EXATEL

Cyberbezpieczeństwo 2022

Trendy i rozwiązania z uwzględnieniem perspektywy EXATEL

exatel.pl

Lepiej, żeby przyjaciel cię obudził, **niż żeby wróg cię usypiał**

Ta zasada wyjątkowo sprawdza się w cyberbezpieczeństwie. Z powodu różnych ciśnień: geopolitycznych, inflacyjnych czy płacowych, kierujemy naszą uwagę w miejsca zapalne. Zapominamy przy tym o rzeczach, które – jak się nam wydaje – funkcjonują dobrze, bezpiecznie. Bo przecież działa strona, jest Internet. W związku z tym często wolimy uważać, że żaden cyberatak nie dotknie naszych firm. Jednak rzeczywistość brutalnie weryfikuje to myślenie życzeniowe.

Zarządzać możemy tylko tym, o czym wiemy. Dlatego znacznie lepiej jest być świadomym istniejących braków, o których możemy się dowiedzieć w wyniku rekonesansu bezpieczeństwa bezpieczeństwa czy też usług Security Operations Center, które proponuje EXATEL. Mogą to być źle skonstruowane czy skonfigurowane usługi, malware zainstalowany na serwerze czy „dziurawe" Wi-Fi. To wszystko miesiącami może zagrażać bezpieczeństwu naszych firm, zanim zostanie wykryte. Z raportów wynika, że średni czas do usunięcia podatności na cyberatak wynosi do 3 miesięcy. Czy możemy pozwolić sobie na to, żeby przeciwnik przez ten czas czytał nasze najbardziej prywatne e-maile? Albo wykorzystywał je do ataku na naszych kontrahentów i partnerów biznesowych? A co atakami DDoS? Prymitywne, brutalne, trywialne – tak możemy je określić, lecz spełniają swoją funkcję. Blokują działanie firm czy instytucji, co przekłada się na realne finansowe straty. Przecież – zwłaszcza teraz – nie możemy sobie na to pozwolić.

Co więcej, coraz częściej mamy do czynienia z bardziej wyrafinowanymi technikami ataku DDoS, na które nie pomagają standardowe mitygacje. Dlatego opracowaliśmy rozwiązanie TAMA, które oferuje wiele finezyjnych metod ochrony. TAMĘ stosujemy już ponad. Przez ten czas odparła już dziesiątki tysięcy ataków na wielkie instytucje i mniejsze firmy.

Mam nadzieję, że informacje zebrane w tym raporcie będą stanowiły dużą dawkę aktualnej wiedzy na temat cyberbezpieczeństwa oraz zachęcą Czytelników do współpracy zespołem EXATEL.

Rafał Magryś

Wiceprezes Zarządu EXATEL

Dług technologiczny **trzeba spłacić**

Ekspresowe dostosowanie pojemności środowisk teleinformatycznych do potrzeb zwiększonego udziału pracy zdalnej z powodu pandemii COVID-19 to działania, które z perspektywy świata IT wydają się być historią starożytną.

Należy jednak pamiętać, że szybkie tempo wprowadzania zmian w infrastrukturze teleinformatycznej, w trakcie przyspieszonej transformacji cyfrowej, obarczone było wysokim prawdopodobieństwem popełnienia błędów architektonicznych i stworzenia długu technologicznego.

Ten dług trzeba spłacić i nie warto czekać na kolejne lata, w których być może będzie lepiej, łatwiej, czy też taniej. Nie będzie. Co gorsza, obserwuję, że przyspieszone wdrażanie systemów i rozwiązań sieciowych stało się nowym „standardem". Tym bardziej spotęgowało to zjawisko współistnienia obok siebie systemów „prawie wdrożonych". W efekcie nakładające się na siebie niedoskonałości poszczególnych elementów składowych systemów IT w sieciach lokalnych i chmurze są rajem dla atakujących.

Do jakich prowadzi to konsekwencji? Zdecydowanie łatwiej dostać się do takich środowisk, łatwiej firmę okraść, łatwiej śledzić i szantażować, łatwiej zniszczyć jej systemy, łatwiej dostać się do środowisk automatyki przemysłowej i zniszczyć ciąg produkcyjny, łatwiej zatrzymać cały biznes.

Wydarzenia 2022 r. utwierdzają nas w przekonaniu, że wiele złożonych wyzwań w świecie cyberbezpieczeństwa jest przed nami – wyzwań, których skalę trudno przewidzieć, a ich wpływ na prowadzoną działalność będzie istotny.

Dlatego poza rozpoznaniem ofensywnym infrastruktury i sprawdzeniem odporności na włamanie, istotne jest systematyczne monitorowanie bezpieczeństwa realizowane przez doświadczonych ekspertów cyberbezpieczeństwa Security Operations Center.

Pamiętajmy, że najlepsze efekty w zwiększaniu bezpieczeństwa i odporności na różnego rodzaju ataki osiągniemy przez systematyczność, powtarzalność i konsekwencję – najefektywniej we współpracy z partnerem godnym zaufania, którym jest EXATEL.

Karol Wróbel

Dyrektor Departamentu Cyberbezpieczeństwa
i Departamentu IT

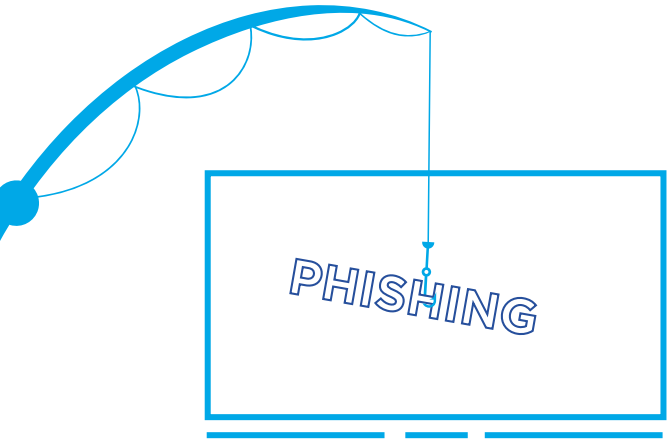
EXATEL

ROZDZIAŁ I

Krajobraz zagrożeń od 2021 roku

W ostatnim roku świat znów przyspieszył – wychodziliśmy z pandemii i wracaliśmy do normalności. W branży cyberbezpieczeństwa – która nie odnotowała pandemicznego spowolnienia – to czas wzmożonych działań. Codziennie trzeba się mierzyć z nowymi rodzajami zagrożeń i wzrastającą liczbą incydentów bezpieczeństwa.

Według raportu Palo Alto Networks najczęściej występują incydenty business email compromise – (BEC[1]) oraz ransomware. W prawie 80% hakerzy włamywali się do systemów informatycznych, stosując phishing, wykorzystując dobrze znane luki w oprogramowaniu oraz zdobywając dane do logowania poprzez ataki brute-force. Ich celami najczęściej były sektory: finansowy, usług prawniczych, produkcji przemysłowej oraz ochrony zdrowia[2].



Na zagrożenie phishingiem zwrócili również uwagę eksperci z Security Operations Center (SOC) EXATEL, którzy wykryli u swoich klientów dużą liczbę podejmowanych prób phishinowych – średnio 100 prób miesięcznie.

Nośnikiem dla ataków tego rodzaju była najczęściej poczta elektroniczna. Część przychodzących wiadomości e-mail miała dołączony „złośliwy" link, który prowadził np. do strony wyłudzającej informacje, a pozostałe zawierały załączniki ze „złośliwym" oprogramowaniem. Eksperci SOC EXATEL zauważyli także coraz więcej prób dostarczania użytkownikom podejrzanych plików poprzez linki. „Złośliwe" pliki w załącznikach zdarzają się rzadziej – zwłaszcza te z pakietu Microsoft Office z makrami VBA (Visual Basic for Applications), chociaż w ich miejsce pojawiają się takie, które pozwalają atakującemu na interakcję z systemem ofiary.

