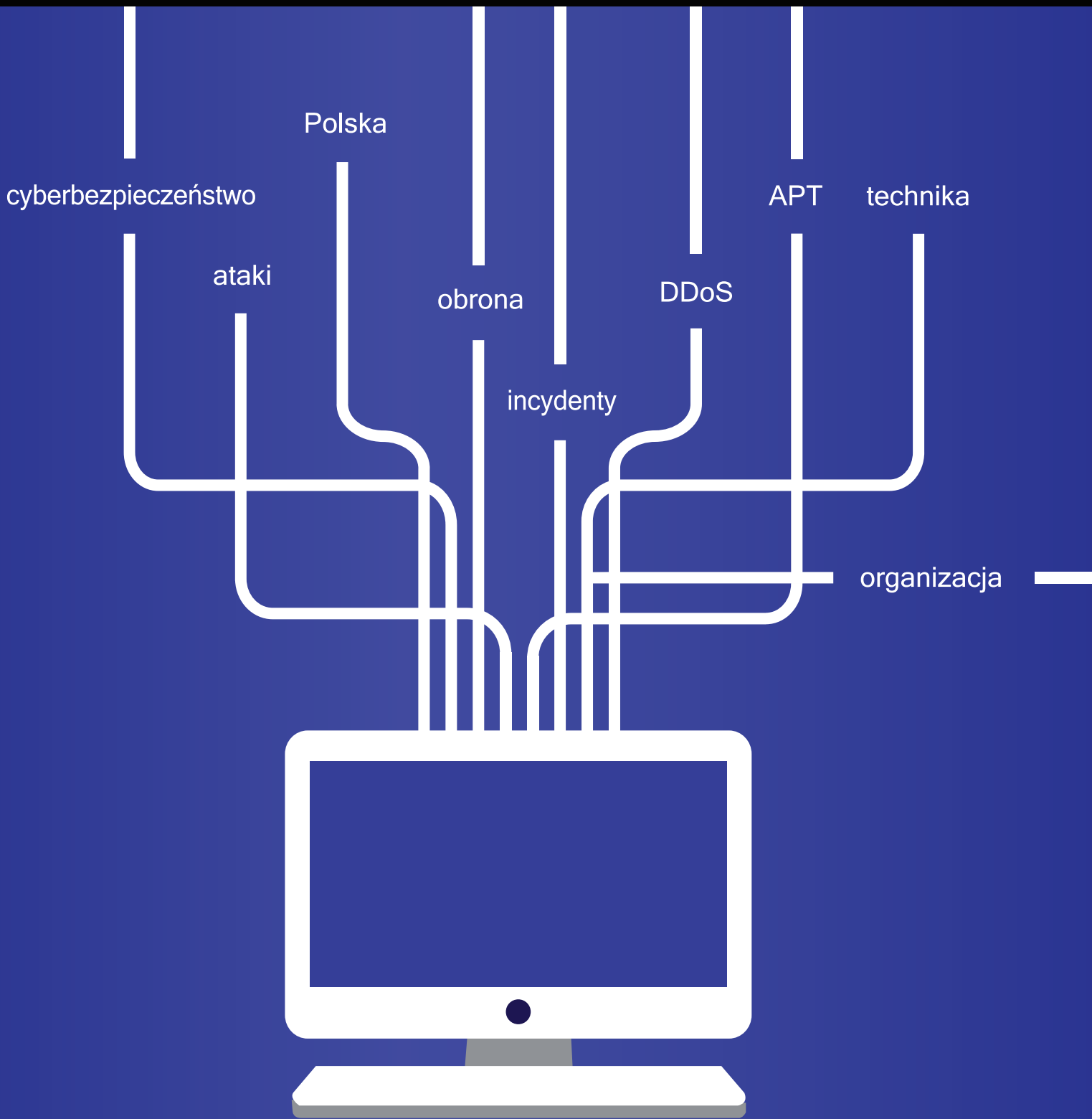
ATAK OBRONA 2013 RAPORT

Ataki i metody obrony w Internecie w Polsce



Edycja 2013

FUNDACJA bezpieczna cyberprzestrzeń

EVENTION
CZAS ZAANGAŻOWANY

Fundacja Bezpieczna Cyberprzestrzeń

Pozarządowa organizacja non-profit, której misją jest działanie na rzecz bezpieczeństwa cyberprzestrzeni, w tym na rzecz poprawy bezpieczeństwa w sieci. Osiągnięcie celów fundacja realizuje poprzez działalność w trzech głównych obszarach: UŚWIADAMIANIE o zagrożeniach teleinformatycznych, REAGOWANIE na przypadki naruszania bezpieczeństwa w cyberprzestrzeni, prowadzenie DZIAŁALNOŚCI BADAWCZO-ROZWOJOWEJ w dziedzinie bezpieczeństwa teleinformatycznego.

