GREY WIZARD

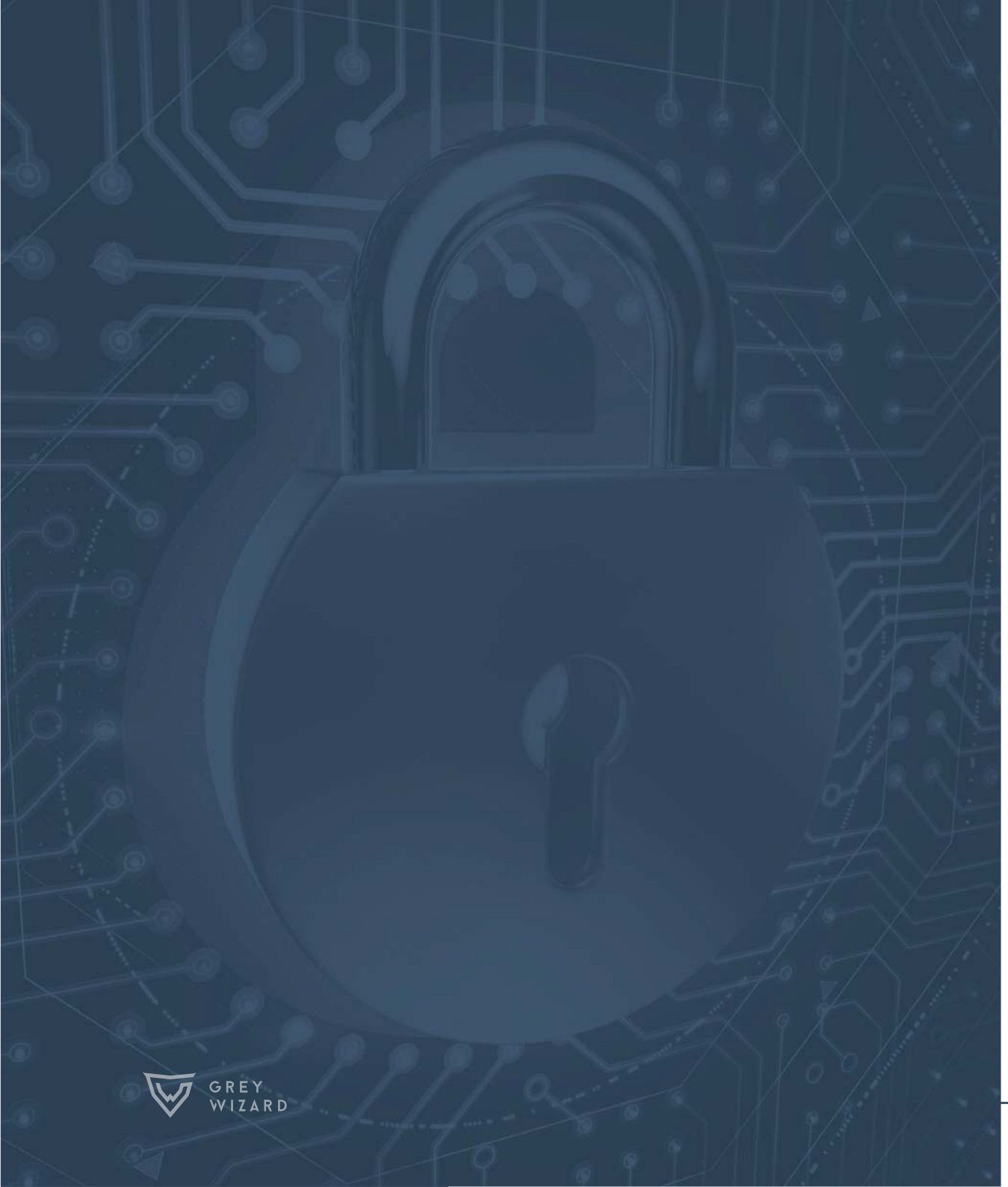
CYBERBEZPIECZEŃSTWO W Q4 2017 ROKU

Spis treści

Cyberbezpieczeństwo to priorytet najwyższej wagi. Każdego roku specjaliści do spraw bezpieczeństwa cybernetycznego stają przed nowymi wyzwaniami oraz nowymi typami i sposobami ataków. Hakerzy cały czas pracują nad nowymi metodami przeprowadzania cyberataków. By wykraść wrażliwe dane, pieniądze lub zablokować dostęp do witryny hakerzy wykorzystują luki w systemach aplikacji internetowych oraz nadal słabo chronione urządzenia Internetu Rzeczy. W 2018 roku możemy spodziewać się jeszcze większej ilości zmasowanych cyberataków. Dlatego, mówiąc o cyberbezpieczeństwie małych, jak i dużych firm, warto zacząć myśleć globalnie i już dziś zaplanować budżet na cyberochronę.

Radosław Wesołowski, CEO Grey Wizard

Wstęp



GREY WIZARD

XXI wiek jest niewątpliwie wiekiem technologii. Komputery, laptopy, smartfony, tablety, urządzenia IoT, samochody te wszystkie rzeczy, tak jak ludzie i firmy są połączone z siecią. Szacuje się, że ich liczba do 2020 roku przekroczy 50 miliardów. Takie rozwiązanie ułatwia pracę i życie codzienne, ale równocześnie rodzi zagrożenia na nieznaną dotąd skalę.

Nowoczesne cyberbezpieczeństwo stoi przed wieloma wyzwaniami, a wiedza z dziedziny cyberzagrożeń niemal codziennie ulega dezaktualizacji. Zapewnienie odpowiedniej ochrony, znalezienie właściwych i skutecznych metod odpierania cyberataków to wyzwanie specjalistów do spraw bezpieczeństwa. Właściwa identyfikacja zagrożenia oraz procedury postępowania w przypadku wystąpienia incydentów bezpieczeństwa stanowią priorytet w walce z zagrożeniami.

Obecnie cyberprzestępca nie musi znać się na złośliwym oprogramowaniu, może je kupić i skierować atak na dowolną stronę. Takie działanie bardzo często sieje ogromne spustoszenie na atakowanej stronie. Dlatego wykrywanie i zwalczanie incydentów wymaga obecnie najnowocześniejszych rozwiązań opartych na Machine Learning i sztucznej inteligencji.

Nie da się zapobiegać zagrożeniom na dużą skalę bez wsparcia ludzkiej pracy inteligentną technologią. Tylko takie rozwiązanie jest w stanie skutecznie przeciwdziałać i odpierać cyberataki.

Zapraszamy do lektury raportu dotyczącego cyberbezpieczeństwa w 2017 roku.

PODSUMOWANIE CYBERBEZPIECZEŃSTWA NA ŚWIECIE W 2017 ROKU

PODSUMOWANIE CYBERBEZPIECZEŃSTWA NA ŚWIECIE W 2017 ROKU

$11,7MLN

ŚREDNI KOSZT CYBERPRZESTĘPSTWA

22,7%

PROCENTOWY WZROST KOSZTÓW CYBERPRZESTĘPSTWA

01. Koszty cyberprzestępczości

PODSUMOWANIE CYBERBEZPIECZEŃSTWA NA ŚWIECIE W 2017 ROKU

130

ŚREDNIA LICZBA NARUSZEŃ BEZPIECZEŃSTWA

27,4%

PROCENTOWY WZROST ŚREDNIEJ ROCZNEJ LICZBY NARUSZEŃ BEZPIECZEŃSTWA

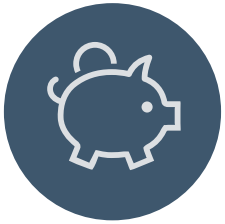
02. Trzy najważniejsze motywy przeprowadzania cyberataków

GREY WIZARD

PODSUMOWANIE CYBERBEZPIECZEŃSTWA NA ŚWIECIE W 2017 ROKU

Ataki hakerskie są coraz powszechniejsze, złożone i wyrafinowane. W celu wyłudzenia pieniędzy i kradzieży danych wrażliwych, cyberprzestępcy korzystają z zaawansowanych algorytmów oraz technik socjotechnicznych. Nieświadomi zagrożenia pracownicy prywatnych przedsiębiorstw i jednostek sektora publicznego oraz osoby prywatne są łatwą ofiarą hakerów. Pozyskane dane są dla hakerów cennym towarem, a rynek nielegalnego handlu nimi rośnie. Rozwój technologii sprawia, że ataki są również coraz łatwiejsze do wykonania oraz nie wymagają specjalistycznej wiedzy. Dlatego z roku na rok wzrasta liczba przeprowadzonych cyberataków.

Wykrycie i zatrzymanie cyberataku wymaga wsparcia wykwalifikowanych specjalistów oraz zaawansowanych technologicznie narzędzi. W 2017 roku doświadczyliśmy zmasowanych cyberataków o globalnym zasięgu oraz ogromnym wycieku danych osobowych.