Interesujący obraz zagrożeń prezentuje też raport amerykańskiej firmy Cisco Talos. Ransomware jest tam również wymieniany jako jeden z najczęstszych rodzajów ataku, ale nie najczęstszy. Ataki tego typu (przy użyciu złośliwego oprogramowania szyfrującego) znalazły się na II miejscu[3]. Było ich mniej także dlatego, że wiele grup, które się tym zajmowały, zakończyło już swoją działalność albo zostało rozbitych przez organy ścigania[4]. Najbardziej znanym przypadkiem jest grupa Conti, która na początku 2022 r. ogłosiła, że przestaje działać. Amerykańscy eksperci wskazali na renesans trojanów, które odpowiadają za ataki przy użyciu poczty elektronicznej. W II kwartale 2022 r. liderem okazało się więc tzw. commodity malware[5] z takim

[1] Business email compromise to rodzaj socjotechnicznego ataku, który wykorzystuje ludzką naiwność i nieuwagę. Cyberprzestępcy podszywają się pod osoby zasiadające w zarządach przedsiębiorstw i np. wysyłają wiadomości do kontrahentów – najczęściej z oddziału finansowego – w których proszą o zmianę rachunku do przelewu albo pilne uregulowanie płatności na jakiś wskazany adres.

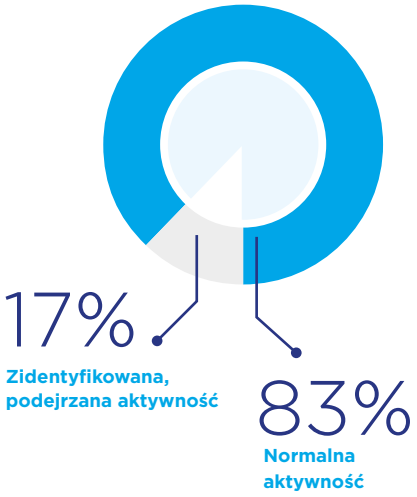
[2] https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2022-unit42-incident-response-report-final.pdf, str. 5

[3] https://blog.talosintelligence.com/2022/07/quarterly-report-incident-response.html

[4] https://blog.talosintelligence.com/2022/07/quarterly-report-incident-response.html

[5] Commodity malware to popularne, szeroko dostępne złośliwe oprogramowanie, które można łatwo kupić lub nawet w niektórych przypadkach bezpłatnie pobrać.

Analiza ruchu kierowanego do typowej strony WWW w internecie:



oprogramowaniem jak Emotet[6] oraz TrickBot[7]. Najczęściej atakowane były sektory edukacji i opieki zdrowotnej oraz firmy z branży telekomunikacyjnej.

Czujni **eksperci EXATEL**

Od początku 2021 r. SOC EXATEL co miesiąc identyfikował około 1400 naruszeń cyberbezpieczeństwa u swoich klientów. Eksperci nie zidentyfikowali skutecznych ataków z wykorzystaniem oprogramowania ransomware. Było to możliwe dzięki temu, że klienci, których obsługuje firma, mają:

- zabezpieczenia, które skutecznie eliminują zagrożenia,
- pracowników, którzy są dobrze przygotowani i świadomi zagrożeń - dzięki programom szkoleniowym z zakresu cyberbezpieczeństwa.

Wykryto natomiast próby ataków typu commodity malware i złośliwe oprogramowanie, takie jak Emotet czy Agent Tesla[8] (przed tym drugim ostrzegał też CERT Polska). Agent Tesla znajdował się w e-mailach zawierających jedynie plik IMG, którego otwarcie mogło spowodować utratę danych wrażliwych[9]. Jednak średnia liczba prób dostarczenia commodity malware pojedynczemu użytkownikowi w organizacjach monitorowanych przez EXATEL, wynosiła tylko około 0,8 na miesiąc. Skutecznie przedostawały się jedynie pojedyncze e-maile. A świadomy i czujny użytkownik mógł szybko i bezpiecznie je zneutralizować.

Inne skuteczne i zaawansowane incydenty dotyczyły prób wykorzystania podatności, z których tylko niewielka część zakończyła się sukcesem. Prób skanowania było jednak zdecydowanie więcej – od kilkunastu do nawet kilkuset miesięcznie. Zależało to od tego, czy atakujący działał masowo, czy tylko punktowo prowadził rozpoznanie technologiczne. Pokrywa się to z ustaleniami ekspertów Palo Alto Networks, którzy obok phishingu i ataków brute-force, właśnie wykorzystanie podatności zaliczyli do wektorów najczęściej wykorzystywanych przez atakujących[10]. Inna amerykańska firma Mandiant, w corocznym raporcie na temat cyberzagrożeń wskazała szczególnie na krytyczną podatność Log4Shell[11]. Nic więc dziwnego, że i SOC EXATEL identyfikował m.in.

[6] Emotet – modularny malware as-a-service, pierwotnie trojan bankowy. Więcej informacji w https://attack.mitre.org/software/S0367/

[7] TrickBot – rodzaj trojana bankowego. Więcej informacji w https://attack.mitre.org/software/S0266/ oraz https://www.cisa.gov/uscert/sites/default/files/publications/TrickBot_Fact_Sheet_508.pdf

[8] Agent Tesla to narzędzie zdalnego dostępu. Umożliwia cyberprzestępcom zdalne sterowanie komputerami. Więcej informacji na https://attack.mitre.org/software/S0331/ oraz https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla

[9] https://www.gov.pl/web/baza-wiedzy/uwaga-csirt-nask-ostrzega-przed-kolejnym-groznym-oszustwem-uwazajcie-na-swoje-skrzynki-e-mailowe

[10] https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2022-unit42-incident-response-report-final.pdf, str.5.

[11] Usługa SSH (secure shell) pozwala na bezpośrednie zarządzanie serwerem z wykorzystaniem połączenia terminalowego.

NASZ EKSPERT

RAFAŁ LITWIŃCZUK
(CISSP, GCIH)
Główny Inżynier ds. Reagowania na Incydenty Bezpieczeństwa

„W dalszym ciągu jednymi z ważniejszych naruszeń cyberbezpieczeństwa są phishing i zdarzenia związane z użytkownikiem końcowym. Na znaczeniu zyskuje jednak wykorzystywanie podatności. Dlatego ważne, aby nie tylko pamiętać o aktualizacjach, ale też aby zadbać o inne mechanizmy, które pozwolą wykryć atakującego w środowisku informatycznym firmy. Dzięki temu możliwe będzie podjęcie działań w przypadku nowych i nieznanych jeszcze podatności w infrastrukturze."

1400
incydentów

- Phishing
- Commodity Malware
- Wykorzystanie podatności

umieszczanie webshelli na serwerze świadczącym usługę WWW oraz aktywności użytkowników określane jako tzw. „insider threats", czyli wykorzystanie zasobów firmowych do celów prywatnych. Były to na tyle zaawansowane incydenty, że wymagały obsługi przez 2 oraz 3 linię SOC. Zwykle zespoły 2 i 3 linii angażowane są wtedy, gdy trzeba połączyć wiedzę ekspercką z często niestandardowymi działaniami, aby zniwelować skutki cyberataku. Specjaliści SOC EXATEL znaleźli i zidentyfikowali również incydenty wymierzone w inne usługi zewnętrzne, takie jak dostęp do poczty korporacyjnej poprzez webmail czy systemy typu e-Commerce oraz CRM. Te ataki były efektami m.in. udanego phishingu i uruchomienia złośliwego pliku przez użytkownika końcowego czy też wykorzystania istniejących podatności.

Phishing jako jedno z głównych rodzajów dostarczenia złośliwego oprogramowania albo przejęcia danych pojawia się od dawna i nie zmieniło się to w ostatnim czasie. Potwierdzają to także raporty Palo Alto Networks.

Eksperci EXATEL wskazali także na problem nadmiarowego udostępniania usług do internetu, takich jak interfejsy administracyjne, usługi SSH[12] czy zdalne pulpity. Szczególnie częste było to w czasie pandemii COVID-19. Zdarzały się nawet takie sytuacje, że pod jednym adresem IP znajdywało się kilka wystawionych usług, a użytkownik nawet o tym nie wiedział.

Czas obsługi wykrytych incydentów wahał się od kilku dni do nawet kilku miesięcy.

Ataki **rozproszonej odmowy dostępu** do usług (DDoS)

Aby osiągnąć cele polityczne, ideologiczne, społeczne, ale również finansowe, hakerzy bardzo często stosują ataki rozproszonej odmowy dostępu do usługi (denial distribiuted of service – DDoS). Naruszenie dostępności danej usługi, jak np. dostępu klientów do sklepu, może powodować odpływ tych klientów, którzy nie mogą korzystać z możliwości zakupu. W efekcie przechodzą więc do konkurencji. Ataki tego typu są relatywnie łatwe do przeprowadzenia oraz nie wymagają dużych zdolności IT.