Evention

Spółka specjalizująca się w podnoszeniu wartości spotkań biznesowych na rynku ICT. W Evention wydarzenia biznesowe traktujemy jako integralny i trudny do zastąpienia element budowania relacji oraz poprawy efektywności tych relacji pomiędzy firmami i tworzącymi je ludźmi. Trzonem działalności spółki są spotkania realizowane w formule „custom event", w których kluczową rolę odgrywa zaangażowanie uczestników w całym procesie przygotowania wydarzenia. Szukamy innowacyjnych form realizacji spotkań, tak by odpowiadało to obecnym aspiracjom, oczekiwaniom oraz potrzebom menedżerów i profesjonalistów.

Ataki i metody obrony
w Internecie w Polsce

FUNDACJA
bezpieczna
cyberprzestrzeń

EVENTION
CZAS ZAANGAŻOWANY

Konferencja ATAK I OBRONA 2013
DDoS/APT

ATAK I OBRONA to nowa formuła spotkania profesjonalistów bezpieczeństwa IT. To konferencja w całości poświęcona cyberbezpieczeństwu – skupiona na najważniejszych i aktualnych zagrożeniach, której celem jest pokazanie i przekazanie istotnych zagadnień w najbardziej przystępnej i praktycznej formule, zakładającej aktywny udział wszystkich uczestników. Tematyka wydarzenia odnosi się do bieżących i istotnych cyberzagrożeń, które zgłaszają sami uczestnicy oraz praktycy, pragnący podzielić się swoimi doświadczeniami. Każdy z tematów, który pojawi się na konferencji, jest przedstawiony w postaci prezentacji praktycznego problemu (atak) i praktycznego rozwiązania (obrona).

W roku 2013 tematem przewodnim były zagrożenia DDoS (Distributed Denial of Service) i APT (Advanced Persistant Threat).

Partner generalny

TREND MICRO

Partnerzy strategiczni

TEAM CYMRU

SOURCEfire

Partnerzy merytoryczni

comCERT

Deloitte.

IS INTEGRATED SOLUTIONS

orange

pwc

Spis treści

Konferencja ATAK I OBRONA 2013
DDoS/APT

Organizatorzy

FUNDACJA bezpieczna cyberprzestrzeń

EVENTION
CZAS ZAANGAŻOWANY

Patronat honorowy:

RCB
Rządowe Centrum Bezpieczeństwa

Ministerstwo Administracji i Cyfryzacji

BBN BIURO BEZPIECZEŃSTWA NARODOWEGO

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Warszawa, styczeń 2014 r.

Szanowni Państwo!

Przekazujemy w Państwa ręce nowy raport „Ataki i metody obrony w Internecie w Polsce". Wydajemy go przy okazji realizacji konferencji „Atak i Obrona 2013. DDoS/APT" współorganizowanej przez Fundację Bezpieczna Cyberprzestrzeń oraz spółkę Evention. Raportów dotyczących różnorodnych aspektów bezpieczeństwa ICT na rynku jest bardzo wiele. Publikują je przede wszystkim dostawcy, renomowane firmy konsultingowe, doradcze i analityczne, różne stowarzyszenia i organizacje profesjonalne. Jednak publikacji i opracowań poświęconych ściśle rynkowi w Polsce jest bardzo mało. Prawdę powiedziawszy, to prawie w ogóle ich nie ma. Dlatego jesteśmy przekonani, że nasz raport znakomicie uzupełnia tę lukę. Większość jego materiałów dotyczy naszego tu i teraz w dziedzinie cyberbezpieczeństwa AD 2013 nad Wisłą. W raporcie znajdą Państwo wypowiedzi i opinie ekspertów z Polski. Oprócz nich dostarczamy całą masę ciekawych danych pochodzących z naszego badania stanu bezpieczeństwa teleinformatycznego. Naszym celem było zbadanie, jakie środki ochrony są stosowane przez specjalistów w polskich firmach i organizacjach, jak oni je oceniają. Jesteśmy przekonani, że takie właśnie dane i informacje są najbardziej wartościowe. Pomogą Państwu krytycznie, ale i konstruktywnie spojrzeć na własny system bezpieczeństwa teleinformatycznego i wprowadzić w nim pożądane zmiany.
Zapraszamy do lektury!