50%

ZYSK FINANSOWY

45%

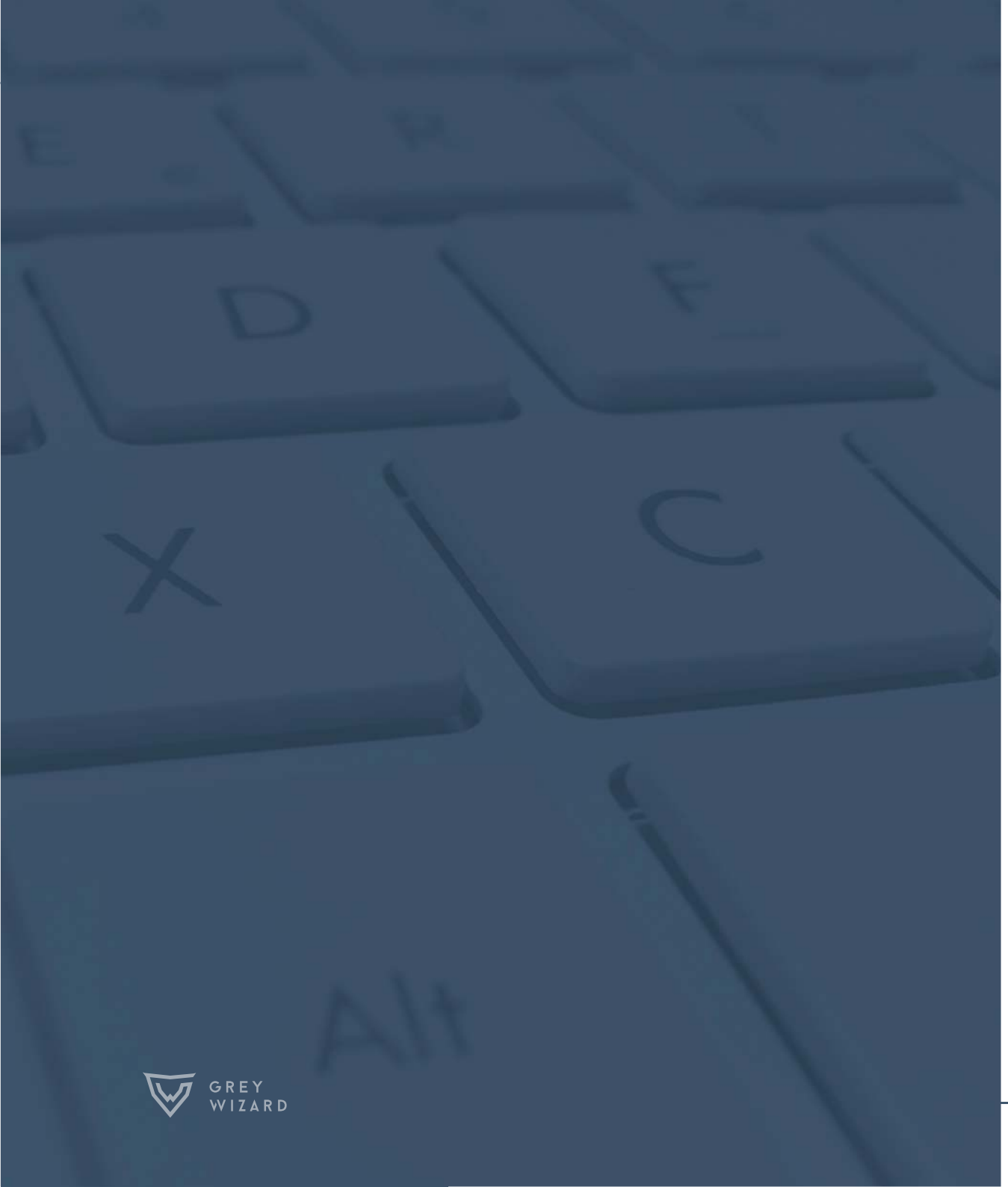
ZAKŁÓCENIA USŁUGI

37%

KRADZIEŻ DANYCH OSOBOWYCH

03. Trzy najważniejszych motywy przeprowadzania cyberataków

GREY WIZARD



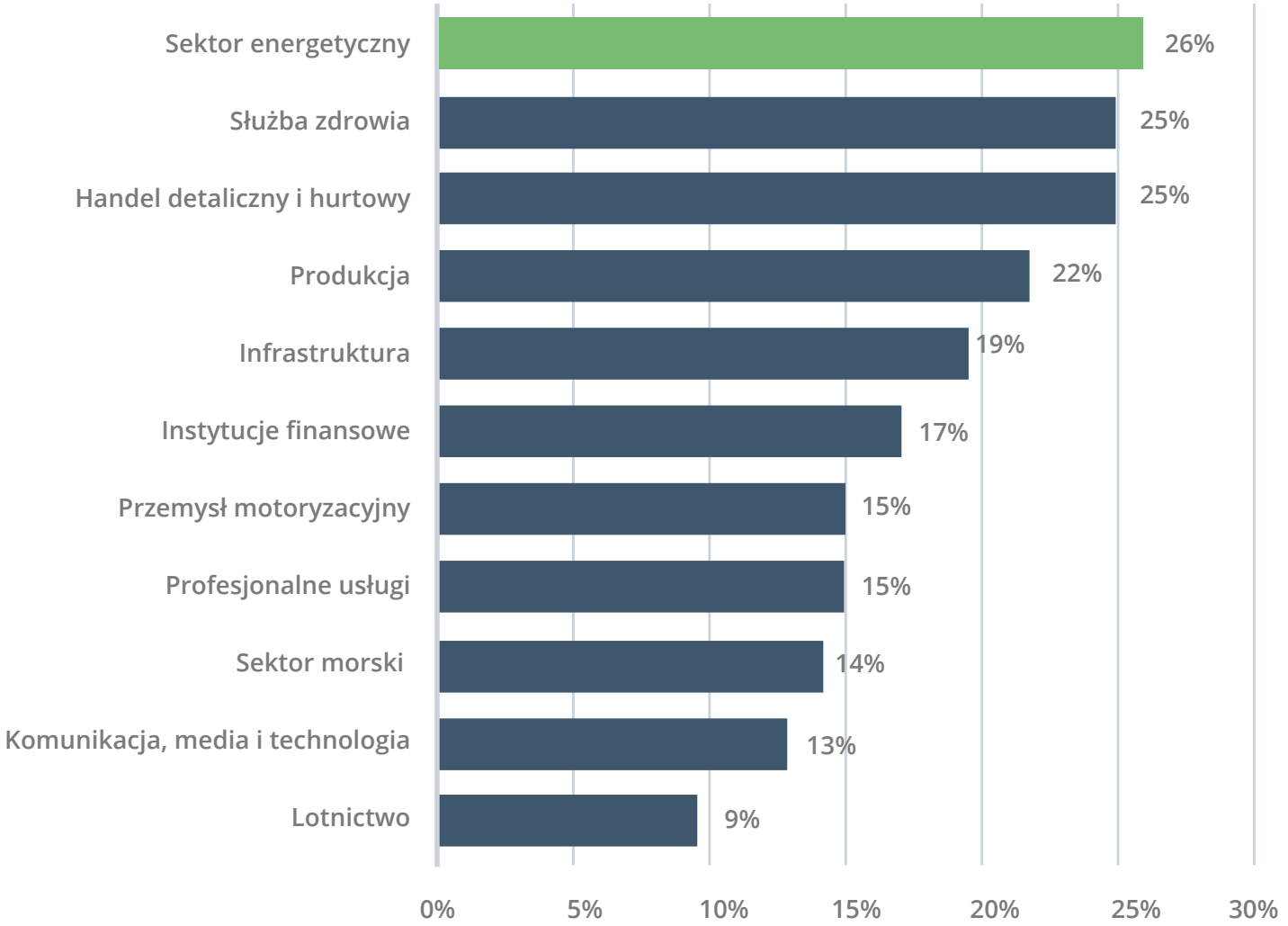
GREY WIZARD

W 2017 roku doszło do wielu naruszeń danych. Świat obiegły informacje o kradzieży danych z Equifax, Verizon czy Kmart. Infrastruktura wielu firm została również sparaliżowana przez ataki Petya, WannaCry, BadRabbit. Te wszystkie incydenty naruszenia bezpieczeństwa, przyniosły ogromne straty finansowe i wizerunkowe. Do przeprowadzania zmasowanych cyberataków hakerzy wykorzystywali również urządzenia IoT (Internet of Things).

2017 rok to przede wszystkim ataki typu ransomware, malware, phishing, ataki na warstwę sieciową, ataki DDoS oraz botnety. Najczęstszym celem cyberataków były firmy z sektora energetycznego, służby zdrowia, sprzedaży detalicznej oraz produkcji. Zagrożony był również sektor finansowy i instytucje państwowe.

Skutkami ataków hakerskich są w pierwszej kolejności straty finansowe, spadek reputacji oraz utrata klientów.

PODSUMOWANIE CYBERBEZPIECZEŃSTWA NA ŚWIECIE W 2017 ROKU



04. Branże dotknięte cyberatakami na całym świecie. Dane od września 2017 roku

GREY WIZARD

Firmy, które w 2017 roku padły ofiarą cyberataku:

- 22% firm utraciło klientów, a 40% z nich straciło ponad 20% istniejącej bazy klientów,
- 29% firm odnotowało spadek przychodów, z czego 38% na poziomie przekraczającym 20%,
- 23% firm uważa, że włamania ograniczyły możliwość rozwoju biznesu, a 42% z nich szacuje stratę w potencjalnych dochodach na ponad 20%.

Dynamiczne zmiany technologiczne i postępująca digitalizacja stwarzają nowe możliwości dla atakujących. Choć hakerzy nadal posługują się tradycyjnymi metodami ataku, to jednocześnie wykorzystują nowe, zaawansowane metody cyberataków.

WYBRANE ATAKI HAKERSKIE Z 2017 ROKU

Luty

KOMISJA NADZORU FINANSOWEGO

Komisji Nadzoru Finansowego i banki padły ofiarą cyberataku. Atak dotyczył danych gromadzonych przez instytucje sektora bankowego. Atak na banki rozprzestrzeniał się przez stronę KNF. Komputery KNF były zainfekowane kilka miesięcy przed wykryciem ataku.

Marzec

YAHOO

Amerykański portal internetowy Yahoo przez dwa lata był atakowany przez hakerów. Ich celem było zdobycie informacji politycznych i gospodarczych. Cyberprzestępcy zdołali wykraść dane do 500 milionów kont użytkowników. Wśród skradzionych danych znalazły się nazwy użytkowników, pomocnicze adresy e-mail, zaszyfrowane hasła i numery telefonów. Do logowania się do kont użytkowników hakerzy używali fałszywych plików cookie.

Kwiecień

WONGA

W wyniku ataku na serwery serwisu Wonga, który oferuje pożyczki online, do sieci wyciekło 300 tysięcy danych osobowych byłych i obecnych klientów. W ręce hakerów dostały się informacje o imieniu i nazwisku, numerze telefonu, PESEL i numery dowodu osobistego. Wyciek dotyczył głównie klientów z Wielkiej Brytanii i Polski.

Maj

MYSPACE

Z portalu MySpace wyciekło 360 milionów adresów e-mail i haseł użytkowników. Wszystkie dane wrażliwe zostały opublikowane w sieci, a ich wartość na czarnym rynku wynosi 2 800 dolarów.

Maj

WannaCry

Szkodliwe oprogramowanie ransomware WannaCry zaatakowało 21 maja 2017 roku. Atak WannaCry dotknął ponad 300 tysięcy komputerów w 99 krajach. Wirus uderzył w jednostki użyteczności publicznej, duże korporacje, uniwersytety, przewoźników kolejowych, fabryki samochodów, instytucje finansowe. Dotknął i osłabił działanie szpitali i placówek służby zdrowia w Wielkiej Brytanii.

Złośliwy robak internetowy WannaCry lub Wanna Decryptor wykorzystuje luki w zabezpieczeniach systemu Windows. Po zarażeniu systemu, następowało zaszyfrowanie danych. Aby je odblokować hakerzy żądali 300-600 dolarów płaconych w BitCoinach.

Ten potężny ransomware rozprzestrzeniał się, gdy nie mógł nawiązać połączenia z niezarejestrowaną domeną uqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com. Darien Huss, który odkrył sposób działania wirusa, zarejestrował domenę i ataki ustały.

Atak WannaCry zasiał spustoszenie w wielu firmach blokując im dostęp do systemu. Robak zagroził hostom, zaszyfrował pliki przechowywane na komputerach i żądał zapłaty w BitCoin. WannaCry rozprzestrzeniał się w oparciu o luki w systemie zabezpieczeń Windows.

Czerwiec

Petya/Not Petya

Petya / Not Petya to kolejnym ransomware o globalnej skali. Oprogramowanie było bardziej zaawansowane niż WannaCry. Atakiem zostały dotknięte firmy i instytucje, które posiadały zaktualizowanego Windowsa. Wirus Petya posiadał wady w postaci nieskutecznego i niewydajnego systemu płatności.

Analiza specjalistów wykazała, że nie był to dokładnie Petya, a jedynie ransomware wykorzystujący niektóre mechanizmy Petya. Eksperci z Kaspersky Lab stwierdzili, że złośliwe oprogramowanie różni się od wcześniej znanych wersji Petyi, stąd jego druga nazwa NotPetya.

Wirus NotPetya zainfekował i sparaliżował instytucje publiczne, systemy bankowe, firmy komunikacyjne i teleinformatyczne na całym świecie. Atak najbardziej dotknął Ukrainę, Danię, Rosję i Wielkę Brytanę. Ucierpiały też firmy m.in. z Polski, Niemiec, Norwegii czy Stanów Zjednoczonych. Podobnie jak w przypadku WannaCry, hakerzy żądali okupu w wysokości 300 dolarów płatnych w BitCoinach.

KMART

Cyberatak na amerykańską sieć supermarketów Kmart powinien być sygnałem dla sprzedawców detalicznych, by zadbać o ochronę przechowywanych danych. Systemy płatności sieci Kmart zostały zainfekowane złośliwym kodem, który był niewykrywalny przez istniejące systemy antywirusowe. Celem hakerów stały się karty kredytowe klientów, które hakerzy używali do prowadzenia nieuprawnionej działalności. Kmart nie ujawnił informacji w ilu sklepach zostały naruszone dane klientów.

Lipiec

VERIZON

Verizon, największy operator telefonii komórkowej w Stanach Zjednoczonych, padł ofiarą cyberataku i stracił ponad 14 milionów danych osobowych swoich klientów. Wrażliwe dane, które znajdowały się na niezabezpieczonym serwerze chmurowym, odkrył Chris Vickery, ekspert do spraw cyberbezpieczeństwa. Ujawnione informacje zawierały imiona i nazwiska, numery telefonu oraz poufny numer PIN klientów. Te informacje wystarczyły, by każdy, kto je posiada, mógł uzyskać dostęp do konta danej osoby.

Wrzesień

EQUIFAX

Wyciek danych wrażliwych z firmy Equifax, jednej z największych agencji informacji kredytowych, dosięgnął ponad 143 milionów Amerykanów, około 400 tysięcy Brytyjczyków i Kanadyjczyków. Atak miał trwał od maja do lipca. W ręce hakerów dostały się dane takie jak imiona i nazwiska, adresy, numery ubezpieczeń społecznych, numery praw jazdy czy kart kredytowych.

Aby uzyskać dostęp do danych przechowywanych przez Equifax, cyberprzestępcy wykorzystali lukę w zabezpieczeniach aplikacji na stronie internetowej. Do walki z hakerami firma wynajęła firmę specjalizująca się w bezpieczeństwie cybernetycznym.

Październik

Bad Rabbit

Ransomware Bad Rabbit to nowa wersja oprogramowania Not Petya. Robak zaatakował m.in. kijowskie metro, lotnisko w Odessie, ukraińskie Ministerstwo Infrastruktury oraz rosyjskie agencje prasowe Interfax i Fontanka. Aby zainstalować wirusa, ofiara musiała zezwolić na instalację zainfekowanej wcześniej wtyczki Flash Playera. Aby odzyskać dostęp do danych ofiara musiała w ciągu 40 godzin wpłacić 0,05 BTC, w przeciwnym razie kwota wzrastała.

Szkodliwe oprogramowanie Bad Rabbit dosięgnęło 15 krajów na całym świecie. Jednak najwięcej, aż 70% ofiar było ulokowanych na terenie Rosji, a 14% na terenie Ukrainy.

13% kodu źródłowego była taka sama jak w przypadku Not Petya. Przemawia za tym podobna struktura kodu, metody sprawdzania istniejących procesów, ze 113 rozszerzeń plików szyfrowanych przez Bad Rabbit, aż 65 jest szyfrowanych przez Not Petyę.