Zespół F5, który prowadził badania na temat ataków DDoS, stwierdził, że liczba naruszeń tego rodzaju w 2020 r. co prawda zmalała o 3%, ale ich rozmiar i stopień skomplikowania się powiększył. Liczba małych i średnich ataków DDoS, do 250 gigabitów na sekundkę (Gbps), zmalała o 5%, podczas gdy liczba dużych ataków, wykraczających poza 250 Gbps, zwiększyła się aż o 1300%. Zmieniła się również metoda – coraz częściej hakerzy zmuszają ofiary do zapłaty ransomware. Grupy, które używają takich technik, to m.in.: Avaddon, DarkSide, Ragnar Locker czy Sodinkibi. Co ciekawe, również cyberprzestępcy obawiają się ataków DDoS skierowanych na swoje cyfrowe rynki, które mogą zostać częściowo sparaliżowane przez konkurencję. Największy atak, jaki został odnotowany w 2021 r., miał wielkość 1,4 terabitów na sekundkę (Tbps) i był pięciokrotnie większy niż największy DDoS z 2020 r. Najczęściej atakowano sektor finansowy – dotyczyło go 25% wszystkich ataków. Ataki wolumetryczne[13] stanowiły 59%[14].

Najczęściej atakowanym sektorem był sektor finansowy, którego dotyczyło 25% wszystkich ataków

Ponad **1000 ataków DDoS** miesięcznie

Wzrost liczby ataków DDoS widać też w statystykach EXATEL. Całkowita liczba mitygacji ataków w okresie od stycznia 2021 r. do lipca 2022 r. wyniosła ponad 22 tys. – średnio ponad 1000 miesięcznie.

Aby odeprzeć próby cyberataków, eksperci stosują 2 główne metody. Pierwszą z nich jest **filtrowanie ruchu IP.** Polega ono na tym, że po wykryciu ataku cały ruch do atakowanego adresu IP zostaje przekierowany do jednostki czyszczącej. Jej celem jest odrzucenie pakietów powiązanych z atakiem i przepuszczenie tych, które są związane z ruchem prawidłowym.

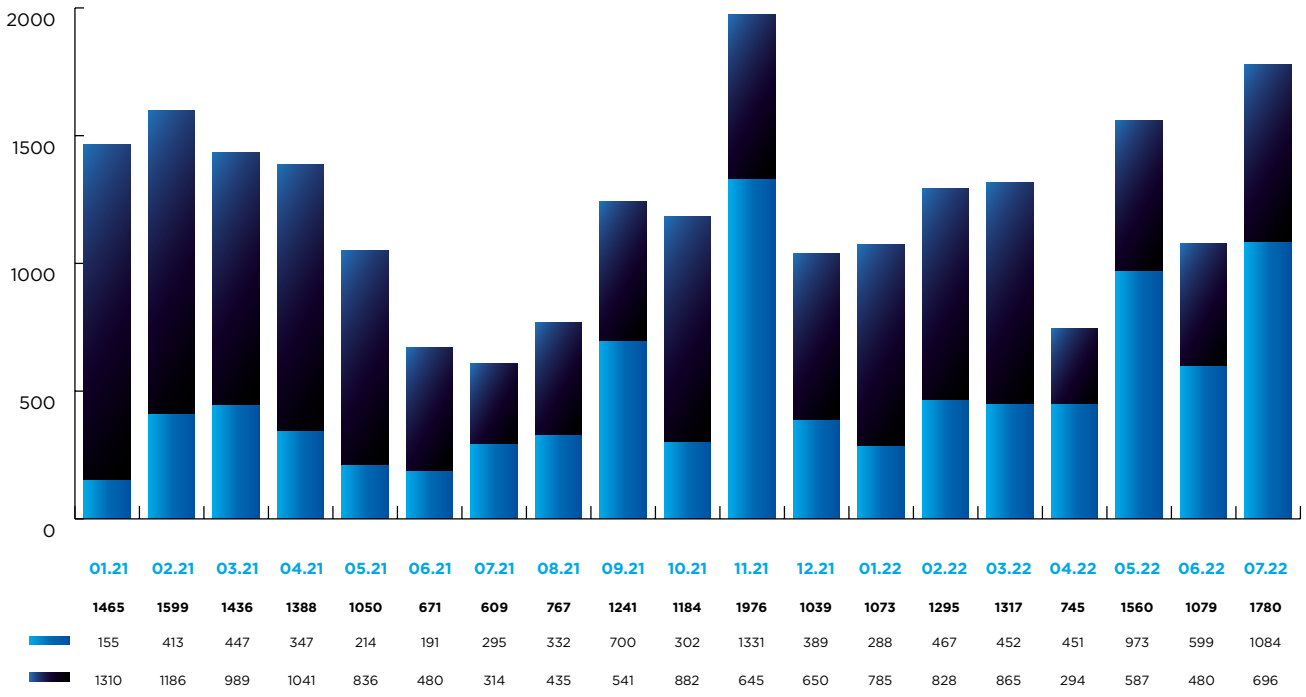
Druga, najbardziej elementarna, metoda mitygacji ataku to blackhole, czyli **odrzucenie wszystkich pakietów IP**

[12] Usługa SSH (secure shell) pozwala na bezpośrednie zarządzanie serwerem z wykorzystaniem połączenia terminalowego.

[13] Wolumetryczne ataki DDoS opierają się na masowej wysyłce niepożądanych danych na konkretny adres IP. Liczba danych jest tak duża, że łącza nie są w stanie ich przyjąć, co prowadzi do wysycenia połączenia sieciowego i uniemożliwia skorzystanie z usługi.

[14] https://www.f5.com/labs/articles/threat-intelligence/2022-application-protection-report-ddos-attack-trends

Liczba mitygacji zarejestrowana przez EXATEL



	01.21	02.21	03.21	04.21	05.21	06.21	07.21	08.21	09.21	10.21	11.21	12.21	01.22	02.22	03.22	04.22	05.22	06.22	07.22
	1465	**1599**	**1436**	**1388**	**1050**	**671**	**609**	**767**	**1241**	**1184**	**1976**	**1039**	**1073**	**1295**	**1317**	**745**	**1560**	**1079**	**1780**
	155	413	447	347	214	191	295	332	700	302	1331	389	288	467	452	451	973	599	1084
	1310	1186	989	1041	836	480	314	435	541	882	645	650	785	828	865	294	587	480	696

skierowanych do atakowanego adresu. Wówczas nie weryfikuje się składników, które są „wrogie", a które są elementem normalnego ruchu. Ma to jednak pewne minusy, ponieważ jeden (atakowany) adres, na czas trwania ataku, traci możliwość komunikacji. Z drugiej strony, dzięki temu pozostałe zasoby sieciowe danego klienta mogą korzystać z sieci w sposób niezakłócony. Ta metoda jest dobrym rozwiązaniem zwłaszcza dla użytkowników, którzy mogą pozwolić sobie na przerwy w komunikacji, a ich budżet przeznaczany na zabezpieczenia jest mocno ograniczony.

Kiedy zaczęła się pandemia COVID-19, liczba ataków DDoS wzrosła. Przyczyniły się do tego: praca i edukacja w trybie online oraz wzrost popularności usług internetowych, zwłaszcza zakupów. Aby zwiększyć swoją skuteczność, atakujący wykorzystali rosnący popyt na usługi online. Dzięki temu mogli szantażować usługodawców, dla których brak możliwości prowadzenia działalności był wyjątkowo dotkliwy i powodował duże straty.

Ten wzrost utrzymywał się także na początku 2021 r., co wykazał zespół EXATEL. Do podobnych wniosków doszli również eksperci firmy ENISA, którzy zauważyli nie tylko znaczny wzrost ataków DDoS w 2020 r., ale także to, że w 2021 r. było ich jeszcze więcej[15]. Atakowano przede wszystkim instytucje zajmujące się edukacją.