MIROSŁAW MAJ

prezes zarządu
Fundacji Bezpieczna Cyberprzestrzeń

PRZEMYSŁAW GAMDZYK

prezes zarządu
Evention sp. z o.o.

Niełatwa rola CSO

Z Jackiem Skorupką, menedżerem bezpieczeństwa informacji i ciągłości działania w Citi Shared Service Center (CSC), rozmawia Przemysław Gamdzyk.

Jakie wyzwania stoją przed menedżerem bezpieczeństwa informacji we współczesnej korporacji – czyli, według obowiązującej nomenklatury, przed CISO lub CSO?

To przede wszystkim duża dynamika zmian biznesu w połączeniu z wciąż zmieniającym się obrazem zagrożeń czy regulacji. Rola i miejsce CISO nie są ani łatwe, ani wygodne. Jesteśmy między młotem a kowadłem. Z jednej strony trzeba rozumieć biznes i umieć rozmawiać z jego ludźmi, a z drugiej strony rozumieć świat IT w wystarczającym stopniu, aby móc proponować rozwiązania techniczne i poprawnie szacować ich koszt. Konieczne jest znalezienie wspólnego języka z departamentami IT, by umieć negocjować podjęcie działań w celu eliminacji ryzyka. Trzeba umieć lobbować i przedstawiać korzyści.

Samo IT nastawione jest na dostarczanie usług, rozwiązań, systemów i aplikacji. Z tego punktu widzenia bezpieczeństwo jest często mniej ważne niż sprawna obsługa biznesu i nierzadko wcale nie jest powiązane z oceną wyników IT czy biznesu. Trzeba umieć się w tym odnaleźć, tak aby nie dopuścić do marginalizacji kwestii bezpieczeństwa.

Zazwyczaj jednak znalezienie wspólnego języka z IT nie jest aż tak dużym wyzwaniem jak zrozumienie biznesu – większość menedżerów bezpieczeństwa wywodzi się przecież z IT.

Czasem droga do tej profesji jest odmienna.

To prawda, coraz częściej można spotkać osoby trafiające tutaj przez audyt, którego elementem jest audyt IT. Stąd już blisko do pozycji menedżera bezpieczeństwa. Niemniej trudniej zdobyć komuś bez doświadczenia w IT odpowiednią wiedzę techniczną i posiąść

rozumienie specyfiki IT niż odwrotnie – komuś, kto ma doświadczenie w IT, nauczyć się rozumienia biznesu.

Nie ma jednak jednej wspólnej ścieżki karier. Wydaje się, że docelowym modelem jest rozbicie kompetencji na dwa powiązane, ściśle współpracujące stanowiska – jakie stanowi biznesowy i techniczny menedżer bezpieczeństwa, jak jest w dużych dojrzałych organizacjach. Należy jednak pamiętać, że na polskim rynku jest to ciągle jeszcze nowa rola w organizacji, często jednoosobowa nawet w kilkusetosobowych i większych firmach.

Jakie kompetencje musi posiadać dobry CSO?

Sama wiedza merytoryczna nie wystarczy. Kluczową kompetencją jest odpowiednie rozumienie rodzajów ryzyka biznesowego. Dobry menedżer bezpieczeństwa IT musi wiedzieć, kiedy dane ryzyko może być zarządzane przez menedżerów biznesowych i kiedy do nich należy decyzja, a w jakiej sytuacji należy eskalować ryzyko na poziom zarządu.

Kluczowe są też zdolności miękkie; wiedza techniczna nie wystarczy, trzeba umieć negocjować z biznesem czy IT. Przede wszystkim trzeba umieć słuchać, unikając uporczywego trzymania się swoich racji. Dodatkowo, jeśli chodzi o zarządzanie komórką bezpieczeństwa, dochodzą do tego także klasyczne umiejętności zarządzania zespołem.

Czyli komórka bezpieczeństwa nie powinna być w samym IT?

Stosowane modele organizacyjne są różne. Raportowanie do IT – w rozumieniu operacji IT – uważane jest za naruszenie zasady niezależności, na drugim biegunie mamy raportowanie bezpośrednio do prezesa, departamentu prawnego, compliance bądź zarządzania ryzykiem (finansowym). Warunek niezależności jest tu spełniony, pojawia się jednak bariera w rozumieniu zagadnień bezpieczeństwa lub brak czasu decydentów. W dojrzałych organizacjach często menedżer bezpieczeństwa raportuje do CIO – przy czym nie należy mylić tej funkcji z szefem IT czy departamentu ryzyka operacyjnego.

