CYBER BLOCK

Polskie firmy coraz bardziej zagrożone przez hakerów

Warszawa, 14 listopada 2017 r.

Ataki hakerskie - liczba zdarzeń

96% polskich firm miało do czynienia z ponad 50 incydentami związanymi z ich danymi i informacjami w 2016 r.
(Raport „Ochrona biznesu w cyfrowej transformacji”, PWC, 2017 r.)

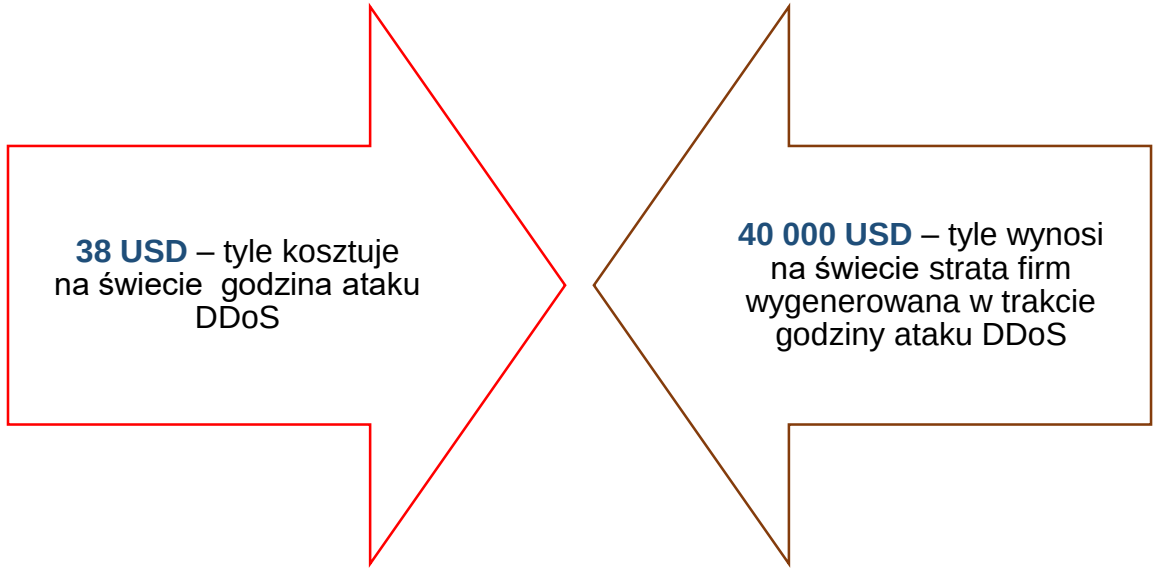
8914 zgłoszeń naruszenia cyberprzestrzeni, które były zakwalifikowane jako incydenty odnotowano w Polsce w 2015 r.
(Raport zespołu Cert.Gov.pl z 2016 r.)

193 – tyle pojawiło się na świecie nowych rodzin ransomware’u, czyli oprogramowania wykorzystywanego do wyłudzania okupu, w 2016 r.
(Raport „State of Cyber Security 2017” autorstwa F-Secure)

Ataki hakerskie - koszty

3 mld USD to łączne straty firm, jakie wygenerowali cyberprzestępcy na świecie w 2016 r.
(dane Światowego Forum Ekonomicznego z 2016 r.)

6 mld USD to szacunkowa wartość rocznych strat w 2021 r., jakie poniosą firmy na świecie na skutek działalności cyberprzestępców
(dane Światowego Forum Ekonomicznego z 2016 r.)



Raport Hewlett Packard i Ponemon Institute, 2016 r.

Ataki hakerskie – najczęstsze metody

Phishing: polega na podstępnym wyłudzeniu od użytkownika jego danych osobistych. Obejmuje kradzież haseł, numerów kart kredytowych, danych kont bankowych i innych poufnych informacji. Wiadomości phishingowe najczęściej są fałszywymi powiadomieniami z banków, komunikatami od dostawców systemów e-płatności i innych poważanych organizacji. Wiadomość zawsze próbuje zachęcić odbiorcę pod pretekstem utraty krytycznych danych, awarii systemu do wprowadzenia lub zaktualizowania swoich poufnych informacji

Główne cele phisherów to banki, elektroniczne systemy płatności oraz aukcje internetowe.