Statystyki ataków w trakcie COVID-19

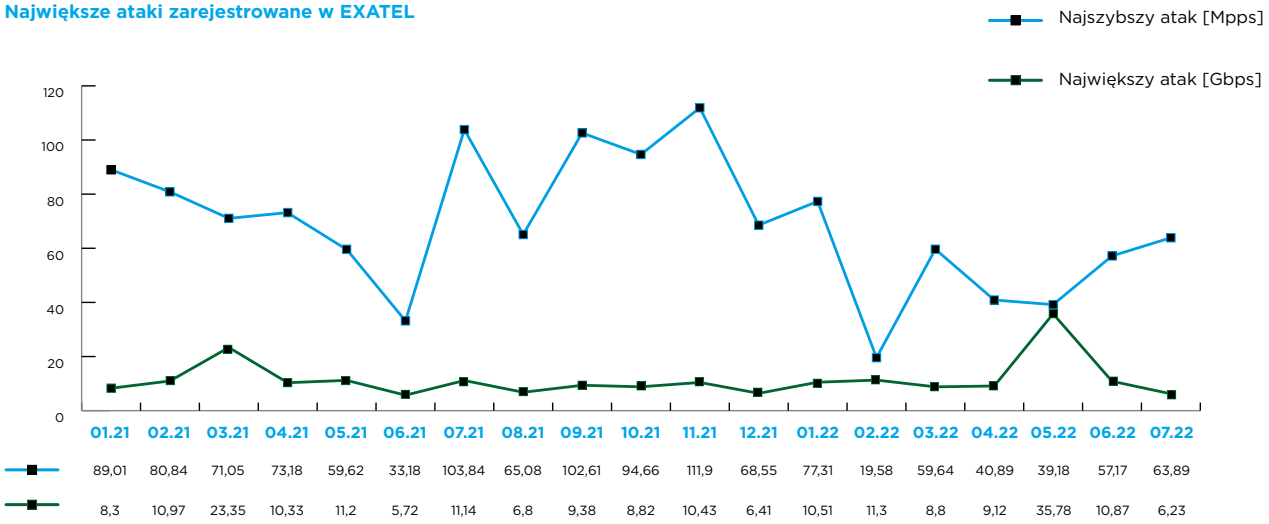
135 851
Liczba alarmów rozpoczętych w zadanym okresie

11 190 Gbps
Największe ataki

3578 Mpps
Najszybszy atak

[15] Telecom Security Incidents 2021, s. 4.

Największe ataki zarejestrowane w EXATEL



	01.21	02.21	03.21	04.21	05.21	06.21	07.21	08.21	09.21	10.21	11.21	12.21	01.22	02.22	03.22	04.22	05.22	06.22	07.22
■	89,01	80,84	71,05	73,18	59,62	33,18	103,84	65,08	102,61	94,66	111,9	68,55	77,31	19,58	59,64	40,89	39,18	57,17	63,89
■	8,3	10,97	23,35	10,33	11,2	5,72	11,14	6,8	9,38	8,82	10,43	6,41	10,51	11,3	8,8	9,12	35,78	10,87	6,23

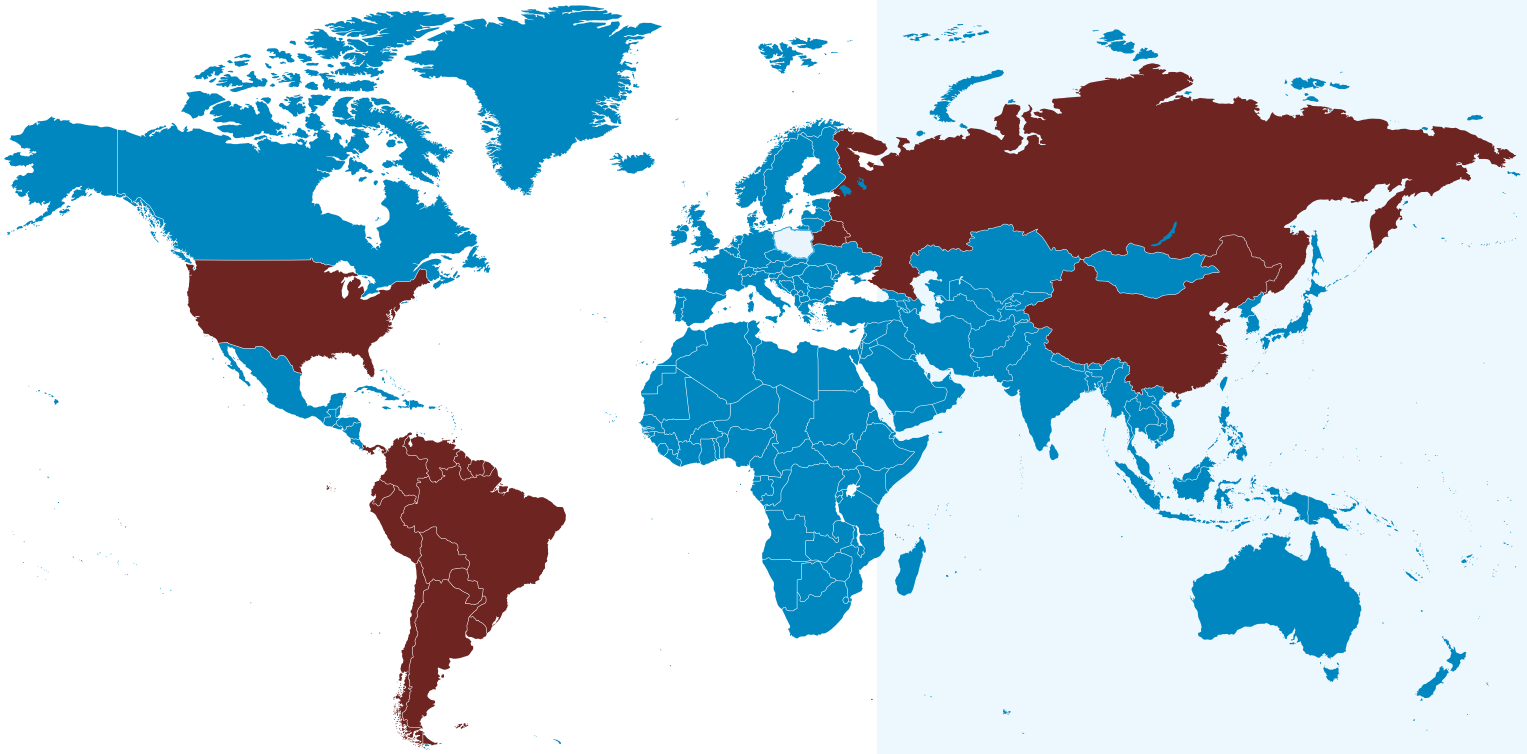
Wojna w Ukrainie to większe ryzyko cyberataków

W okresie wakacyjnym w 2021 r. liczba przeprowadzanych ataków DDoS zmalała. Jednak spadek aktywności cyberprzestępców niekoniecznie wiązał się z wielkością ataków. Dla przykładu w lipcu 2021 r. odnotowano mniej ataków, a jednocześnie w tym miesiącu zarejestrowano jeden z największych ataków.

Obszary geograficzne,

z których najczęściej pochodzą ataki DDoS:

USA, Chiny, Państwa Ameryki Południowej, Rosja, Białoruś



Na początku 2022 r. hakerzy znów zwiększyli swoją aktywność. Charakterystyka ich działalności pokazuje, że miało to bezpośredni związek z wojną w Ukrainie. Obserwacje EXATEL są tutaj tożsame z ustaleniami ekspertów Cloudfare, którzy również zidentyfikowali zwiększoną liczbę ataków DDoS w związku z rosyjską agresją 24 lutego 2022 r. Cyberataki były wymierzone zarówno w obiekty rosyjskie, jak i ukraińskie oraz zachodnie[16]. Dlatego uzasadnione jest utrzymanie w cyberprzestrzeni poziomu alarmowego Charlie-CRP[17].

Każdy atak trwa średnio 10 minut. Jednak takie działania często prowadzone są seriami (np. około 10 minut ataku, przerwa, i kolejny atak). Trwa to nierzadko przez kilka kolejnych dni.

Obecnie najpopularniejsza metoda radzenia sobie z atakami to odrzucanie całości ruchu do atakowanego celu (adresu lub adresów IP). Widać jednak, że coraz więcej podmiotów wykorzystuje mechanizmy filtrujące, których celem jest zachowanie ciągłości działania infrastruktury.