Z pewnością zarządzanie bezpieczeństwem informacji to przede wszystkim element zarządzania ryzykiem jako takim. Kluczową umiejętnością jest zdolność do określenia, co jest istotnym ryzykiem dla biznesu. Tego konkretnego, w danej organizacji. Rodzajów ryzyka i możliwych scenariuszy zagrożeń jest bardzo wiele, ale należy wybierać te, które mogą w istotny sposób oddziaływać na kluczowe elementy biznesu w firmie.

Zdiagnozowane luki w systemie kontroli trzeba umieć przekładać na scenariusze ryzyka, by te docelowo przekładać na liczby, a więc język zrozumiały dla biznesu. Przy tym samym obrazie zagrożeń inne są kluczowe rodzaje ryzyka dla firmy budowlanej, elektrowni czy banku.

> ***„Bezpieczeństwo informacji to często zmaganie z różnymi zjawiskami natury nie tylko technicznej, ale po prostu ludzkiej – to konieczność ciągłego przekonywania innych do swoich racji”.***

Co jest najtrudniejsze?

Może to truizm, ale ważne jest, aby być wytrwałym i się nie poddawać. Bezpieczeństwo informacji to często zmaganie z różnymi zjawiskami natury nie tylko technicznej, ale po prostu ludzkiej – to konieczność ciągłego przekonywania innych do swoich racji.

Brak zrozumienia ze strony współpracowników często popycha osoby odpowiedzialne za bezpieczeństwo do zamknięcia się w swoim, odizolowanym silosie („robię to, co mi każą i tyle, tu nic się nie da zrobić, próbowałem”).

To silna pokusa ucieczki do swojej strefy komfortu, która w efekcie sprawi, że jest się izolowanym w firmie. Wszystko to razem sprawia, że nie jest to łatwa rola.

Na szczęście, coraz więcej zarządów firm rozumie wagę bezpieczeństwa informacji, szczególnie w dojrzałych organizacjach.

O co menedżer bezpieczeństwa powinien dbać, żeby się nie wypalić w swojej pracy?

Trzeba przygotować dobrą strategię bezpieczeństwa, a tak naprawdę strategiczne priorytety i cele. W wielu firmach w obszarze bezpieczeństwa nie ma formalnej strategii.

Z punktu widzenia menedżera zarządzającego bezpieczeństwem informacji kluczową sprawą jest, by mieć taki kompas, nawet jeśli nie jest on sformalizowany. Bardzo to się przydaje na dłuższą metę. Oczywiście, kwestie bezpieczeństwa muszą być zsynchronizowane ze stopniem rozwoju biznesu i kultury organizacyjnej.

Ale czy nie ma tutaj zagrożeń, że wszystko może pójść w drugą stronę, że to bezpieczeństwo zacznie rządzić i w efekcie utrudniać działania innych?

Oczywiście, trzeba mieć to na uwadze. Łatwo o przesterowanie kontroli i tak się zdarza w firmach o silnej kulturze nadzoru. Bywa też tak, że funkcje

> ***„Idealny CSO wie, że bezpieczeństwo jest ważne i potrafi przekonać do tego innych, ale zarazem rozumie, że celem firmy jest generowanie przychodu”.***

nadzorcze, takie jak bezpieczeństwo, aspekt prawny czy compliance, działają asekuracyjnie, na zasadzie: „na wszelki wypadek nie wolno”, i paraliżują firmę. Gdzieś jest jednak punkt równowagi tworzący idealnego CSO, który wie, że bezpieczeństwo jest bardzo ważne i potrafi przekonać do tego innych, ale zarazem rozumie, że celem firmy jest generowanie przychodu.

W karierze może na pewno pomóc doświadczenie z pracy w różnych rolach – a więc nie tylko jako spec od bezpieczeństwa w przedsiębiorstwie, ale również u dostawcy czy integratora rozwiązań. Dobrze też mieć networking w swojej firmie wśród tych, którzy są sprzymierzeńcami security officera. To przede wszystkim równoważne rangą stanowiska w dziale audytu, zarządzania ryzykiem, compliance. Trzeba umieć zbudować sieć sojuszników w korporacji.