(6.11.2017): informacja o ataku na użytkowników **Netfliksa**

Spear phishing (atak celowany): mechanizm podobny do zwykłego phishingu, oparty na wysłaniu do ofiary e-mail, który wydaje się pochodzić od zaufanej osoby bądź organizacji. Celem ataku są pojedyncze osoby, wobec których oszust przeprowadza pogłębiony wywiad środowiskowy oparty na informacjach dostępnych w internecie

Ostatnie komunikaty dot. cyberprzestępczości:

- (8.11.2017 r.): Chińska klawiatura MantisTek GK2 z keyloggerem
- (10.11.2017 r.): Atak hakerów na stronę www lotniska w Modlinie – zablokowanie strony

Wyzwanie dla polskich firm - RODO

25 maja 2018 r. - wejście w życie rozporządzenia Parlamentu Europejskiego i Rady Europejskiej w sprawie ochrony osób fizycznych, w związku z przetwarzaniem danych osobowych i ich swobodnym przepływem (w skrócie RODO).

Czego dotyczy RODO:
Dotyczy wszystkich podmiotów, które w związku z prowadzoną działalnością gospodarczą przetwarzają dane osobowe.

Jakie zmiany przynosi RODO:
Obowiązek przedsiębiorcy polegający na doborze odpowiednich środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa w procesie przetwarzania danych osobowych.

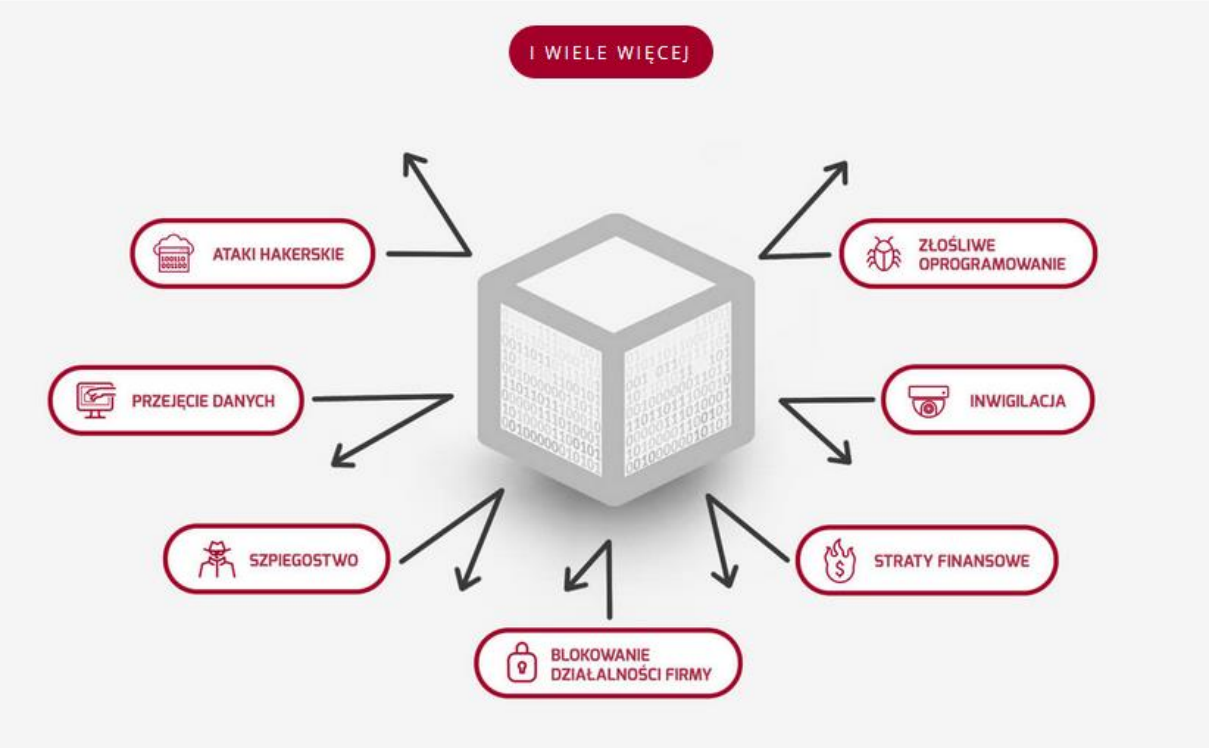
- Ze względu na rosnące zagrożenie cyberatakami i ewoluujące metody takich działań, proces ten powinien być cyklicznie monitorowany, tak, aby pozwalał skutecznie reagować na wszelkie zagrożenia i potencjalne wycieki danych.

Nowe obowiązki nałożone na Przedsiębiorców przez RODO:

- Szyfrowanie danych osobowych,
- Zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów,
- Zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
- Regularne testowanie, mierzenie i ocena skuteczności środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzania.