[16] https://blog.cloudflare.com/ddos-attack-trends-for-2022-q1/

[17] Stopień Charlie-CRP jest trzecim z czterech stopni alarmowych określonych w ustawie o działaniach antyterrorystycznych. Stopień ten jest wprowadzany w przypadku wystąpienia zdarzenia potwierdzającego prawdopodobny cel ataku o charakterze terrorystycznym w cyberprzestrzeni albo uzyskania wiarygodnych informacji o planowanym zdarzeniu.

ROZDZIAŁ II

Problemy i zaniedbania dotyczące cyberbezpieczeństwa

Eksperci SOC EXATEL zrealizowali u klientów (sektory: edukacyjny, finansowy, bankowy, publiczny) 250 projektów weryfikacji cyberbezpieczeństwa. Sprawdzili poziom zabezpieczeń:

- oprogramowania,
- urządzeń, m.in. systemów służących do transmisji satelitarnej,
- programowalnych sieci komputerowych (SDN)[18].

Pozwoliło to sformułować wnioski dotyczące najczęściej spotykanych problemów oraz zaniedbań bezpieczeństwa w sieci.

250 projektów

w sektorach: edukacyjnym, finansowym i publicznym

Eksperci odnotowali, że w infrastrukturze klientów często znajdują się narzędzia, systemy, urządzenia, które nie są w odpowiedni sposób zabezpieczone. Problemem jest też niewłaściwa polityka aktualizacji oprogramowania. W efekcie najnowsze łatki, w tym łatki bezpieczeństwa, nie są instalowane. Jest to niebezpieczne zwłaszcza, gdy występują podatności krytyczne, które atakującym ułatwiają działanie i powodują większe zagrożenie dla infrastruktury informatycznej organizacji. Co więcej pracownicy wykorzystują sprzęt służbowy do celów prywatnych, przez co narażają go na dodatkowe zagrożenia.

Ryzyko cyberataku u klientów EXATEL wzrasta również dlatego, że uruchamiają oni usługi z uprawnieniami administratora oraz nadają wysokie uprawnienia zwykłym użytkownikom. Jeżeli atakujący uzyska dostęp do urządzenia końcowego, którego usługi uruchamiają się z uprawnieniami administratora, to ma pełną swobodę w swojej szkodliwej działalności.

Wydawałoby się, że odpowiednie zabezpieczenie korporacyjnych sieci Wi-Fi jest obecnie standardem. Niestety przeanalizowane projekty wykazały poważne uchybienia. Brakuje odpowiednich mechanizmów uwierzytelnienia, co skutkuje ryzykiem podsłuchu czy modyfikacji ruchu sieciowego. W skrajnych przypadkach może dojść nawet do uzyskania przez cyberprzestępców dostępu do sieci przewodowej w danej organizacji. Może to wyrządzić poważne szkody – od kradzieży danych do paraliżu organizacji.

Eksperci EXATEL wskazali również na problem z podziałem lokalnej sieci komputerowej (LAN), który pozwala ograniczyć dostęp z jednego segmentu sieci do drugiego. Dzięki takiemu podziałowi łatwiej zarządzać dostępami oraz powstrzymać potencjalnego hakera przed atakiem na całą sieć. Z kolei brak podziału zwiększa pole do ataku, a przejęcie kontroli nad dowolnym urządzeniem końcowym znacznie przyspiesza całkowite przejęcie sieci.

Problemem jest także pozostawienie fabrycznych ustawień oraz poświadczeń w systemach wewnątrz sieci bądź w ich segmentach. Eksperci stwierdzili też brak izolacji z sieci systemów, które wycofano z produkcji i zastąpiono nowszymi.

Ponadto aplikacje, które są tworzone na zamówienie poszczególnych klientów, wymagają dokładnego testowania bezpieczeństwa. Niestety, ich twórcy to zaniedbują i rzadko w trakcie pisania aplikacji wykonują

[18] SDN – sieć definiowana programowo. Idea, dzięki której warstwa fizyczna urządzenia (interfejsy fizyczne, układy ASIC, NPU) staje się jedynie częścią wykonawczą „mózgu sieci", czyli tzw. kontrolera. W rozwiązaniach SDN to aktywna warstwa kontrolera z aplikacjami definiuje funkcjonalności każdej maszyny i zarazem całej sieci, którą zarządza.

testy penetracyjne. Wynika to z braku czasu i konieczności dostarczenia danego produktu jak najszybciej na rynek.

Najczętsze problemy dotyczące cyberbezpieczeństwa (według ekspertów EXATEL)

- **Występowanie w infrastrukturze klienta niewłaściwie zabezpieczonych systemów, narzędzi i usług**
- **Wykorzysywanie prywatnego sprzętu do celów służbowych**
- **Niewystarczająca polityka aktualizacji aplikacji**
- **Niewłaściwe zabezpieczenie Wi-Fi**
- **Niedostateczne testowanie aplikacji pod kątem bezpieczenstwa**

Badania bezpieczeństwa wykazały, że zdecydowanie za to poprawiła się kwestia kopii bezpieczeństwa serwerów i usług. Z reguły kopie bezpieczeństwa są wykonywane. Niestety cały czas pojawiają się problemy z ich odpowiednim przechowywaniem. Eksperci wykryli na przykład stworzenie backupu systemu kontroli dostępu w katalogu serwera WWW, co pozwalało na wyświetlanie zawartości wybranego katalogu lub pliku kopii obecnych haseł.

Spostrzeżenia ekspertów EXATEL pokrywają się z wnioskami z raportu firmy Palo Alto Networks. Podstawowym problemem, według autorów raportu, jest brak wielostopniowego uwierzytelnienia na takich systemach jak:

- poczta korporacyjna,
- VPN,
- inne usługi dostępne zdalnie.

Kolejnym ważnym zagadnieniem jest brak narzędzi albo ich niewłaściwa konfiguracja niezbędna do wykrywania zagrożeń na urządzeniach końcowych. Amerykanie wskazali również na niewłaściwą politykę aktualizacji oprogramowania, przez co zaniedbywane jest instalowanie łatek bezpieczeństwa. Organizacje nie są ponadto przygotowane na ataki brute-force. Nie bez znaczenia jest to, że przez te różne błędy i przeoczenia część podejrzanych aktywności pozostaje niewykryta.

Bezpieczeństwo to nie tylko audyt

Dlatego analitycy SOC EXATEL uważają, że bezpieczeństwo jest dynamicznym procesem, a nie stanem, który nie podlega żadnym przekształceniom. To, że systemy i sieci są bezpieczne teraz, nie oznacza, że będą bezpieczne również za kilka miesięcy, a nawet tygodni. Potrzebna jest systematyczna kontrola i sprawdzanie zabezpieczeń. Bezpieczeństwo nie może być postrzegane tylko przez pryzmat audytu, a niestety często tak się dzieje.

Security Operations Center (SOC) EXATEL to dynamiczna struktura, która ciągle się adaptuje i zmienia wraz z zagrożeniami, które również ulegają transformacji

Uruchomienie SOC w danej organizacji i pierwsze miesiące działania pozwalają poznać środowisko, zagrożenia oraz uporządkować to, co nie działa zbyt dobrze. Jednak, by tak się stało i by eksperci mogli zagwarantować bezpieczeństwo w sieci, konieczna jest współpraca ze strony tej organizacji.

Ponad 250 zrealizowanych projektów pozwoliło firmie EXATEL storzyć rekomendacje dla klientów. Przede wszystkim należy dbać o aktualizacje rozwiązań, zwłaszcza tych udostępnionych do internetu, i je monitorować. Drugą rekomendacją jest to, aby firmy upewniły się, że logi, których używają, zapewniają odpowiedni zakres informacji. Chodzi zwłaszcza o to, aby uniknąć sytacji, w których np. pojawiają się informacje o próbie logowania, natomiast brakuje nazwy konta użytkownika, którego dotyczy ta aktywność. Ważne jest także, aby mieć więcej rozwiązań, które wykrywają zagrożenia, np. narzędzi do analizy ruchu sieciowego i złośliwych plików czy do wykrywania podejrzanej aktywności na serwerach.

Przykład **działania ekspertów EXATEL**

Badanie haseł w korporacjach

Eksperci EXATEL przeprowadzili badanie odporności haseł użytkowników na ataki słownikowe oraz ataki brute-force.