** CSC to inicjatywa stworzenia sieci centrów serwisowych świadczących wysokiej jakości usługi innym podmiotom z grupy Citi. W Polsce zajmujemy się m.in.: monitorowaniem przeciwdziałania praniu pieniędzy; obsługą operacji bankowych, papierów wartościowych i funduszy inwestycyjnych; rozliczaniem należności i płatności, technologicznymi funkcjami kontrolnymi oraz obsługą infrastruktury teleinformatycznej. CSC posiada kilka lokalizacji w Polsce – największe to Warszawa i Olsztyn. Obecnie w CSC pracuje ok. 2300 osób.*

Nowe zagrożenia, nowe potrzeby

Skala zagrożeń oraz ich potencjalny wpływ na działalność biznesową wymagają zmiany dotychczasowego spojrzenia na to, co stanowić powinno bezpieczną infrastrukturę IT.

Piotr Waszczuk

„Obserwując skalę oraz tempo zmian cyberzagrożeń, można założyć, że każda organizacja została lub zostanie zaatakowana" – czytamy we wstępie wydanego w kwietniu 2013 roku raportu *„Cyberodporność w świecie ewoluujących zagrożeń. Nowe drogi w bezpieczeństwie informacji"*.

Publikacja Deloitte nie pozostawia złudzeń. Ataki cyberprzestępców są prowadzone w sposób profesjonalny, precyzyjny i ukierunkowany na osiągnięcie konkretnych celów. Duże znaczenie dla wzrostu skali zagrożeń ma fakt, że obecnie rola informatyki w biznesie jest większa niż kiedykolwiek wcześniej. Rozwiązania informatyczne zyskują coraz większą samodzielność działania i często są w stanie w sposób autonomiczny wymieniać informacje za pomocą różnych kanałów. Świat połączonych organizacji biznesowych, urządzeń i technologii wymaga diametralnej zmiany podejścia do bezpieczeństwa IT tym bardziej, im bardziej cenne są informacje przechowywane w firmowych systemach i im bardziej unikalna jest wiedza danej organizacji.

Eksperci podkreślają, że w ciągu ostatnich dwóch czy trzech lat radykalnie zmieniła się struktura zagrożeń IT. *„Najczęściej spotykane ataki możemy podzielić na trzy grupy. Pierwsza z nich to zwykły wandalizm, druga – proste ataki nastawione na kradzież tożsamości lub informacji finansowych. Trzecią grupę stanowią wyspecjalizowane, ukierunkowane i dobrze zaplanowane ataki wymierzone w firmy"* – mówi Maciej Iwanicki, inżynier systemowy firmy Symantec.