Grudzień

BITFINEX

Bitfinex, jedna z największych giełd kryptowalutowych na świecie padła ofiarą ataku DDoS. Ataki trwały od kilku godzin nawet do kilku dni. Masowe zapytania z fikcyjnymi transakcjami do serwera były wysyłane tak długo, aż ten przestał na nie odpowiadać. W konsekwencji atak DDoS zablokował większość transakcji prawdziwych klientów.

KRAJE POCHODZENIA ATAKÓW

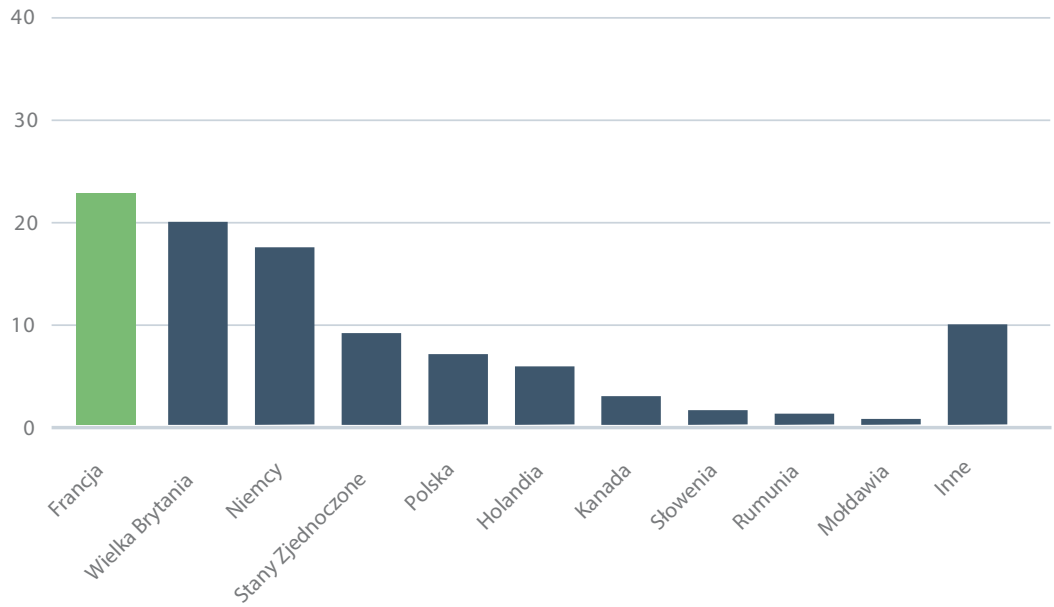
KRAJE POCHODZENIA ATAKÓW

W czwartym kwartale 2017 roku zarejestrowaliśmy 167 324 652 ataków. Najwięcej, bo aż 22,04% wszystkich incydentów bezpieczeństwa i ataków, które były skierowane na strony chronione przez Grey Wizard Shield pochodziła z Francji.

Na drugim miejscu wśród krajów źródłowych cyberataków znalazła się Wielka Brytania - 20,08%. Kraje, z których zarejestrowaliśmy wzmożony ruch to również Niemcy 18,73%, Stany Zjednoczone 9,07% oraz Polska 7,81%.

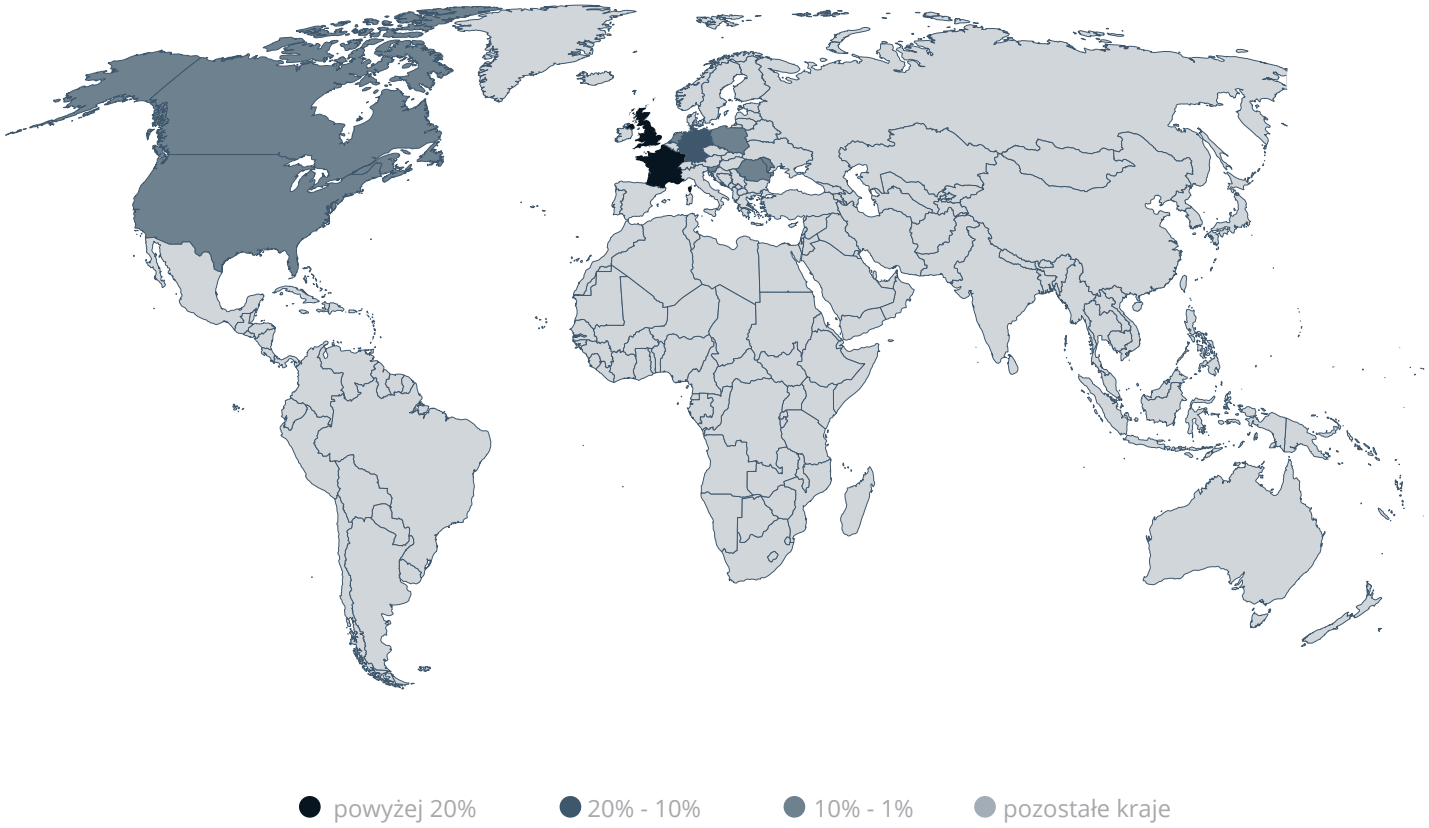
Pozostałe kraje z dość wysokim wskaźnikiem incydentów i zaangażowania cyberprzestępców to Holandia 5,12% i Kanada 2,35%. Ze Słowenii zarejestrowaliśmy 1,60%, z Rumunii 1,53%, a z Mołdawii 1,35%.

Ataki z innych krajów wyniosły 10,32%. Należą do nich kraje z aktywnością incydentów i ataków poniżej 1%. Były to m.in. Ukraina 0,95% i Węgry 0,73%.



05. Kraje pochodzenia cyberataków

KRAJE POCHODZENIA ATAKÓW



06. Kraje pochodzenia cyberataków

CZAS TRWANIA CYBERATAKÓW

CZAS TRWANIA CYBERATAKÓW

Czas trwania cyberataków ma ogromny wpływ na przedsiębiorstwo. Im dłuższy atak tym większe szkody finansowe i wizerunkowe ponosi atakowana firma. Najczęściej celem cyberataków jest ograniczenie dostępności serwisu internetowego, kradzież wrażliwych danych i treści strony oraz pieniędzy.

W Q4 2017 roku zarejestrowaliśmy 167 324 652 incydentów. Dziennie liczba incydentów wynosiła średnio 1 394 372,1.

1 394 372,1

ŚREDNIA LICZBA INCYDENTÓW DZIENNIE

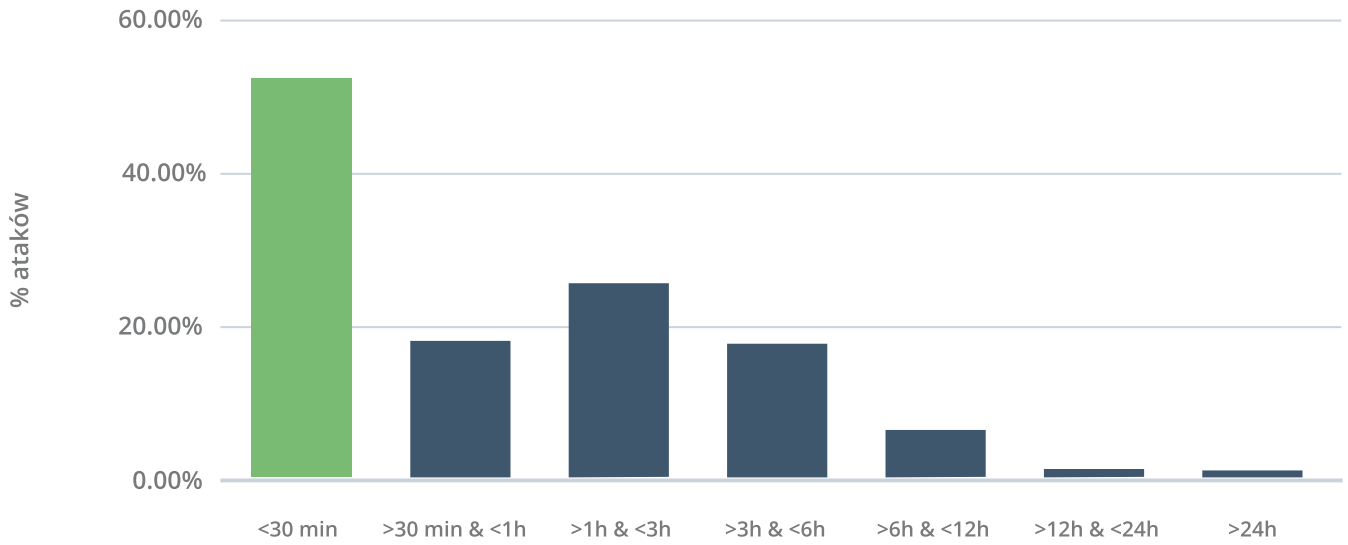
GREY WIZARD

CZAS TRWANIA CYBERATAKÓW

Najwięcej, aż 52,83% stanowiły ataki Brute Force trwające mniej niż 30 minut. Zaraz po nich zarejestrowaliśmy ataki, które trwały od 1-3 godzin. Te ataki stanowiły 28,77% wszystkich incydentów. 18,40% stanowiły ataki od 30-60 minut oraz od 3-6 godzin (18,87%).

Najmniej cyberataków, ponieważ tylko 1,42% to ataki trwające od 12-24 godzin oraz powyżej 24 godzin.

Z tych danych wynika, że ataki poniżej 30 minut "cieszą się" na czarnym rynku największą popularnością. Wynika to z niskich kosztów takich ataków (koszt to kilka do kilkunastu dolarów). Cyberprzestępcy wykorzystują krótkie, ale intensywne ataki, by zakłócić działania usług internetowych, jednocześnie mają świadomość, że nawet chwilowy brak dostępu do serwisu jest w stanie wygenerować wiele strat.



07. Czas trwania ataków Brute Force

TYPY ATAKÓW APLIKACYJNYCH

TYPY ATAKÓW APLIKACYJNYCH

Internet przyzwyczaił nas do wygody. Naturalne jest dla nas robienie zakupów online, blogowanie, korzystanie z usług bankowych, robienie rezerwacji hotelowych czy nawet korzystanie z internetowych usług instytucji państwowych. To wszystko jest nieodłączną częścią współczesnego świata. Wzrost usług internetowych sprawił, że jednocześnie wzrosła liczba atakowanych stron i aplikacji internetowych.