Metoda

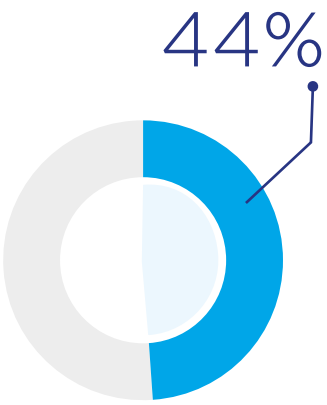
Dane zagregowali z domen Active Directory dwóch dużych firm. Aby uzyskać hashe haseł LM, wykonali kopie zapasowe plików NTDS.DIT oraz rejestru HKLM\SYSTEM z kontrolerów domeny. Następnie, za pomocą pakietu Impacket, dane zostały sparowane w celu otrzymania hashy LM poszczególnych użytkowników. Konta „maszynowe" (czyli takie, które mają $ na końcu nazwy użytkownika) nie były liczone do pełnej puli kont użytkowników, ponieważ użytkownicy zazwyczaj nie mają kontroli nad ustawionymi tam hasłami. Ponadto według dokumentacji Microsoft hasła tych kont składają się ze 120 znaków z alfabetu UTF-16, co skutecznie uniemożliwia ich złamanie metodą brute-force.

W sumie, w obu domenach znalazło się 2412 hashy haseł. Wśród nich mogły być hashe haseł do kont, które w momencie wykonywania badań były nieaktywne, jednak – ze względu na różnice między danymi zwróconymi przez pakiet Impacket, a rzeczywistym stanem domeny – nie zostały odfiltrowane. Udało się odzyskać około 35% (843/2412) haseł do unikalnych kont.

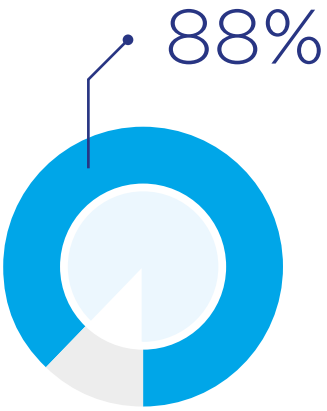
Eksperci zbadali też dane historyczne (tam gdzie było to możliwe). Zebrali 15 668 hashy haseł, z czego odzyskali 38% (6083/15 668). W badaniu wykorzystano następujące słowniki:

- wordlist_pl.txt – słownik najpopularniejszych polskich haseł, udostępniony przez CERT Polska,
- słownik oparty o maskę: „Nazwa_firmy?a?a?a?a" – gdzie „?a" oznacza znak możliwy do wpisania na klawiaturze (małe litery, wielkie litery, cyfry, znaki specjalne),
- rockyou.txt – lista haseł z wycieku danych z firmy RockYou.

Dodatkowo eksperci użyli skryptu przetworzeń (rules): OneRuleToRuleThemAll (https://github.com/NotSoSecure/password_cracking_rules).



W 44% przypadków nazwa firmy była jednym z członów hasła



W 88% przypadków występował przynajmniej jeden problem związany ze stosowaniem hasła o niewystarczającej sile

Wnioski

Okazało się, że najwięcej było ataków słownikowych, z włączonymi skryptami przetworzeń narzędzia hashcat.

W aż 44% (376/843) przypadków nazwa firmy była jednym z członów hasła (w hasłach historycznych było to 41% – 2503/6083). Wśród odzyskanych haseł były też takie typu „Lato2022” lub „Styczen2021”. Co więcej, na podstawie analizy danych historycznych (także zapisanych w domenie Active Directory), można stwierdzić, że użytkownicy, którzy muszą okresowo (np. co miesiąc) zmieniać hasło, zmieniają jedynie jego początek lub koniec. Oto przykłady takich zmian:

- „Haslo1234” -> „Haslo1235”,
- „Haslo1234” -> „1234Haslo”.

Takie działanie daje znikomy poziom bezpieczeństwa przed atakami słownikowymi. Dostęp nawet do danych sprzed kilku miesięcy lub lat może pozwolić hakerowi odgadnąć hasło, które atakowany użytkownik stosuje aktualnie. Warto także pamiętać, że Narodowy Instytut Samorządu Terytorialnego (NIST) w dokumencie NIST 800-63B, zaleca odejście od dotychczasowej praktyki okresowej zmiany haseł. Niestety, to zalecenie wciąż spotyka się ze zdziwieniem wśród administratorów i osób odpowiedzialnych za cyberbezpieczeństwo.

Innym, i wciąż dużym, problemem są także „słabe” hasła. Według ekspertów EXATEL aż w 88% przypadków, które analizowali u swoich klientów, występował przynajmniej jeden problem związany ze stosowaniem hasła o niewystarczającej sile. Co oznacza, że „słabe” hasło pośrednio lub bezpośrednio przyczyniło się do przejęcia infrastruktury informatycznej danej firmy.

ROZDZIAŁ III

Jak pracują **eksperci SOC EXATEL**

Security Operations Center (SOC) EXATEL to wyspecjalizowane centrum bezpieczeństwa, które bazuje na trzech fundamentach:

- ludzie,
- technologia,
- procesy i proceduy.

SOC zaczął działać w 2017 r. Początkowo eksperci skupiali się na potrzebach firmy EXATEL. Z czasem jednak poszerzali pole swojej działalności. Obecnie zespoły pracują w trybie 24 godziny przez 7 dni w tygodniu. Dzięki temu prowadzą ciągły monitoring sieci, na bieżąco wykrywają zagrożenia i analizują bezpieczeństwo systemów oraz infrastruktury IT. Gwarantują szybkie reagowanie na incydent, który może stanowić poważne ryzyko dla działania danej organizacji.

Eksperci SOC w pracy – stacjonarnej i zdalnej – korzystają z rozwiązań własnych oraz takich jak: SIEM[19], EDR[20], AntyMalware z m.in. platformami GRC[21]. Zakres ich usług można podzielić na trzy kategorie:

- monitorowanie i obsługa incydentów,
- reakcja na incydent (rozwinięcie usługi monitorowania i obsługi incydentów),
- prewencja.

[19] SIEM (security information and event management) – platforma, która jest wykorzystywana do gromadzenia, monitorowania i analizowania zdarzeń związanych z bezpieczeństwem.

[20] EDR (endpoint detection and response) – rozwiązanie z zakresu cyberbezpieczeństwa pozwalające wykrywać i reagować na zagrożenia znajdujące się na urządzeniu końcowym.

Usługi SOC EXATEL

Monitorowanie i obsługa incydentów:

- zbieranie, analizowanie oraz kojarzenie zdarzeń, które zachodzą w sieciach i systemach klienta,
- analizowanie zebranych danych po automatycznej weryfikacji w systemach klienta,
- wykrywanie zdarzeń lub incydentów bezpieczeństwa,
- ocena wpływu incydentu bezpieczeństwa IT na systemy klienta,
- sprawdzenie fałszywych alarmów (false positive),
- obsługa zdarzeń zgodne z procedurami (np. eskalacja incydentu).

Reakcja na incydenty (rozwinięcie usługi monitorowania i obsługi incydentów):

- zdalna reakcja na wykryte zdarzenie w cyberprzestrzeni,
- kontakt z zespołem bezpieczeństwa z firmy klienta,
- doradztwo w zakresie działań niwelujących negatywne skutki incydentu,
- zbieranie brakujących informacji w przypadku bardziej zaawansowanych ataków,
- pogłębione analizy, np. znalezionych próbek złośliwego oprogramowania, komunikacji z sieciami botnet czy command and control (C&C),
- wsparcie w zakresie analiz powłamaniowych (forensics).

Prewencja:

- proaktywna kontrola, która zapobiegająca wielu incydentom bezpieczeństwa ICT,
- testy penetracyjne i rekonesans bezpieczeństwa,
- audyty i przeglądy bezpieczeństwa,
- wyszukiwanie i ocena podatności,
- wsparcie w zakresie bezpieczeństwa informacji dotyczące zapewniania zgodności z wymaganiami prawnymi lub korporacyjnymi,
- doradztwo w zakresie organizacji własnych zespołów bezpieczeństwa (procesów, technologii, zasobów ludzkich).

Centrum bezpieczeństwa EXATEL

działa na trzech liniach wsparcia:

1 linia (L1) – zespół analityków odpowiedzialny za:
- monitoring bezpieczeństwa ICT,
- monitoring selekcji i priorytetyzacji incydentów,
- obsługę incydentów – zgodnie z zaprojektowanymi scenariuszami,
- podstawową analizę aplikacji.