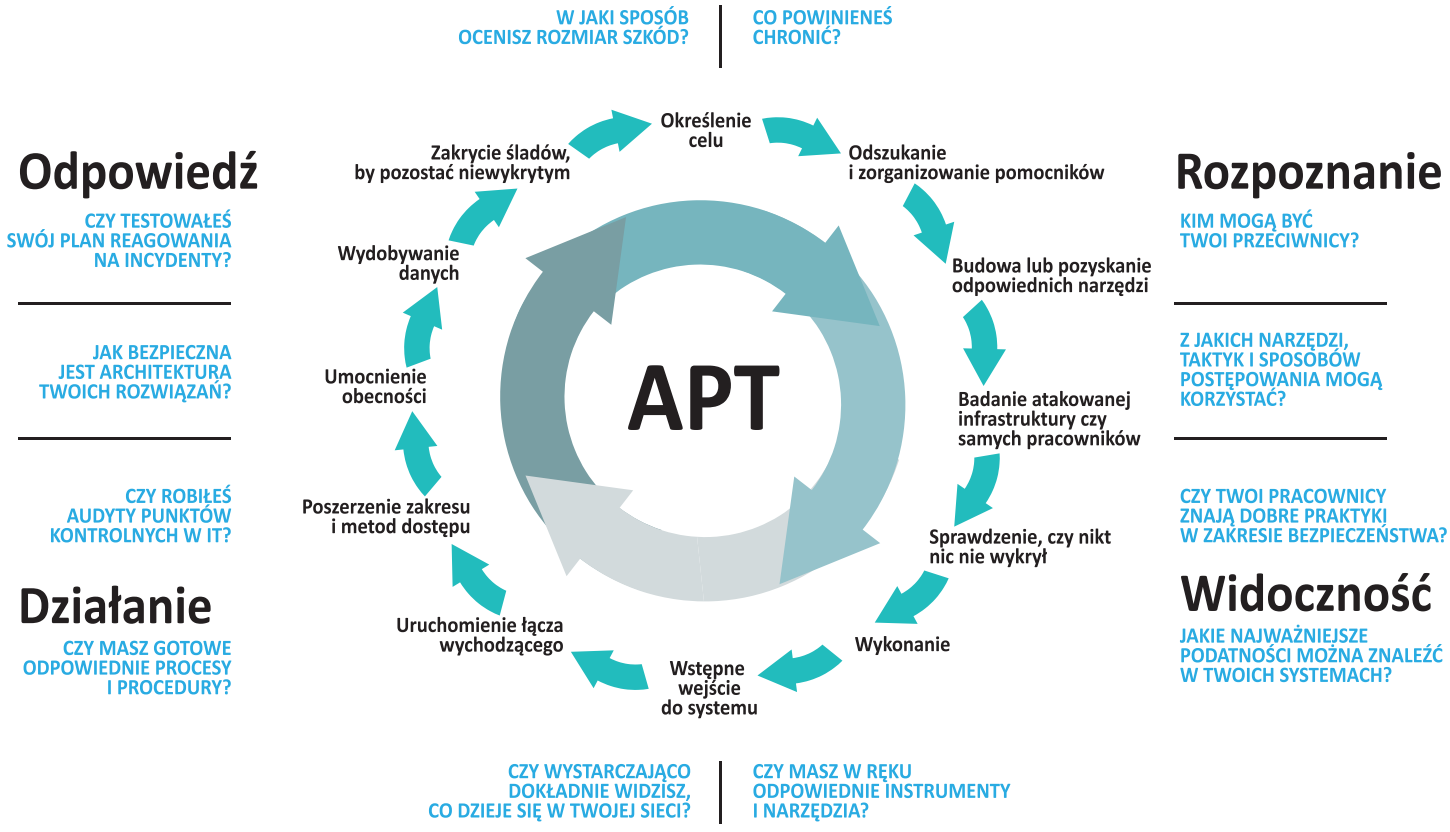
Zmienia się też charakter zagrożeń. Jeszcze kilka lat temu większość ataków wykorzystywała niższe warstwy sieci – głównie warstwę transportową. Dziś przestępcy stosują nowoczesne techniki maskowania szkodliwych aplikacji, przez co typowe systemy antywirusowe nie są w stanie ich wykryć, a klasyczne zapory zablokować. Nie brakuje też ataków wykorzystujących socjotechnikę. Jednak co najważniejsze, znacznie wzrasta liczba zagrożeń opartych na warstwie aplikacji. Niestety, w wielu organizacjach brakuje wiedzy

na temat nowych zagrożeń oraz narzędzi pozwalających je wykrywać, a co dopiero skutecznie przed nimi się bronić. To z kolei powoduje, że wielu przedsiębiorców mylnie sądzi, że najpilniej strzeżone informacje o ich firmach są bezpieczne. *„Mamy na rynku kilkaset dużych i setki tysięcy mniejszych firm, które co chwilę padają ofiarami różnych incydentów. W dodatku dzieje się tak niezależnie od wielomilionowych inwestycji w zabezpieczenia”* – twierdzi Tomasz Gładkowski, prezes firmy Eversys.

Antywirus nie wystarczy

Zapytani o najbardziej niebezpieczne spośród nasilających się ataków eksperci zgodnie powtarzają skrót „APT”. Chodzi o bardzo punktowe, długofalowe i nastawione na konkretne cele ataki określane mianem „Advanced Persistent Threat”. Kompleksowe i rozłożone w czasie ataki wykorzystują m.in. specjalnie tworzone aplikacje typu malware w celu zdobycia podstawowej kontroli nad wybranym – często przypadkowo – nieodpowiednio zabezpieczonym komputerem włączonym do firmowej sieci.

> ***„Atakujący dzisiaj robią wszystko, żeby przejąć kontrolę nad konkretnymi maszynami i jak najdłużej pozostać niezauważonym”.***
>
> ***Tomasz Gładkowski,*** *prezes Eversys*



„Obserwujemy odwrót od klasycznego, ilościowego podejścia do zarażania komputerów. W większym stopniu liczy się wartość poszczególnych maszyn i zapisanych w ich pamięci informacji” – podkreśla Aleksander Łapiński, Sales Engineer w Trend Micro. Kolejne kroki typowego ataku APT zakładają utrzymanie posiadanego dostępu do jednej maszyny i stopniowe rozszerzanie go na inne maszyny, systematyczną analizę sieci zmierzającą do zlokalizowania cennych informacji, wreszcie kradzież danych. O jakie informacje może chodzić? Dane o klientach, historiach transakcji, informacje finansowe, plany biznesowe oraz projekty nowych produktów to informacje najcenniejsze z perspektywy cyberprzestępców, a także potencjalnych nabywców. Co ciekawe, priorytetem przestępców pozostaje zwykle zachowanie niewykrywalności ataku. *„Do niedawna atakujący tworzyli kawałek złośliwego kodu po to, żeby zdestabilizować jakiś element infrastruktury. Dziś robią wszystko, żeby przejąć kontrolę nad konkretnymi maszynami i jak najdłużej pozostać niezauważonym”* – mówi Tomasz Gładkowski.