W Q4 2017 roku łączna liczba incydentów, którą zanotowaliśmy wynosiła 167 324 652. Składały się na nie następujące typy ataków aplikacyjnych:

- SQL Injection
- Illegal Resource Access
- Security Vulnerability Scanners
- Software Crawlers
- Cross Site Scripting (XSS)
- Shellshock

Najpopularniejszym typem ataku aplikacyjnego w Q4 2017 był SQL Injection. Liczba incydentów wyniosła 40,53% wszystkich ataków. SQL Injection (SQLi) to metoda cyberataku polegająca na wstrzykiwaniu dodatkowych procedur do zapytania SQL, które

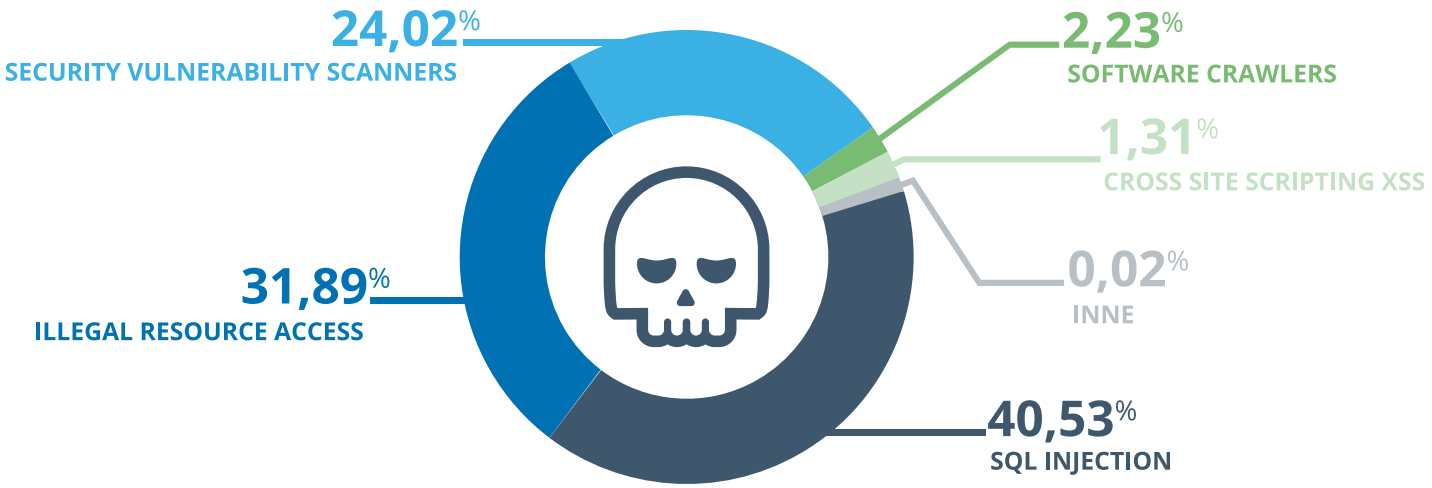
wygenerowane przez aplikacje są przekazywane do bazy danych i tam wykonywane.

Na drugim miejscu wśród najpopularniejszych typów incydentu znalazł się Illegal Resource Access, czyli nielegalny dostęp do zasobów - 31,89%. Są to wszystkie nielegalne działania mające na celu uzyskanie dostępu do stron prywatnych lub zastrzeżonych oraz próby wyświetlenia bądź kradzieży plików systemowych.

24,02% incydentów to Security Vulnerability Scanners, czyli ataki skierowane na skanery podatności aplikacji internetowych na zagrożenia.

Najmniej incydentów odnotowaliśmy z wykorzystaniem typu ataku Cross Site Scripting (XSS) - 1,31%. Atak XSS (Cross-site scripting) jest wykonywany po stronie przeglądarki. Jest to atak na klienta podatnej aplikacji WWW. Zagraża on samej aplikacji i danym znajdującym się po jej stronie.

TYPY ATAKÓW APLIKACYJNYCH



09. Procentowy rozkład incydentów

Hakerzy coraz częściej wykorzystują luki w zabezpieczeniach warstwy aplikacyjnej. Z kilku powodów jest ona częstym celem cyberataków. Po pierwsze przechowuje dane użytkowników, takie jak dane osobowe, numery kart kredytowych czy loginy i hasła. Po drugie warstwa aplikacyjna obsługuje protokoły m.in. HTTP, SQL, DNS, SNMP, FTP i inne. Brak właściwych zabezpieczeń tych protokołów daje hakerom możliwość skorzystania z wielu potencjalnych metod ataków. Po trzecie, ataki skierowane na warstwę aplikacyjną są skomplikowane i często trudne do wykrycia. Dlatego, aby skutecznie chronić przed tego typu atakami należy używać równie skomplikowanych i inteligentnych mechanizmów obrony. Najlepszym rozwiązaniem jest posiadanie ochrony Web Application Firewall, która m.in. zapewnia całodobową automatyczną ochronę przed atakami aplikacyjnymi, posiada niski współczynnik fałszywych alarmów i ma możliwość definiowania wyjątków.

Radosław Wesołowski, CEO Grey Wizard

BEZPIECZEŃSTWO SYSTEMÓW DO ZARZĄDZANIA TREŚCIĄ

BEZPIECZEŃSTWO SYSTEMÓW DO ZARZĄDZANIA TREŚCIĄ

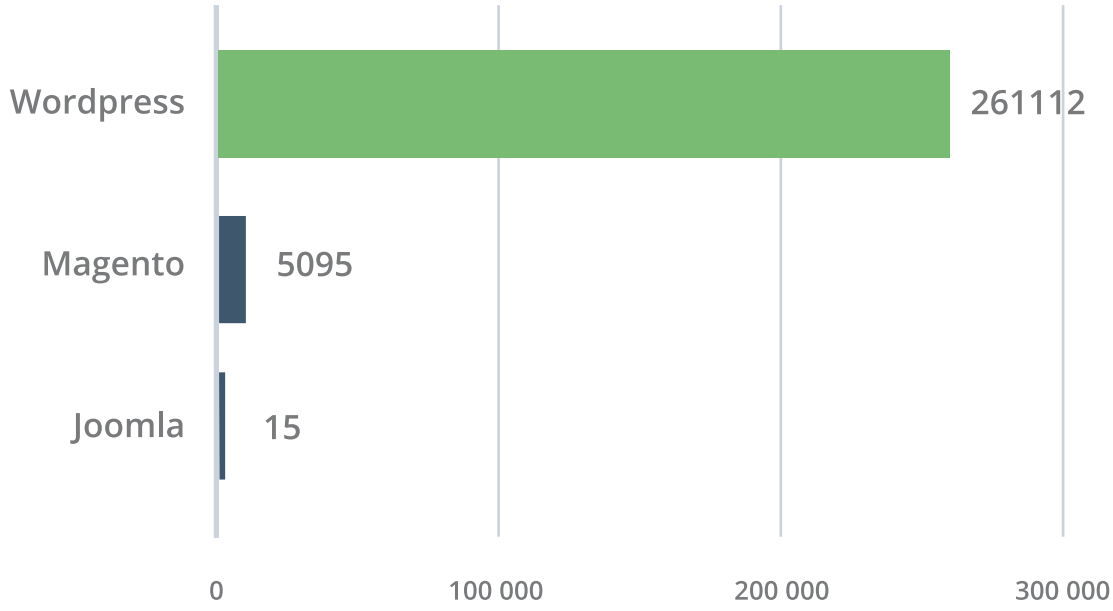
Systemy zarządzania treścią to oprogramowanie pozwalające na tworzenie serwisu www oraz jego późniejszą aktualizację i rozbudowę. W Q4 2017 system WAF Grey Wizard Shield odnotował aż 266 222 incydentów powiązanych z wadami tych systemów.

Z chronionych przez nas platform, największa uwaga hakerów była skierowana na platformę WordPress. Zarejestrowaliśmy aż 261 112 incydentów naruszających bezpieczeństwo przechowywanych danych, co stanowi 98,1%. Liczba ataków na system CMS WordPress wynika z jego dużej popularności - jest na niej zbudowanych ponad 24% stron na świecie. Najczęstszym powodem zaniedbań bezpieczeństwa jest częsty brak aktualizacji oraz duża podatność na ataki dodatków do systemu WordPress.

1,91% incydentów odnotowaliśmy na platformę Magento. Jest to jedna z najbardziej rozbudowanych platform do obsługi dużych sklepów internetowych. Obsługuje blisko 10% wszystkich sklepów internetowych.

10. Liczba incydentów, a typ incydentu

BEZPIECZEŃSTWO SYSTEMÓW DO ZARZĄDZANIA TREŚCIĄ



11. Liczba incydentów, a typ incydentu

ATAKI BRUTE FORCE CREDENTIAL STUFFING

ATAKI BRUTE FORCE CREDENTIAL STUFFING

W czasach szybkiego internetu hakerzy wykorzystują wiele metod cyberataków. W Q4 2017 roku odnotowaliśmy aż 212 ataków typu Brute Force. Średnia liczba ataków dziennie wynosiła 1.96.

Ataki typu Brute Force polegają na próbie złamania hasła przez generowanie wszystkich możliwych kombinacji ciągu znaków. W konsekwencji cyberprzestępcy są w stanie przejąć dane logowania do konta, którego login i hasło składają się z krótkich i nieskomplikowanych znaków.

212

LICZBA ATAKÓW BRUTE FORCE

1,96

ŚREDNIA LICZBA ATAKÓW DZIENNIE

GREY WIZARD

ATAKI BRUTE FORCE CREDENTIAL STUFFING

Wykorzystując metodę ataku Brute Force cyberprzestępcy są w stanie złamać każde hasło. Jedynym ograniczeniem jest czas. Złamanie krótkiego, nieskomplikowanego hasła może zająć kilka do kilkunastu godzin, natomiast złamanie hasła składającego się z co najmniej 10 znaków, w tym z liter, cyfr oraz znaków specjalnych, może potrwać dni, a nawet tygodnie.

W IV kwartale 2017 roku średni czas ataku Brute Force trwał 138 minut, a najdłuższy atak wynosił 2 dni i 37 minut.

>2

GODZINY

ŚREDNI CZAS TRWANIA ATAKU BRUTE FORCE

>48

GODZIN

NAJDŁUŻSZY ATAK BRUTE FORCE

GREY WIZARD

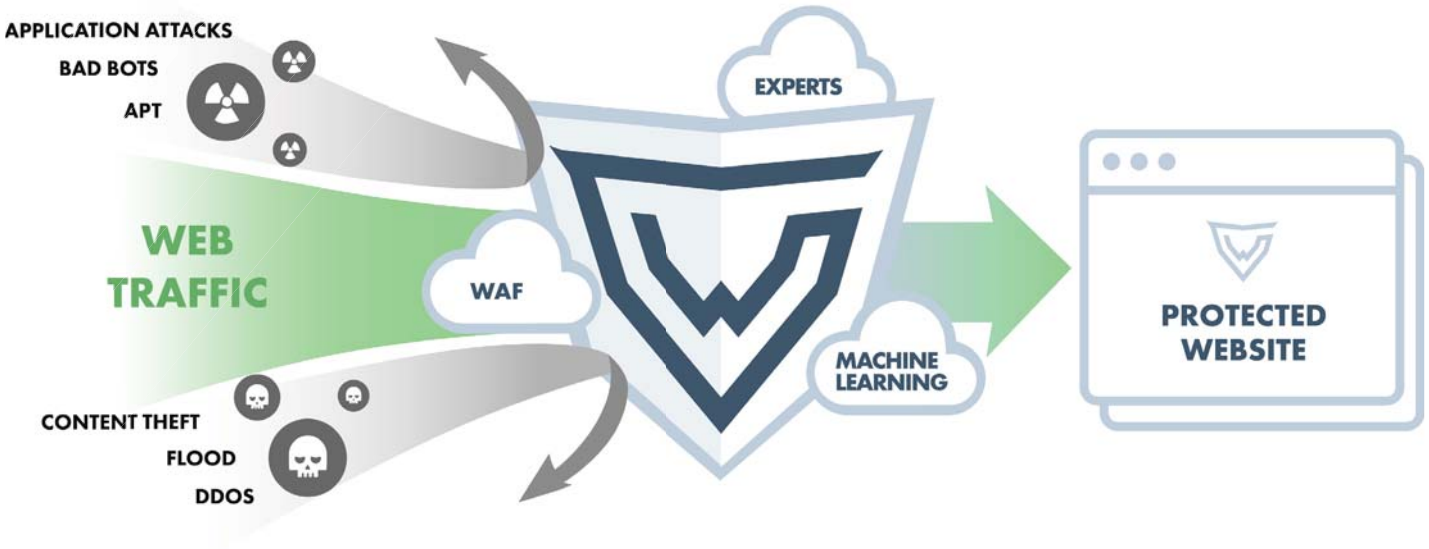
MACHINE LEARNING W CYBERBEZPIECZEŃSTWIE

MACHINE LEARNING W CYBERBEZPIECZEŃSTWIE

Strony internetowe, e-sklepy, instytucje państwowe oraz finansowe czy urządzenia Internetu Rzeczy cały czas się rozwijają. Obecnie coraz więcej technologii wykorzystuje sztuczną inteligencję, która oparta na zaawansowanych algorytmach, jest w stanie sama się rozwijać. Dlatego nowoczesna technologia wymaga zaawansowanych rozwiązań z zakresu cyberbezpieczeństwa wykorzystujących uczenie maszynowe.