2 linia (L2) – zespół analityków odpowiedzialny za:
- obszar zarzadzania incydentami, w tym koordynację obsługi incydentów,
- zamykanie biletów problemowych,
- projektowanie korelacyjnych reguł bezpieczeństwa oraz ich ciągłe udoskonalanie,
- przygotowanie dla analityków L1 scenariuszy obsługi incydentów.

3 linia (L3) – zespół ekspertów z dziedziny zaawansowanych usług bezpieczeństwa odpowiedzialny za:
- analizę skomplikowanych zagrożeń i technik ataków,
- administrację i strojenie platform bezpieczeństwa.

Zespoły L2 i L3 działają, gdy dochodzi do eskalacji naruszeń wykrytych przez zespół L1. Podejmują także działania dotyczące naruszeń zgłoszonych przez klienta. Analiza, którą prowadzą eksperci z linii L2 i L3, może trwać od kilku dni do nawet kilku miesięcy.

Wsparcie dostosowane do potrzeb

Warianty usług, jakie proponuje SOC EXATEL, zależą od potrzeb klientów, złożoności systemów ICT, wdrożonych procesów i procedur bezpieczeństwa. W oparciu o te czynniki każdą ofertę można dopasować do konkretnych wymagań danej organizacji.

- **Usługa SOC Assistance** – najprostsza oferta wsparcia, która obejmuje reagowanie na wykryte przez klienta incydenty bezpieczeństwa. Eksperci SOC pozostają w gotowości w trybie 24/7/365 i w sytuacji kryzysowej prowadzą obsługę incydentu.
- **Usługa SOC Wsparcie** – szersze wsparcia SOC, które wykracza poza asystę przy incydentach bezpieczeństwa. Eksperci SOC realizują także prace w trybie projektowym z zakresu zaawansowanych usług cyberbezpieczeństwa, takie jak szkolenia, audyty czy pentesty.
- **Usługa SOC** – monitorowanie przez zespół SOC sieci i systemów klienta – w trybie 24/7/365. Klient może wybrać:
  1. ofertę, która polega na obserwacji newralgicznych źródeł danych oraz dostarczaniu okresowych raportów na temat stanu bezpieczeństwa infrastruktury,
  2. usługę, która jest świadczona w innych trybach niż 24/7/365, np. w trybie 16/7/365 – po godzinach pracy i na jego rozwiązaniach bezpieczeństwa.

Szczegółowe i przejrzyste raporty

Eksperci SOC EXATEL rozwiązują ponadto częsty problem, który jest związany z brakiem czasu klientów na analizę zdarzeń rejestrowanych przez ich rozwiązania i narzędzia bezpieczeństwa. W efekcie braku takiej analizy atak na infrastrukturę firmy może nie zostać zauważony. Eksperci z 2 liniii (L2) tworzą szczegółowe raporty okresowe. Każdy raport zawiera:

- analizy,
- statystyki,
- informacje o tym, gdzie i kiedy wydarzył się dany incydent oraz jego charakterystykę,
- wykresy pomocne przy ocenie bezpieczeństwa analizowanego okresu,
- pogłębioną analizę złożonych i zaawansowanych incydentów,
- porównanie bieżącego okresu z poprzednim,
- rekomendacje dalszych działań, aby uniknąć podobnych zdarzeń w przyszłości,
- porady, jak poprawić bezpieczeństwo usług, których dotyczył dany incydent.

Raport jest opracowany w sposób czytelny dla każdego odbiorcy. Dzięki temu klient może łatwo ocenić stan cyberbezpieczeństwa swojej firmy i podjąć odpowiednie działania.

Eksperci SOC EXATEL organizują również cykliczne spotkania z klientem. Podczas tych spotkań klient może przekazać swoje uwagi dotyczące wsparcia SOC, szerzej omówić dane przedstawione w raporcie okresowym czy dowiedzieć się, co powinno zostać poprawione w jego środowisku informatycznym. Dzięki kompleksowym poradom klient może zaplanować także szersze działania dotyczące innych usług SOC.

NASZ EKSPERT

MAREK MAKOWSKI,
Główny Inżynier ds. Rozwoju Zaawansowanych Usług Bezpieczeństwa w Departamencie Cyberbezpieczeństwa

Business Product Owner autorskiego rozwiązania chroniącego przed atakami DDoS – TAMA

„Ataki DDoS są tanim i skutecznym sposobem na doprowadzenie atakowanego do poważnych strat finansowych i wizerunkowych. Ochrona przed wszelkiego rodzaju zagrożeniami cybernetycznymi, w tym przed DDoS, powinna być wielopoziomowa. Jako EXATEL koncentrujemy swoje wysiłki na dostarczaniu najskuteczniejszych rozwiązań z pozycji operatora telekomunikacyjnego. Dzięki temu, że (w ramach prowadzonych w spółce projektów R&D) opracowaliśmy autorski system ochrony przed atakami DDoS, mamy dużą swobodę działania w tym zakresie."

Skuteczna **TAMA**

TAMA (usługa anty-DDoS) to autorskie, skalowalne i wydajne rozwiązania, które chronią sieć przed atakami typu DDoS. Ochrona oparta jest na platformie centralnej. EXATEL proponuje to rozwiązanie w modelu usługowym (as a service). System TAMA bada poziom ruchu IP w dwóch ujęciach: bity na sekundę oraz pakiety na sekundę. Składa się z kilku elementów:

- **Aperture** monitoruje ruch sieciowy z routerów brzegowych oraz agreguje informacje statystyczne i przekazuje do Kontrolera.
- **Kontroler** integruje z sond informacje o aktualnym stanie monitorowanej sieci oraz zapisuje je do bazy analitycznej. Podejmuje też decyzje o wykryciu, podtrzymaniu i zamknięciu alarmu oraz uruchamia i zatrzymuje automatyczne mitygacje.
- **GlaDDoS** to jednostka filtrująca. Jej przepustowość zależy od polityki mitygacji oraz parametrów serwera, na którym filtr został uruchomiony. Aby osiągnąć jak najlepszą wydajność, jednostki filtrujące są rozproszone.
- **Chell** to konsola zarządzająca, która pozwala administratorom i operatorom dbać o bezpieczeństwo sieci klientów.
- **Portal klienta** to dodatkowy element, za pośrednictwem którego klienci mogą obserwować alarmy i mitygacje wyzwolone dla swoich obiektów oraz monitorować ruch w swojej sieci.

Rozwiązanie firmy EXATEL jest inne od produktów konkurencji. Wyróżnia je:

- architektura oparta na ogólnodostępnym sprzęcie x86 bez konieczności zakupu drogich układów FPGA[22] i ASIC[23],
- przepustowości 100 Gbps dzięki wykorzystaniu efektywnych technik skalowania pionowego oraz poziomego,
- zastosowanie autorskich mechanizmów i technik zawierających elementy uczenia maszynowego,
- możliwość równoczesnej ochrony wielu klientów o różnych politykach oraz ochrony łącz niezależnie od działania dostawcy,
- szybki i elastyczny silnik decyzyjny do identyfikacji i neutralizacji zagrożeń.

[22] FPGA - (field programmable gate array) - rodzaj programowalnego układu logicznego.

[23] ASIC – Application-specific integrated circuit

Jeszcze lepsza ochrona SOC EXATEL
Poza TAMĄ i własnym SOC, EXATEL oferuje również inne usługi z zakresu cyberbezpieczeństwa.

Antymalware pozwala na kompleksowe zabezpieczenie zasobów IT klienta przed złośliwym oprogramowaniem. W porównaniu do tradycyjnych rozwiązań antywirusowych nie posługuje się wyłącznie sygnaturami wirusów, ale korzysta z zaawansowanych mechanizmów analitycznych. EXATEL oferuje pełne uruchomienie, konfigurację oraz zarządzanie oprogramowaniem. Usługa jest świadczona na platformie Elevate XDR firmy Fidelis, lidera w dziedzinie automatycznego wykrywania i reagowania na zagrożenia w sieci.

Antymalware pozwala lepiej chronić własność intelektualną i inne zasoby organizacji. Zapewnia też pełną widoczność na wszystkich portach i protokołach sieciowych oraz automatyzację zabezpieczeń w oparciu o elastycznie tworzone, a także modyfikowane reguły i polityki. Ponadto usługa ta:

- minimalizuje koszty obsługi,
- skraca czas potrzebny, aby rozwiązać incydenty bezpieczeństwa ICT,
- poprawia dostęp do szczegółowych danych historycznych, które mogą być przydatne w analizach powłamaniowych.