Z analiz firmy Deloitte wynika, że aż osiem na dziesięć przestępstw informatycznych jest przeprowadzanych przez wyspecjalizowane, zorganizowane grupy cyberprzestępców bądź przy ich współudziale. Atakując konkretne firmy czy wręcz komputery, hakerzy starają się uzyskać dostęp do najcenniejszych informacji biznesowych. Nawet jedna maszyna może stać się przyczółkiem do prowadzenia bardziej zaawansowanych ataków wymierzonych w konkretne osoby lub informacje. Zagrożone są więc praktycznie wszystkie elementy sieci firmowej. Zresztą nie tylko one. Działania cyberprzestępców są też często wymierzone w zupełnie nowe kategorie urządzeń.

> ***„Obserwujemy odwrót od klasycznego, ilościowego podejścia do zarażania komputerów. W większym stopniu liczy się wartość poszczególnych maszyn i zapisanych w ich pamięci informacji".***
>
> ***Aleksander Łapiński,*** *Sales Engineer w Trend Micro*

„Niedawno pojawił się nowy robak zarażający terminale płatnicze i wykradający informacje dotyczące autoryzacji płatności. Ochrona, która do tej pory była zorientowana na stacje robocze i urządzenia przenośne, w tej chwili powinna sięgać urządzeń POS, bankomatów, systemów SCADA czy sterowania budynkami” – dodaje Michał Ceklarz, dyrektor regionalny firmy Sourcefire w regionie Europy Wschodniej. Typowe systemy antywirusowe, choć potrzebne, są w stanie ochronić firmę tylko przed niewielką częścią zagrożeń. Wprowadzenia skutecznej ochrony nie ułatwia rosnący stopień skomplikowania środowiska IT. Postępująca integracja z innymi organizacjami, popularyzacja aplikacji dostępnych w chmurze czy rosnąca rola urządzeń przenośnych to tylko niektóre z przyczyn wzrostu złożoności środowisk IT.

Ochrona szyta na miarę zagrożeń

Do niedawna systemy bezpieczeństwa w większości przedsiębiorstw koncentrowały się wokół ochrony przed tradycyjnymi zagrożeniami. I słusznie. *„Pamiętajmy, że firmy – także te największe – na co dzień muszą zmagać się też z takimi samymi problemami, z jakimi walczą zwykli użytkownicy”* – mówi Maciej Iwanicki. Proste ataki negatywnie odbijają się na produktywności i mogą doprowadzić do utraty danych. Są też potencjalnym początkiem serii działań niemożliwych do wykrycia bez odpowiednich narzędzi. Wówczas jednak zwykle mamy do czynienia z unikalnym oprogramowaniem. *„Ataki ukierunkowane opierają się na oprogramowaniu, które z założenia jest niewykrywalne dla typowych systemów bezpieczeństwa. Potrzebne są dodatkowe warstwy ochronne i rozwiązania będące w stanie analizować działanie całej infrastruktury czy weryfikować zachowanie poszczególnych aplikacji i uczyć się zachowań szkodliwych aplikacji”* – podkreśla Aleksander Łapiński.

Nierzadko po wdrożeniu systemów analizujących działanie całego środowiska informatycznego okazuje się, że inwigilacja sieci już nastąpiła.

„Odpowiedź na takie zagrożenia wymaga zwiększenia bezpieczeństwa kosztem operatywności. Nowym zagrożeniom nie da się sprostać bez zmiany dotychczasowych nawyków czy ograniczenia niektórych uprawnień” – twierdzi Maciej Iwanicki. W wielu firmach potrzebne są narzędzia wspierające kontrolę ruchu internetowego – serwisy internetowe coraz częściej stają się bowiem źródłem infekcji omijających tradycyjne metody ochrony.