Grey Wizard Shield opiera się na inteligentnych algorytmach Machine Learning. W Q4 2017 roku udział algorytmów uczenia maszynowego w blokadach niebezpiecznych zapytań z sieci wyniósł 16,02%.

W przyszłości, wraz z uczeniem się i rozwijaniem algorytmu, będzie on w stanie jeszcze dokładniej monitorować ruch i wykrywać anomalie, co zminimalizuje ryzyko fałszywych alarmów oraz będzie w stanie jeszcze szybciej rozpoznać ataki, które wymykają się tradycyjnym systemom regułowym.



12. Tarcza Grey Wizard działa jako serwer pośredniczący pomiędzy użytkownikami a serwerami klienta.

Cyberbezpieczeństwo w XXI wieku należy traktować priorytetowo. Właśnie dlatego, w walce z cyberatakami, sięgamy po uczenie maszynowe, które dzięki inteligentnym algorytmom jest w stanie skutecznie zabezpieczyć strony internetowe, sieci i aplikacje. Machine Learning, poprzez kompleksowy monitoring aplikacji internetowych oraz identyfikację niebezpiecznych zapytań z sieci, wykrywa wszelkie anomalie i natychmiast podejmuje próby ich odparcia. Algorytmy uczenia maszynowego pozwalają nam być zawsze o krok przed cyberprzestępcami i wykryć nawet takie metody ataków, które nie zostały wcześniej zidentyfikowane. Są w stanie rozpoznawać ataki, które wymykają się tradycyjnym systemom regułowym.

Oleg Daroszewski, Menedżer ds. rozwoju biznesu w Grey Wizard

PROGNOZY BEZPIECZEŃSTWA NA 2018 ROK

PROGNOZY BEZPIECZEŃSTWA NA 2018 ROK

Stojąc na progu 2018 roku warto pamiętać, że jednym z fundamentów współczesnego biznesu jest dbanie o ochronę przechowywanych danych. Obecnie, na cyberbezpieczeństwo, firmy na świecie przeznaczają tylko około 20% budżetu IT. W Polsce ten budżet to zaledwie 10%. Jest to poważny błąd, ponieważ wyciągając lekcje z cyberataków przeprowadzanych w 2017 roku, warto uświadomić sobie, że straty poniesione przez zaatakowane przedsiębiorstwa mogły być o wiele niższe, a do niektórych incydentów bezpieczeństwa wcale nie musiało dojść.

W 2018 roku technologia nadal będzie się rozwijała. Wraz z nią zmienią się także sposoby przeprowadzania cyberataków oraz ochrony przed nimi. Należy spodziewać się zwiększonej liczby ataków na urządzenia IoT. Luki w zabezpieczeniach urządzeń Internetu Rzeczy sprawią, że będą one wykorzystywane do przeprowadzania ataków DDoS. Hakerzy nadal będą wykorzystywali zainfekowane wiadomości e-mail oraz będą używali cyberataków do szantażowania właścicieli witryn internetowych w celu wyłudzania pieniędzy.

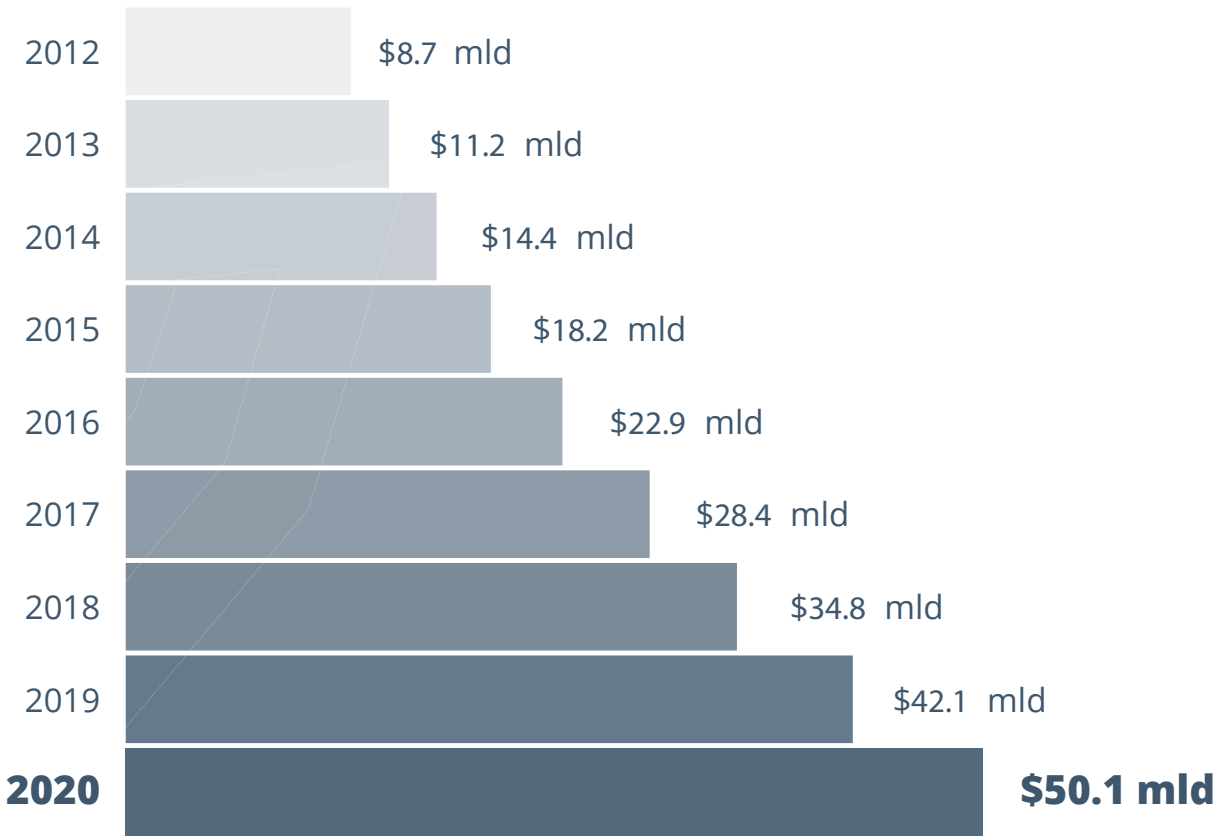
Wzrost urządzeń Internetu Rzeczy

Z roku na rok inteligentne urządzenia Internetu Rzeczy stają się coraz bardziej popularne. Jednak, by mogły w pełni funkcjonować i być ze sobą zintegrowane muszą być podłączone do sieci. Obecnie aż 32% firm posiada ponad 5000 urządzeń IoT. Natomiast aż 85% firm wprowadza lub rozważa wdrożenie do organizacji inteligentnych urządzeń.

Niestety rozwój technologii idzie w parze z rozwojem zagrożeń. Dlatego w 2018 roku możemy spodziewać się, że cyberprzestępcy zwrócą jeszcze większą uwagę na urządzenia IoT. Luki, braki odpowiednich zabezpieczeń i bagatelizowanie aktualizacji systemu urządzeń Internetu Rzeczy będą powodem wykorzystywania ich do przeprowadzania cyberataków i kradzieży treści. Urządzenia IoT będą również używane jako botnety, które mogą być użyte do ataków wolumetrycznych.

Przejęcie urządzeń IoT pozwoli hakerom na przeprowadzanie zmasowanych ataków DDoS, blokowanie dostępu do usług. Ponadto wszechobecne urządzenia domowe, takie jak telewizory, bezprzewodowe głośniki i odkurzacze czy asystenci głosowi, mogą umożliwić hakerom określenie lokalizacji domu, a także ułatwić próby włamania.

PROGNOZY BEZPIECZEŃSTWA NA 2018 ROK



13. Liczba urządzeń IoT podłączonych do sieci

W 2017 roku cyberprzestępcy wykorzystywali znane luki w zabezpieczeniach, co miało katastrofalne skutki. Gdyby firmy i instytucje zadbały o właściwe zabezpieczenie lub wyeliminowanie owych luk, wiele incydentów naruszenia bezpieczeństwa mogło zostać zablokowanych. Każdego roku, liczba urządzeń IoT podłączonych do sieci zwiększa się o około 23%. Do roku 2020 liczba tych urządzeń ma przekroczyć 50 miliardów. W przyszłym roku, wraz ze wzrostem urządzeń Internetu Rzeczy, będzie wzrastać liczba płaszczyzn ataku i samych luk, które będą wykorzystywane przez hakerów. Dlatego w 2018 roku, zaawansowane technologicznie urządzenia będą wymagały ochrony opartej na uczeniu maszynowym i sztucznej inteligencji, by skutecznie blokować incydenty naruszenia bezpieczeństwa.

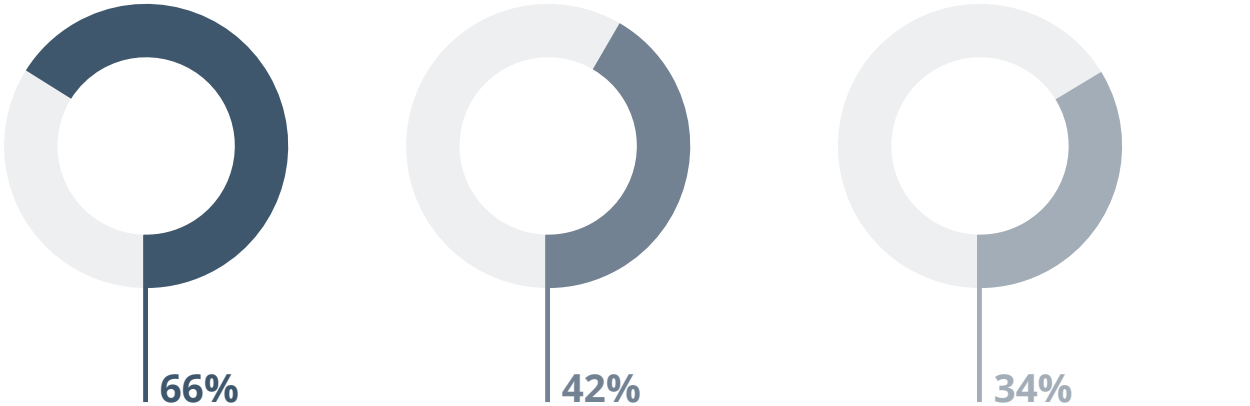
Oleg Daroszewski, Menedżer ds. rozwoju biznesu w Grey Wizard

Ochrona danych osobowych - RODO

Świadomość prawna przedsiębiorców w zakresie ochrony danych osobowych, niestety, była i jest niewielka. Firmy często ignorują kwestie związane z bezpieczeństwem zasobów IT, co opóźnia lub uniemożliwia wykrywanie ewentualnych incydentów naruszenia bezpieczeństwa. Od dnia 25 maja 2018 r. wchodzi w życie unijna dyrektywa o ochronie danych osobowych RODO. Nakłada ona na firmy i instytucje publiczne obowiązek zgłaszania naruszeń ochrony danych, w ciągu 72 godzin, organowi nadzorczemu i informowania o tym osób, których dane zostały naruszone.

Rozporządzenie unijne nakłada surowe kary pieniężne za naruszenie zasad przetwarzania danych osobowych, w tym za ich niewłaściwe zabezpieczenie. Mogą one wynieść od 10-20 mln euro lub 2-4% wartości rocznego światowego obrotu przedsiębiorstwa.

Nowe przepisy dotyczące ochrony danych osobowych niosą za sobą radykalne i poważne zmiany. Firmy zbierające dane wrażliwe będą musiały sprostać wyzwaniom związanym z wdrożeniem i egzekwowaniem przepisów RODO. Przedsiębiorcy będą musieli zadbać nie tylko o zewnętrzne bezpieczeństwo danych osobowych, ale również wprowadzić wewnętrzne obostrzenia związane z unijną dyrektywą.