173 rodzaje usług

ochrony przed atakami DDoS oferuje EXATEL

Usługa DLP (data loss prevention) pozwala chronić firmę przed jednym z największych obecnie problemów – wyciekiem danych - jednym, które nie tylko powodują utratę reputacji i wiarygodności, ale też poważne straty finansowe. Usługa EXATEL zabezpiecza przed wyciekiem informacji, które zawierają własność intelektualną, dane osobowe i inne wrażliwe zasoby klienta. Ochrona bazuje na platformie centralnej Fidelis Elevate XDR i na urządzeniach (sensorach) w lokalizacji klienta. Cały ruch sieciowy jest badany na poziomie protokołów, aplikacji i treści. Platforma Fidelis Elevate XDR wykorzystuje opatentowaną technologię Deep Session Inspection, której działanie polega na dekodowaniu i ekstrakcji treści, nawet jeżeli są one głęboko ukryte.

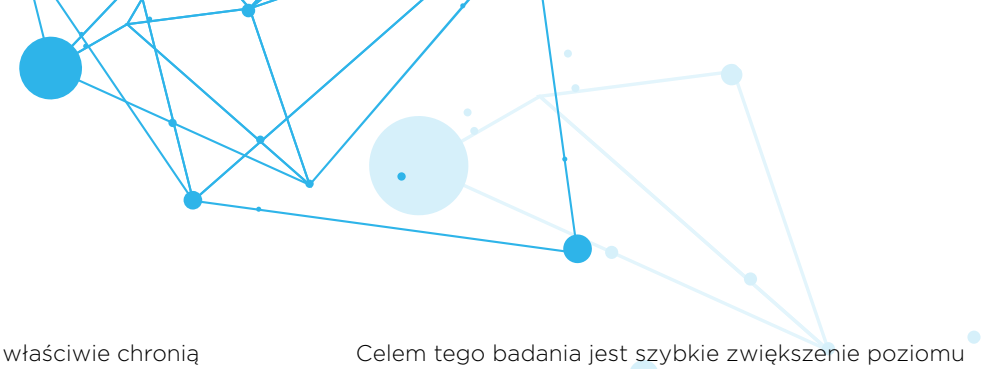
Usługa DLP gwarantuje ochronę wizerunku i reputacji firmy oraz zapewnia zgodność z wymaganiami regulacyjnymi, takim jak RODO, dyrektywa PSD2 czy Ustawa o Krajowym Systemie Cyberbezpieczeństwa (UKSC). Przy czym sama ochrona danych wspomagana automatycznymi mechanizmami nie wymaga angażowania dużych zasobów ludzkich po stronie klienta. DLP za pomocą tej samej platformy można łączyć z usługą antymalware.

Testy penetracyjne polegają na przeprowadzaniu na systemach teleinformatycznych kontrolowanego ataku, który ma pomóc ocenić bieżący stan bezpieczeństwa sieci. Eksperci EXATEL analizują badane systemy pod kątem występowania potencjalnych zagrożeń i błędów, takich jak niewłaściwa konfiguracja, luki w oprogramowaniu lub sprzęcie, słabości w technicznych albo proceduralnych środkach zabezpieczeń czy niewystarczająca świadomość użytkowników. Testy penetracyjne mogą być realizowane na trzy sposoby:

- **Blackbox** – brak wiedzy o testowanym systemie,
- **Graybox** – z ograniczoną wiedzą o testach,
- **Whitebox** – z dostępem do pełnej wiedzy o testach.

Pentesterzy, czyli osoby przeprowadzające testy, posługują się wieloma narzędziami automatyczymi, takimi jak skanery podatności itp. Uzyskane wyniki zawsze manualnie weryfikują, próbując wykorzystać daną podatność, i przedstawiają dowody, które potwierdzają możliwość realnego ataku. Pozwala to firmie lepiej rozpoznawać i inwentaryzować własne zasoby informatyczne oraz weryfikować wdrożone rozwiązania techniczne i procesowo-proceduralne. Testy penetracyjne pozwalają również uzyskać zgodność z regulacami prawnymi, takim jak RODO czy UKSC oraz normami ISO 27001 czy ISO 22301.

Audyty bezpieczeństwa to z kolei kompleksowe procesy zbierania i oceniania dowodów. Ich celem jest określenie, czy system informatyczny i związane



z nim elementy procesowe właściwie chronią zasoby firmy. Podczas audytu eksperci analizują techniczne i nietechniczne środki ochrony, które są wykorzystywane w organizacji, aby utrzymać dostępność, poufność i integralność danych.

Po zakończonym audycie klient otrzymuje raport, w którym omówione są zarówno słabe punkty w systemach bezpieczeństwa, ocena ryzyka ich występowania, a także konkretne wskazówki dotyczące usprawnień, które mogą zminimalizować zagrożenia. Audyty bezpieczeństwa mogą dotyczyć:

- systemów informatycznych, np. konkretnych aplikacji WWW,
- konfiguracji platform bezpieczeństwa czy sieci lokalnych – przewodowych i bezprzewodowych,
- punktów styku sieci z internetem.

Audyty bezpieczeńswa również pomagają uzyskać zgodność z regulacjami prawnym, takimi jak RODO czy UKSC oraz normami ISO 27001 czy ISO 22301.

Rekonesans bezpieczeństwa jest eksperckim kilkudniowym, pogłębionym i efektywnym badaniem poziomu cyberbezpieczeństwa infrastruktury firmy. Celem tego badania jest szybkie zwiększenie poziomu jej bezpieczeństwa. Eksperci EXATEL dostarczają wymiernych wyników, które osiągają, wybiórczo weryfikując procedury i rozpoznając środowisko teleinformatyczne pod kątem potencjalnych zagrożeń. Następnie wytypowane w ten sposób elementy sieci badają pod kątem najbardziej istotnych zagrożeń. Na koniec przekazują firmie raport zawierajacy opis wykrytych luk bezpieczeństwa, które mogą być wykorzystane w potencjalnych wektorach ataku, oraz propozycje działań mitygujących. Zalety takiego rowiązania dla firm to:

- szybka i skuteczna weryfikacja systemu zabezpieczeń organizacji,
- określenie priorytetowych działań dzięki uporządkowaniu kwestii cyberbezpieczeństwa,
- uzyskanie przekrojowej wiedzy na temat bezpieczeństwa organizacji we wszystkich kluczowych aspektach: ludzi, procesów i technologii,
- dostęp do rekomendacji, propozycji w zakresie cyberbezpieczeństwa,
- minimalny nakład zasobów.

Cyberbezpieczeństwo to branża, która nie zwalnia – niezależnie od aktualnych wydarzeń lokalnych czy globalnych.

Niezadresowane problemy z bezpieczeństwem są wykorzystywane przez atakujących już nie tylko do najprostszych ataków skutkujących, np. niedostępnością usługi, ale również do osiągania wymiernych korzyści finansowych. Ataki cybernetyczne jako usługa to jest rzeczywistość w jakiej funkcjonujemy, np. RaaS (Ransomware-as-a-Service). Przykład programu Bug Bounty organizowanego przez operatora ransomware LockBit 3.0, nie pozostawia wątpliwości, że kwestie bezpieczeństwa w organizacjach nie mogą być pomijane. Powinny być znacznie intensywniej dyskutowane niż dotychczas.

Nasze doświadczenia pozwalają stwierdzić, że – na szczęście – rośnie wśród kadry zarządzającej świadomość skutków niepodjęcia działań po zidentyfikowaniu ryzyka dotyczącego cyberbezpieczeństwa. W dalszym ciągu jednak potrzeba więcej rozwiązań praktycznych, które realnie poprawiają bezpieczeństwo w środowiskach teleinformatycznych IT oraz OT. Konieczne jest także utrzymywanie w firmach właściwego security awarness wśród pracowników.

Warto cały czas pamiętać, że bezpieczeństwo to proces, który powinien być stale udoskonalany ze względu na zmieniające się zagrożenia.

EXATEL

EXATEL S.A.
ul. Perkuna 47, 04-164 Warszawa
exatel.pl

Biuro Obsługi Klienta:
tel. 22 340 66 60
email: bok@exatel.pl

Twitter: Exatel_pl
LinkedIn: Exatel
Facebook: EXATELPL