Kary przewidziane przez RODO:
Naruszenie postanowień rozporządzenia będzie podlegało grzywnie pieniężnej. Kara może wynieść nawet **20 000 000 EUR**, a w przypadku przedsiębiorstwa **– 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.**

Jak działamy



Nasz zespół tworzy grupa ekspertów. Jesteśmy informatykami, inżynierami oraz analitykami, których łączy wieloletnie doświadczenie w obszarze techniki specjalnej i bezpieczeństwa informatycznego.

Pomagamy naszym Klientom na każdym etapie procesu zapewnienia bezpieczeństwa informacji. Poszukując najlepszych rozwiązań dla naszych Klientów, stale współpracujemy z najlepszymi praktykami i specjalistami branżowymi. W ten sposób możemy zaoferować profesjonalne rozwiązania nawet najbardziej skomplikowanych zagadnień, trapiących naszych Klientów. Kierujemy się przy tym zasadą etyki i lojalności wobec nich. Oferujemy ponad standardowe zaangażowanie się w wykonywanie zadań, dyskrecję oraz wysoką kulturę osobistą.

Nasz zespół

Białe Kapelusze (White Hats)

Działający zgodnie z prawem hakerzy, zajmujący się wyszukiwaniem luk w systemach bezpieczeństwa. Specjaliści do spraw szeroko rozumianego bezpieczeństwa IT. Posiadają doświadczenie w prowadzeniu audytów bezpieczeństwa, testów penetracyjnych oraz wdrożeniach procedur bezpieczeństwa. Współpracowali m.in. z instytucjami państwowymi w obszarze cyberprzestępczości. Praktycy posiadający m.in. poświadczenie bezpieczeństwa z klauzulą „ściśle tajne", operujący na specjalistycznym oprogramowaniu i urządzeniach forensic, służącym do badań urządzeń mobilnych UFED, XRY, Mobiledit czy Oxygen. Uczestnicy Akademii Cisco oraz autoryzowanych szkoleń CISCO CWENT, CISCO BCMSN oraz CISCO SI POBYT. Część członków grupy jest biegłymi sądowymi z zakresu informatyki śledczej. W ramach programu ISEC – Europol brali udział w szkoleniu Vista Forensic Training Course. Niektórzy członkowie zespołu posiadają certyfikat FBI – Introdution to network capture and analysis course. Ukończyli też certyfikowane szkolenie Certified Ethical Hacker.

Jarosław Bartniczuk, Prezes Zarządu

Jest absolwentem Wojskowej Akademii Technicznej i Politechniki Warszawskiej. Zdobywał doświadczenie pracując na polu technicznych zabezpieczeń najważniejszych osób i obiektów rządowych w kraju i zagranicą. Od 7 lat zajmuje się bezpieczeństwem teleinformatycznym, korporacyjnym w zakresie ochrony informacji, IT i danych osobowych. Posiada Certyfikat Inżyniera Bezpieczeństwa ISecMaan Information Security Management ,,Projektowanie Systemu Zarządzania Bezpieczeństwem Informacji w/g ISO 27001'' oraz Certyfikat Audytora Wewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji wg ISO 27001:2005.

Nasz zespół

Piotr Bazylewicz, Wiceprezes Zarządu

Od początku swojej kariery zawodowej związany z branżą IT&T. Przed objęciem stanowiska w CyberBlock, aktywnie działał na polskim rynku nowych technologii, m.in. firmie COMP S.A. przy realizacji zagadnień związanych platformą szyfrowania łączności rządowej oraz jako dyrektor handlowy w Asseco Poland, gdzie był współodpowiedzialny m. In. za zintegrowane rozwiązania systemowe z portfela obronności dla państw członkowskich Paktu Północnoatlantyckiego, Wojska Polskiego i służb specjalnych. Project Manager, zawodowo związany z procesem stanowienia prawa.

Katarzyna Majewska, Dyrektor ds. Operacyjnych

Przez ostatnie lata aktywna w sektorze bezpieczeństwa gospodarczego. Jako analityk realizowała projekty dla kancelarii prawnych, funduszy akcyjnych oraz spółek nowych technologii w zakresie audytu, doradztwa biznesowego i transakcyjnego. Jednocześnie współpracowała z kancelarią prawną gdzie była odpowiedzialna za obsługę prawną spółek kapitałowych oraz wsparcie prawno - administracyjne dla działalności firm. Absolwentka Wydziału Prawa i Administracji na Uniwersytecie Warszawskim.

biuro@cyberblock.pl

ul. Stanisława Moniuszki 1A
00-014 Warszawa