66%
FIRM LEKCEWAŻY WYSOKOŚĆ KAR NAKŁADANYCH PRZEZ RODO

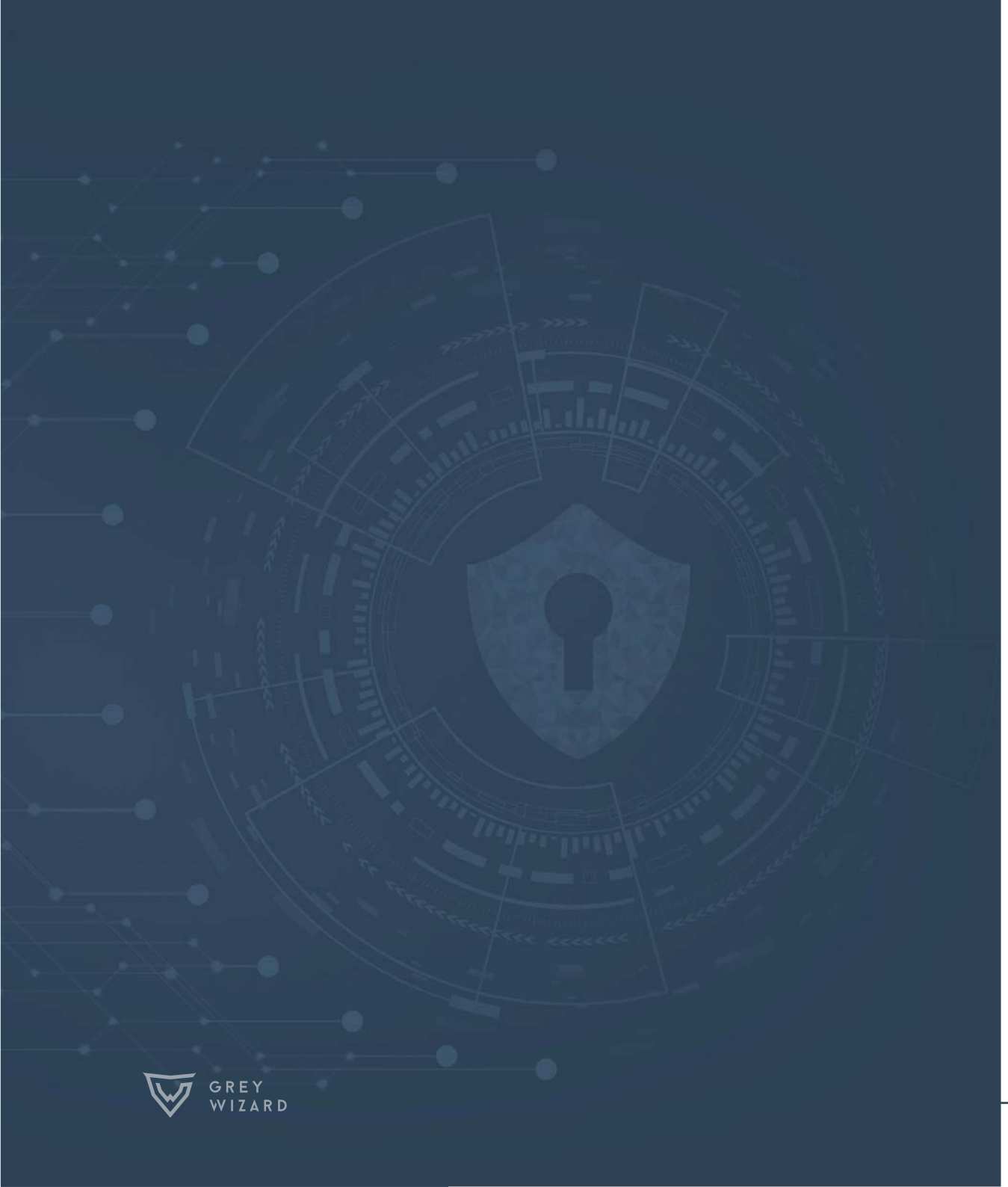
42%
FIRM NIE WIE, ŻE BAZY DANYCH WYKORZYSTYWANE DO E-MAIL MARKETINGU ZAWIERAJĄ DANE OSOBOWE

34%
FIRM ZAINWESTOWAŁO W TECHNOLOGIĘ IDENTYFIKUJĄCĄ INTRUZÓW

14. Ochrona danych osobowych w firmach

W maju 2018 roku wchodzi w życie rozporządzenie o ochronie danych osobowych RODO. Dyrektywa nie wskazuje jednoznacznie konkretnych środków bezpieczeństwa w celu realizacji obowiązku zabezpieczenia danych osobowych. Przywołane są jednak, nie zawsze wprost, możliwe sposoby zabezpieczania danych, które Ustawodawca uznaje za odpowiednie: pseudonimizację, szyfrowanie danych, zapewnienie bezpieczeństwa informacji i systemów - cyberbezpieczeństwo, gotowość zapobiegania skutkom katastrof oraz testowanie przyjętych rozwiązań. Metody te, w szczególności szyfrowanie danych, zapewniają odpowiedni poziom ochrony, ponieważ praktycznie uniemożliwiają dostęp do danych osobowych przetwarzanych w systemach informatycznych osobom nieuprawnionym. Obowiązek monitorowania i reagowania na incydenty bezpieczeństwa sprawi, że przedsiębiorcy wreszcie zaczną poważnie podchodzić do kwestii zabezpieczania danych. Ustawodawca stawia jasne warunki - dane osobowe muszą być bezpieczne, a w przypadku kontroli, należy udowodnić, że dochowaliśmy wszelkiej staranności, aby nie doszło do niepożądanych zdarzeń.

Radosław Wesołowski, CEO Grey Wizard



GREY WIZARD

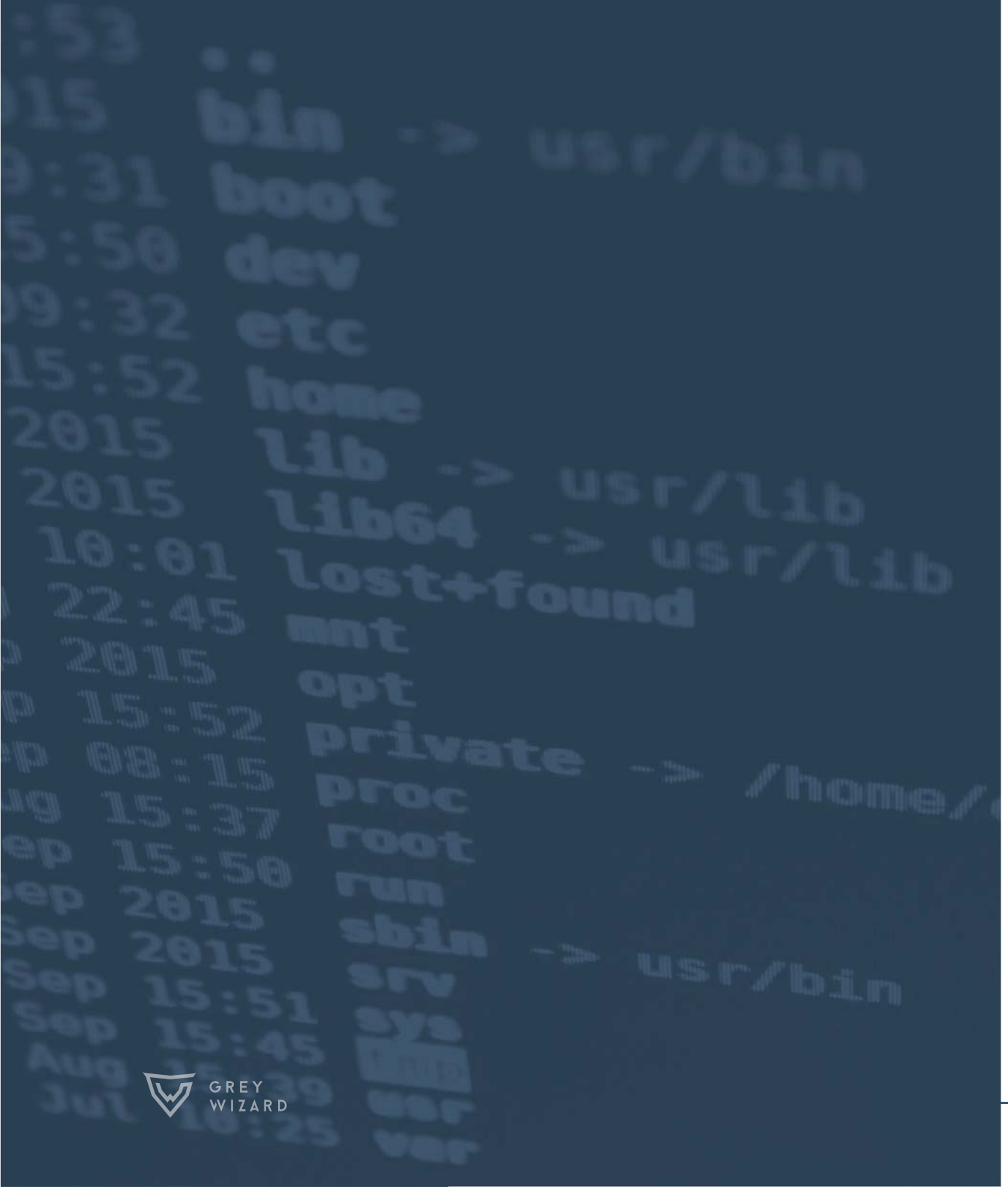
Sztuczna inteligencja w cyberochronie

Świadomość toczącej się cyberwojny, coraz częstszych i bardziej zaawansowanych cyberataków, w wyniku których pozyskiwane są nie tylko dane osób fizycznych, ale również informacje objęte tajemnicą przedsiębiorstwa, mającą, co do zasady, dużą wartość rynkową, przedsiębiorstwa powinny potraktować priorytetowo bezpieczeństwo tych danych.

W 2018 roku cyberbezpieczeństwo będzie musiało w jeszcze większym stopniu rozwijać i wykorzystywać technologię opartą na sztucznej inteligencji. We współczesnym świecie, w którym urządzenia są ze sobą zintegrowane, uczenie maszynowe pozwoli na szybkie wykrycie zagrożenia i natychmiastowe odpieranie ataków. Priorytet będzie stanowiło zadbanie o kompleksowe zabezpieczenia systemów informatycznych, aplikacji webowych oraz serwisów www.

W dzisiejszej cyberrzeczywistości trudno sobie wyobrazić skuteczniejszą broń niż inteligentna technologia oparta na maszynowym uczeniu. Tylko z pomocą sztucznej inteligencji jesteśmy w stanie skutecznie zabezpieczyć się przed cyberatakami, tzw. atakami jutra.

Radosław Wesołowski, CEO Grey Wizard



Wycieki danych

Wycieki danych osobowych czy wrażliwych informacji o firmach lub wyborach zdarzają się niemal każdego dnia. Niektóre z nich zdobywają światowy rozgłos, jak wyciek danych z Yahoo czy Equifax z 2017 roku, inne zostają w cieniu i nie docierają do informacji publicznej. Incydenty związane z wyciekiem danych bardzo często wynikają z braku podstawowych zabezpieczeń, braku właściwej konfiguracji oprogramowania lub nieznanych luk w systemie.

Nadal wiele firm nie zdaje sobie sprawy z tego jak ważne informacje przechowuje i koncentruje swoją uwagę na rozwoju i sprzedaży, pomijając kwestie związane z bezpieczeństwem. Wielu wyciekom danych można zapobiec, przeprowadzając audyt infrastruktury IT, aktualizując oprogramowanie i programy antywirusowe.

W 2018 roku, pomimo wprowadzenia zaostrzonych przepisów o ochronie danych osobowych RODO, incydenty związane z wyciekiem danych nadal będą stanowiły główny problem wielu dużych i małych firm.

WYZWANIA I ZAGROŻENIA DLA BEZPIECZEŃSTWA W 2018 ROKU

WYZWANIA I ZAGROŻENIA DLA BEZPIECZEŃSTWA W 2018 ROKU

Rok 2017 zapamiętamy jako rok wielu zmasowanych ataków hakerskich takich jak Petya, WannaCry czy Bad Rabbit. To także rok, w którym doszło do wielu naruszeń danych, w szczególności w przypadku Equifax, Verizon i Kmart. W Polsce głośnym wydarzeniem był incydent naruszenia bezpieczeństwa w bankach oraz w Komisji Nadzoru Finansowego.

