Citigroup, E*Trade Financial Corp., Regions Financial Crop, HSBC Holdings i ADP	Hacking	
Wrzesień 14	IberiaBank	Kradzież/ wyciek danych	
Wrzesień 14	Banki duńskie (NemID)	Ataki typu phishing	
Wrzesień 14	Skye Bank	Insiders	
Wrzesień 14	Banki amerykańskie (Tinba)	Złośliwe oprogr. klientów	
Wrzesień 14	RBS	Złośliwe oprogr. klientów	
Wrzesień 14	Banki na całym świecie (Heartbleed)	Hacking	●
Sierpień 14	JP Morgan Chase	Kradzież/ wyciek danych	●
Sierpień 14	Santander UK	Insiders	
Sierpień 14	Delaware's Treasury Division	Hacking	
Lipiec 14	EBC	Kradzież/ wyciek danych	●
Lipiec 14	Federal Deposit Insurance Corp.	Hacking	●
Lipiec 14	Nordea i Danske Bank	Ataki typu phishing	
Lipiec 14	Benjamin F. Edwards & Co	Złośliwe oprogr. klientów	
Lipiec 14	NASDAQ	Hacking	●
Lipiec 14	TotalBank	Hacking	
Lipiec 14	Banki norweskie	Brak dostępu (DDoS)	
Lipiec 14	Prosperity Bank	Hacking	
Lipiec 14	Gateway Savings and Loans Limited	Hacking	
Lipiec 14	Sterne, Agee and Leach	Utrata sprzętu komputerowego	
Lipiec 14	Santander España	Ataki typu phishing	
Czerwiec 14	Privatbank	Hacking	
Czerwiec 14	Banki kanadyjskie(Pandemiya)	Złośliwe oprogr. klientów	
Czerwiec 14	American Express	Kradzież/ wyciek danych	●
Czerwiec 14	America First Credit Union	Kradzież/ wyciek danych	
Maj 14	Lloyds y Halifax	Hacking	
Kwiecień 14	Lloyds	Insiders	●
Kwiecień 14	NCO Financial	Kradzież/ wyciek danych	
Kwiecień 14	Banki Korei Południowej	Kradzież/ wyciek danych	●
Kwiecień 14	Ellie Mae	Brak dostępu (DDoS)	
Kwiecień 14	Experian	Kradzież/ wyciek danych	●
Marzec 14	Banki ukraińskie	Kradzież/ wyciek danych	●
Marzec 14	Oak Associates Funds	Kradzież/ wyciek danych	
Luty 14	US Federal Reserve	Hacking	●
Luty 14	Karachi Stock Exchange	Hacking	
Luty 14	Bank of the West	Kradzież/ wyciek danych	
Luty 14	Barclays	Kradzież/ wyciek danych	●
Luty 14	TD Bank	Insiders	
Styczeń 14	Bank of America y JPMorgan Chase	Brak dostępu(DDoS)	●
Styczeń 14	KB Kookmin Card, Lotte Card i NH Nonghyup Card	Kradzież/ wyciek danych	

● **Duża dotkliwość**

Dziękujemy
za poświęcony nam czas

Małgorzata Kałach,
malgorzata.kalach@bzwbk.pl

Bank Zachodni WBK
Grupa Santander