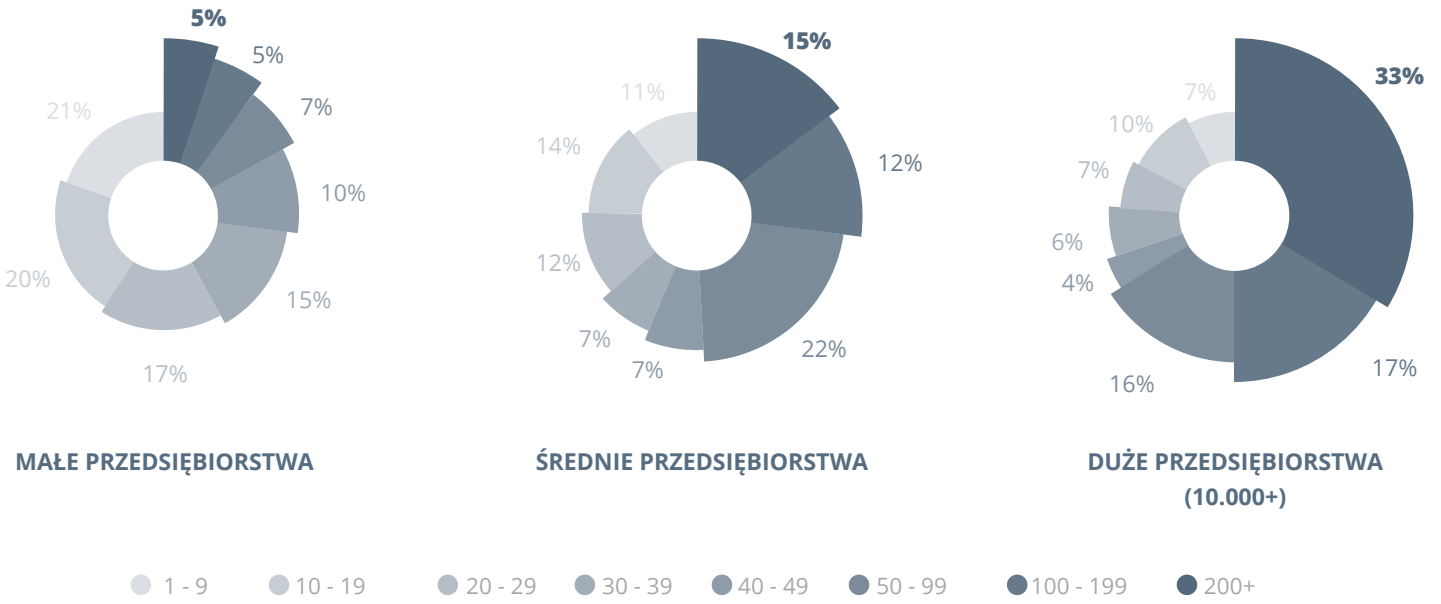
Ostatni rok pokazał, że przed przedsiębiorstwami i instytucjami publicznymi stoi ogromne wyzwanie związane z zapewnieniem bezpieczeństwa firmom i danym wrażliwym. Tym bardziej, że średnia wielkość naruszenia danych wzrosła o prawie 2%. Nowe techniki i metody działania cyberprzestępców sprawiają, że ochrona biznesu staje się coraz trudniejsza, a ryzyko cyberataku cały czas wzrasta.

Małe budżety i brak specjalistów do spraw bezpieczeństwa ograniczają firmom ochronę przed cyberatakami. Pomimo rosnącej świadomości zagrożeń, nadal ochrona jest niewystarczająca. W przedsiębiorstwach korzysta się z popularnych rozwiązań jak firewall i programy antywirusowe. Niestety, w przypadku ataku hakerskiego są one niewystarczające, ponieważ najczęściej ataki są sprofilowane pod kątem konkretnej firmy.

Problemem firm, które dosięga cyberatak jest najczęściej brak wykwalifikowanych pracowników z tej dziedziny, którzy byliby w stanie wykryć, ocenić i rozpoznać zagrożenie oraz podjąć odpowiednie kroki bezpieczeństwa.

W ciągu najbliższych kilku lat, specjaliści do spraw cyberbezpieczeństwa nadal będą należeli do grupy najbardziej poszukiwanych ekspertów w branży IT. Do 2020 roku aż 15% stanowisk związanych z cyberbezpieczeństwem nadal pozostanie nieobsadzonych.

WYZWANIA I ZAGROŻENIA DLA BEZPIECZEŃSTWA W 2018 ROKU



15. Liczba specjalistów ds. bezpieczeństwa według wielkości organizacji

W 2017 roku firmy i instytucje zostały sparaliżowane przez wiele ataków hakerskich. Do ich przeprowadzenia cyberprzestępcy wykorzystywali luki w zabezpieczeniach. Przykładem może być ransomware WannaCry wykorzystujący tylko jedną lukę w zabezpieczeniach. Ta pojedyncza luka umożliwiła stworzenie oprogramowania ransomware, który w bardzo szybkim czasie rozprzestrzenił się po całym świecie.

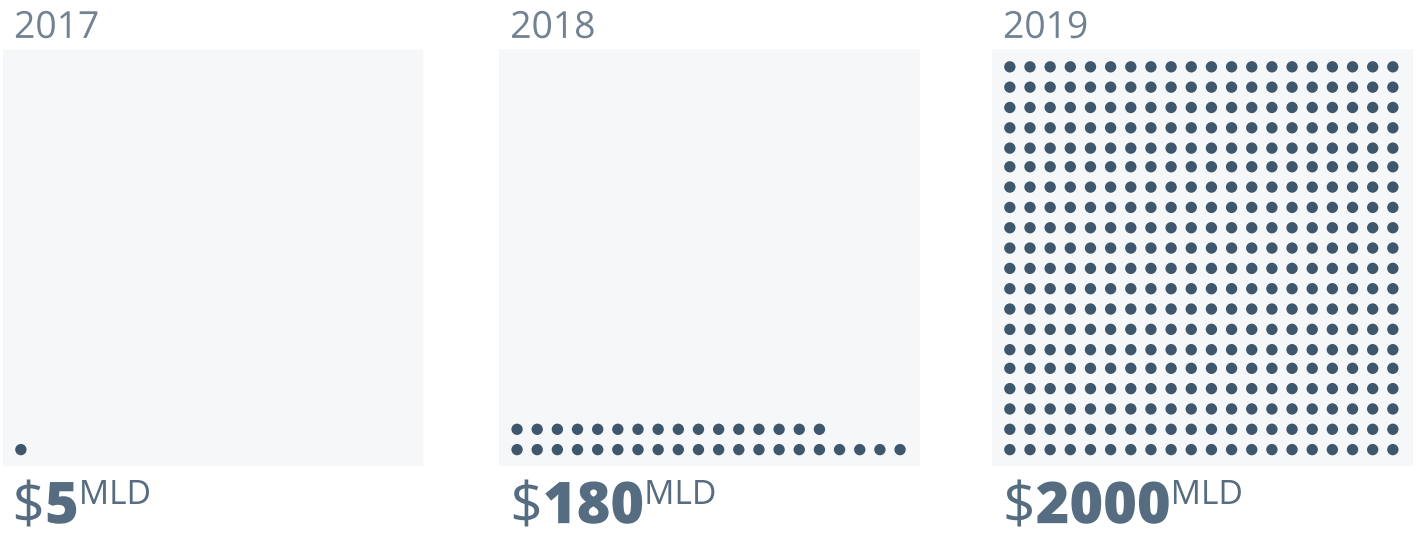
WannaCry i wiele innych cyberataków uświadamiają nam, że cały czas należy dbać i udoskonalać system, by nie stał się narzędziem w rękach hakerów. Niestety świadomość istnienia luk i braku właściwej ochrony sprawiają, że wykorzystanie ich przez przestępców jest tylko kwestią czasu. Producenci na bieżąco tworzą aktualizacje, które usuwają istniejące luki. Jednak w priorytecie powinno być wykrycie i załatanie owych luk, zanim zostaną one wykryte i wykorzystane przez hakerów.

Oleg Daroszewski, Menedżer ds. rozwoju biznesu w Grey Wizard

WYZWANIA I ZAGROŻENIA DLA BEZPIECZEŃSTWA W 2018 ROKU

Cyberataki mają ogromny wpływ na wiele aspektów działania firmy. Każdy skradziony rekord generuje ogromne straty finansowe i wizerunkowe oraz utratę zaufania klientów i partnerów. W 2017 roku koszty cyberataku wyniosły 5 miliardów dolarów.

Prognozy na rok 2018 nie są optymistyczne. Specjaliści do spraw bezpieczeństwa prognozują, że w tym roku koszty cyberataków mogą wynieść nawet 180 miliardów dolarów. Ten 36-krotny wzrost kwoty jest wyraźnym sygnałem dla firm, by wdrożyć procedury bezpieczeństwa oraz zadbać o dodatkowe zabezpieczenie stron internetowych przed cyberprzestępcami.



16. Koszty cyberataków

USŁUGI BEZPIECZEŃSTWA
GREY WIZARD

Grey Wizard oferuje szereg usług, które zwiększają bezpieczeństwo firm i skutecznie odpierają cyberataki.

Ochrona przed atakami DDoS

Ochrona DDoS gwarantuje skuteczne odpieranie wolumetrycznych ataków odmowy dostępu. Rozproszona odmowa usługi, jaką jest atak DDoS stanowi jedno z największych zagrożeń współczesnego świata. Zagraża wielu firmom i sklepom internetowym, instytucjom rządowym i finansowym oraz osobom prywatnym.

Koszt przeprowadzenia ataku jest niski (około kilkuset złotych), a wygenerowane straty mogą być mierzone w milionach. Głównym celem cyberprzestępców jest kradzież wrażliwych danych. Konsekwencje ataków rozproszonej odmowy usługi sięgają dalej niż tylko działów IT. DDoS powoduje realne i mierzalne straty finansowe i wizerunkowe, co w efekcie prowadzi do utraty ciągłości procesów biznesowych.

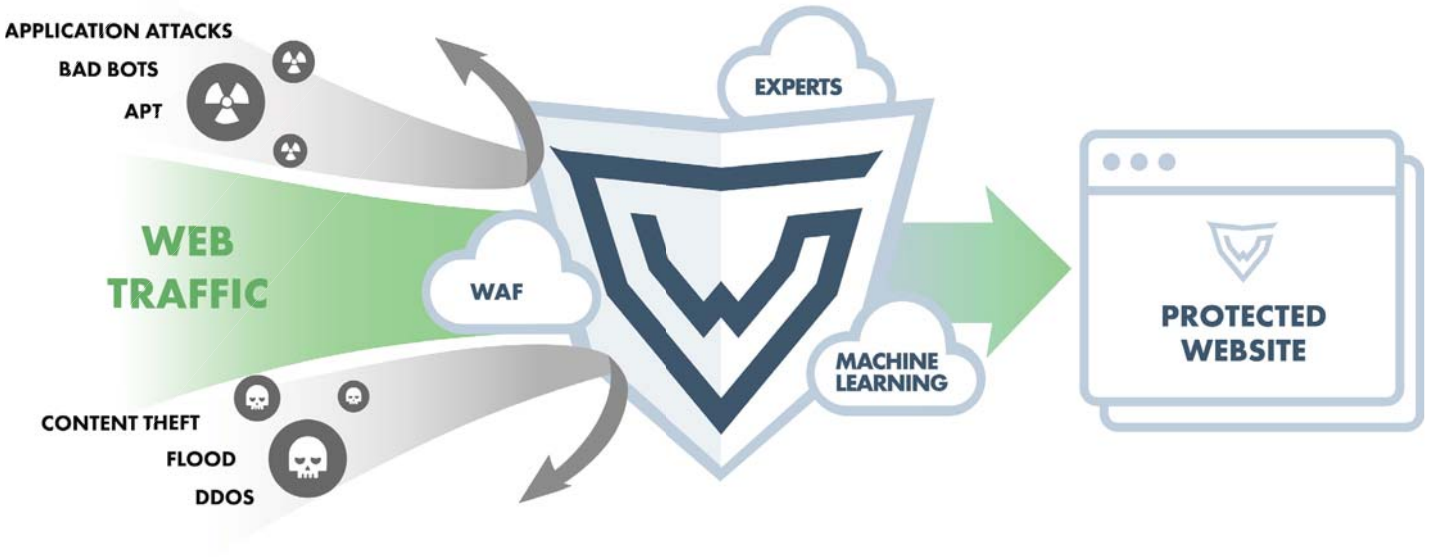
Ataki mogą mieć różną formę i rozmiar. Mogą dotyczyć wielu protokołów UDP i ICMP, a także SYN / ACK oraz DNS i ataku na warstwę 7.

17. Aktywacja ochrony Grey Wizard.

Ochrona przed atakami DDoS

Podstawą obrony przed atakami DDoS jest wdrożenie rozwiązań gwarantujących ciągłą ochronę, uwzględniających nowoczesne narzędzia do monitorowania i zarządzania zasobami sieciowymi. Przeciwdziałanie atakowi wymaga szybkiego dostępu do alternatywnych połączeń z operatorami internetowymi, zapasowych serwerów i kopii danych, dlatego przedsiębiorstwa decydują się na outsourcing kompetencji cybersec do wyspecjalizowanych podmiotów.

Dedykowane systemy zewnętrzne nieustannie analizują ruch tra ający do serwisów klientów i w ciągu kilku sekund mogą wykryć oraz powstrzymać kilkaset typów ataków. Specjalistyczne, samouczące algorytmy pozwalają zidenty kować i zneutralizować nowe, do tej pory nieznane zagrożenia.



18. Tarcza Grey Wizard działa jako serwer pośredniczący pomiędzy użytkownikami a serwerami klienta.

Web Application Firewall

Ochrona aplikacji jest szczególnie trudna, ponieważ pisane aplikacje nie mają zwykle żadnego standardowego scenariusza budowy związanego z wymogami bezpieczeństwa. Większość firm piszących oprogramowanie nie posiada kompetencji do sprawdzania wrażliwości stworzonego oprogramowania na ataki DDoS.

Grey Wizard zapewnia bezpieczeństwo aplikacji internetowej chroniąc przed XSS (Cross-site scrip ng) i SQL injection. Do ochrony przed tego typu atakami służy WAF (Web Applica on Firewall).

Jego zadaniem jest monitorowanie zachowań użytkowników w konkretnym serwisie internetowym lub aplikacji internetowej, a następnie weryfikacja każdej aktywności użytkownika, włącznie z wprowadzaniem wszelkich danych w formularzach występujących w serwisie internetowym. WAF uczy się aplikacji i potrafi wykrywać zachowania użytkowników, które mogą być groźna dla stabilności pracy aplikacji lub są próbą włamania się do danych aplikacji.

19. Web Application Firewall.

Web Application Firewall

Aktywny WAF zablokuje także bardziej przemyślane ataki, jak np. path-traversal polegający na próbie wyjścia z podstawowego katalogu poprzez doklejenie do zmiennej (interpretowanej jako ścieżka katalogu) określonego ciągu znaków. Bazując m.in. na mechanizmach reputacji, WAF sprawdza integralność i zgodność z RFC zapytań HTTP, co pozwala mu zapobiegać przejęciu kontroli nad aplikacją w wyniku ataków wymierzonych w podatności serwerów www.

Najważniejsze cechy WAF

- Automatyczna ochrona przed atakami aplikacyjnymi 24/7
- Ochrona przed “zero-day exploits”
- Systemy reputacji
- Szczegółowa inspekcja pakietów / zapytań
- Dane w czasie rzeczywistym
- Brak dodatkowych urządzeń
- Niski współczynnik fałszywych alarmów
- Możliwość definiowania wyjątków

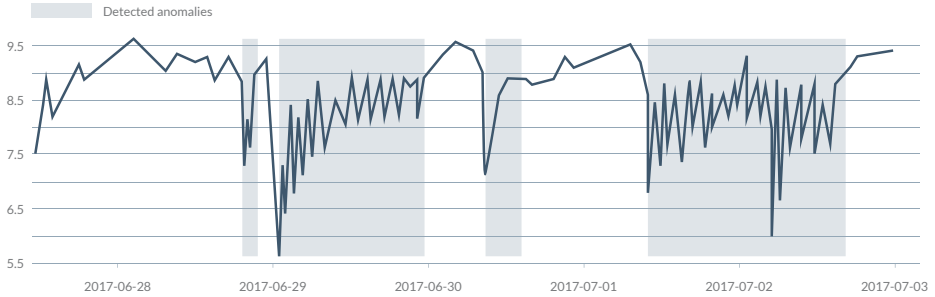
Machine Learning

Ochrona przed cyberatakami wymaga dziś rozwiązań zaawansowanych technologicznie, gotowych nie tylko do odpierania ataków w czasie rzeczywistym, ale przede wszystkim do wychwytywania zagrożeń i skutecznego zabezpieczenia stron www, sieci i aplikacji.

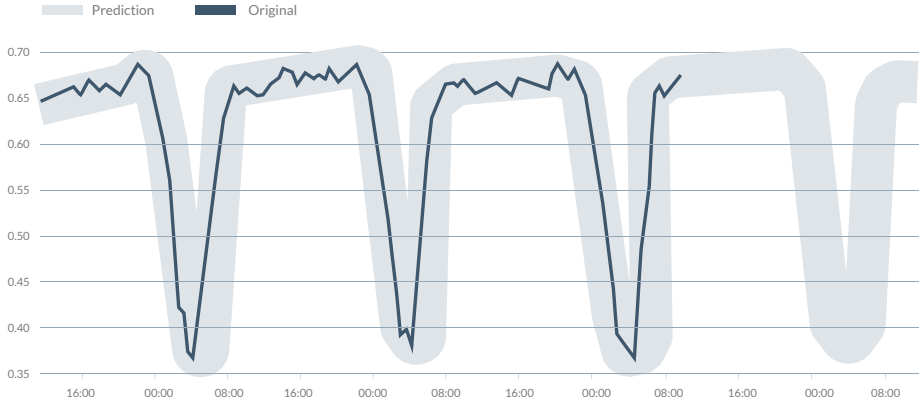
Skuteczność Tarczy Grey Wizard w dużej mierze opiera się na wykorzystaniu inteligentnych algorytmów maszynowego uczenia. Dzięki nim jest w stanie wykryć wszelkie anomalie poprzez kompleksowy monitoring aplikacji internetowych oraz identyfkację niebezpiecznych zapytań z sieci.

Działanie inteligentnych algorytmów zastosowanych w tarczy Grey Wizard polega na szczegółowej analizie ruchu sieciowego pomiędzy użytkownikami i aplikacjami webowymi. Na bazie wielu współczynników aplikacja Grey Wizard określa modelowy ruch i jego dynamikę, dzięki czemu możliwe jest wykrycie wszelkich anomalii przy jednoczesnym zminimalizowaniu ryzyka fałszywych alarmów.

Monitoring aplikacji w czasie rzeczywistym pozwala na błyskawiczną reakcję zespołu Grey Wizard na wszelkie zagrożenia związane z atakami na aplikacje klientów.



20. Wizualizacja ataków - na szaro zaznaczone są ataki (anomalie) wykryte na jednym z monitorowanych atrybutów.



21. Prezentacja innego atrybutu oraz przewidywania algorytmu, co do zakresu wartości, jaki może przyjmować w przyszłości (wyliczenie na bazie danych historycznych).

Content Delivery Network (CDN)

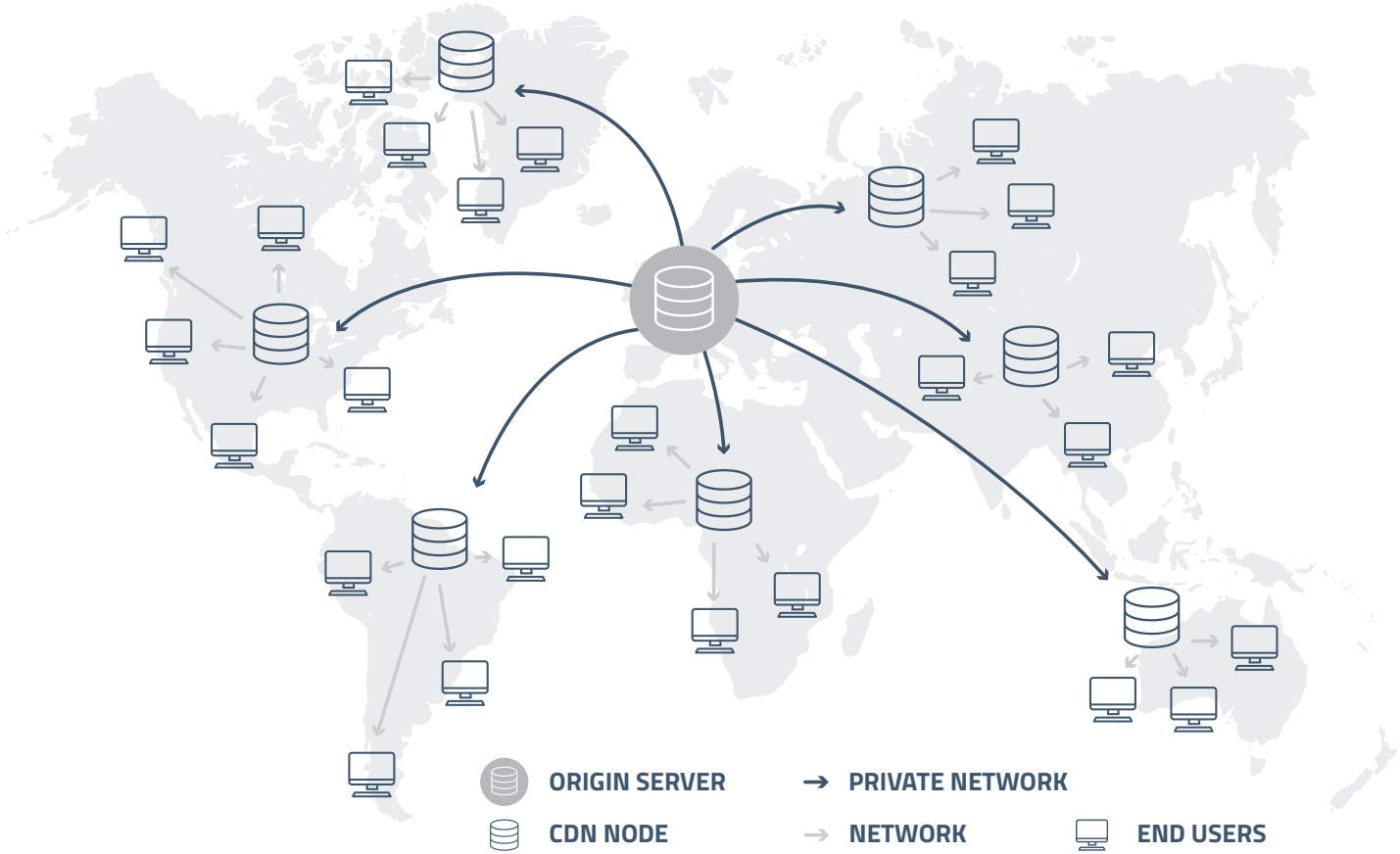
Usługa CDN Grey Wizard odpowiada za zwiększenie dostępności i wydajności stron www dla użytkowników końcowych, zmniejszenie obciążenia serwerów, ograniczenie zużycia łącza internetowego oraz ochronę przed atakami DDoS.

Użytkownicy korzystający ze stosunkowo nowych wersji przeglądarek zauważą zwiększenie wydajności serwisów www w przypadku włączenia szyfrowania TLS/SSL na stronie, ponieważ Grey Wizard umożliwia komunikację z wykorzystaniem standardu HTTP/2 niezależnie od tego, czy jest on obsługiwany w infrastrukturze klienta.

Ruch do chronionych witryn przesyłany jest przez inteligentną rozproszoną sieć Grey Wizard. Usługa zbudowana jest w oparciu o mechanizm Anycast, który kieruje użytkowników końcowych do najbliższego miejsca, gdzie dostępne są zasoby. Transfer treści do odwiedzających stronę może być automatycznie optymalizowany, jeśli klient chce skorzystać z takiej opcji. Użytkownicy przeglądający witrynę w praktyce będą pobierać dane statyczne z serwerów Grey Wizard, w szczególności dotyczy to gra ki, arkuszy stylów CSS oraz plików Javascript wykorzystywanych na stronach. Dane przesyłane do przeglądających witrynę są dodatkowe kompresowane oraz oznaczone tak, aby przeglądarki przechowywały je w pamięci podręcznej zamiast pobierać ponownie, jeśli nie uległy one zmianie.

Istnieje również możliwość sterowania CDN za pośrednictwem API, co w znacznym stopniu ułatwia proces modyfkowania treści, na chronionej stronie, przez jej developerów.

USŁUGI BEZPIECZEŃSTWA GREY WIZARD



22. Schemat działania CDN

Content Delivery Network (CDN)

Dodatkowo, usługa CDN aktywuje ochronę strony www przed atakami sieciowymi i aplikacyjnymi poprzez blokowanie dostępu dla złych robotów wykorzystujących pasmo i zasoby obliczeniowe konta hostingowego.

Korzyści:

- globalna infrastruktura, która chroni strony,
- krótszy czas odpowiedzi strony do odwiedzających serwis,
- odciążenie serwerów klienta,
- wzrost wydajności i przepustowości,
- większa dostępność oraz zoptymalizowany poziom usługi dla klienta końcowego,
- ochrona przed atakami DDoS.

Load Balancing

Load Balancing to system równomiernego rozkładania obciążenia systemów informatycznych (m.in.: pamięci, mocy procesora) w celu uniknięcia przeciążenia pojedynczego serwera.

23. Grey Wizard w roli balansera ruchu pomiędzy serwerami.

24. Grey Wizard w roli balansera ruchu pomiędzy centrami danych.

Jeżeli w infrastrukturze klienta znajduje się więcej niż jeden serwer wówczas wskazane jest, by Grey Wizard występował w roli balansera ruchu pomiędzy nimi. W przypadku wykrycia problemów z serwerem, zapytania zostaną automatycznie rozdystrybuowane do pozostałych maszyn. To bardzo korzystne rozwiązanie, gdyż nie wymaga instalacji dodatkowego sprzętu i kosztownego oprogramowania. Wystarczy zdefiniowanie listy adresów IP by uruchomić Load Balancing.

W przypadku infrastruktury rozproszonej i rozlokowania maszyn klienta w kilku centrach danych, w celu zapewnienia wysokiej dostępności, Grey Wizard balansuje ruch pomiędzy nimi. W sytuacji wykrycia niedostępności jednego z nich, ruch automatycznie zostanie przekierowany do drugiego.

GREY WIZARD

Grey Wizard sp. z o.o.
ul. Piekary 12/12, 61-823 Poznań
kontakt@greywizard.com