Ochronę przed rozproszonymi i precyzyjnie ukierunkowanymi działaniami przestępców zapewniać mają tzw. rozwiązania bezpieczeństwa nowej generacji. *„Założenie jest takie, że powinny one stanowić kolejną warstwę i zapewniać dodatkowe funkcjonalności usprawniające działanie posiadanych wcześniej zabezpieczeń”* – mówi Michał Ceklarz. Przykładem działania tego typu systemów jest weryfikacja pakietów danych, które przepuści zapora firewall, bądź kontrola bezpieczeństwa na poziomie aplikacji. Nowoczesne rozwiązania pozwalają również rozszerzyć ochronę na zwirtualizowane środowiska aplikacyjne czy usługi dostępne w modelu chmurowym.

Nie tylko cena

Do tej pory większość przedsiębiorców nie była przygotowana do radzenia sobie ze skrupulatnie zaplanowanymi, złożonymi i rozproszonymi w czasie atakami. Skala zagrożeń jest trudna do oszacowania. W wielu firmach brakuje narzędzi pozwalających analizować przepływ danych i powiązać te informacje z wykrywanymi incydentami. Duża część naruszeń bezpieczeństwa pozostaje również niewykrywalna.

„Podczas audytów bezpieczeństwa, które prowadziliśmy w polskich organizacjach, trafialiśmy na przypadki, w których z dużym prawdopodobieństwem mogliśmy stwierdzić, że ponad 50% komputerów tworzyło aktywny botnet” – twierdzi Tomasz Gładkowski. Szczęśliwie potrzebę posiadania kompleksowych systemów bezpieczeństwa dostrzegają już nie tylko podmioty z branży finansowej i telekomunikacyjnej. W ślad za tym idzie też wzrost rangi osób odpowiedzialnych za bezpieczeństwo IT w firmach. Niestety, w procesach zakupowych nadal kluczową rolę odgrywa cena. *„Firmy zachodnie zdają sobie sprawę z tego, że różnica w cenie niesie ze sobą różnicę w funkcjonalności. Natomiast w Polsce głównym kryterium wyboru często pozostaje cena, co bardzo utrudnia wybór najlepszych rozwiązań, które niekoniecznie są najtańsze”* – mówi Michał Ceklarz. Wybór najlepszego rozwiązania nierzadko utrudnia również brak wiedzy na temat potrzebnych funkcjonalności.

> ***„Ochrona, która do tej pory była zorientowana na stacje robocze i urządzenia przenośne, w tej chwili powinna sięgać urządzeń POS, bankomatów, systemów SCADA czy sterowania budynkami”.***
>
> ***Michał Ceklarz**, dyrektor regionalny Sourcefire*

Odpowiedzią na potrzebę racjonalizacji kosztów często okazuje się konsolidacja posiadanych systemów bezpieczeństwa IT i zmniejszenie liczby dostawców. Jednocześnie do najbardziej zaawansowanych systemów bezpieczeństwa zaliczane są dziś narzędzia typu SIEM. Integrując różne wykorzystywane w firmie zabezpieczenia, pozwalają one łatwo analizować i korelować dane o – istotnych z perspektywy bezpieczeństwa informacji – zdarzeniach zachodzących w całej organizacji. Takie informacje pomagają odszukać źródła wykrytych infekcji oraz skalę związanych z nimi zagrożeń. Stanowią też nieocenione wsparcie na etapie planowania kolejnych inwestycji z zakresu bezpieczeństwa.

„Proces rozwoju infrastruktury to proces ciągły, zmierzający do nieustannego podnoszenia poziomu bezpieczeństwa. Nie chodzi tu jednak o wymianę istniejących, tradycyjnych rozwiązań, tylko o dostrzeganie potrzeby posiadania dodatkowych mechanizmów bezpieczeństwa adresujących najnowsze zagrożenia, co w efekcie pozwala skutecznie uszczelnić całe środowisko IT” – kwituje Tomasz Gładkowski.

Czy Polska jest źródłem cyberataków?

W statystykach i raportach bezpieczeństwa Polska pojawia się rzadko. Są to krótkookresowe skoki do TOP-10. Warto jednak zająć się w Polsce likwidacją serwerów rozsyłających spam i hostujących phishing.

Mirosław Maj

Przegląd kilkudziesięciu zagranicznych raportów, opublikowanych przez 13 firm[1] i organizacji zajmujących się bezpieczeństwem teleinformatycznym, na temat stanu bezpieczeństwa w internecie pokazuje, że Polska nie jest szczególnym poligonem aktywności cyberprzestępców w porównaniu z innymi krajami. To stwierdzenie przede wszystkim odnosi się do statystyk wskazujących źródła cyberataków. Trochę częściej pojawiamy się jako cel tych ataków. Mimo postrzegania „polskiego internetu" jako obszaru o raczej średnim poziomie ryzyka w skali światowej, można wskazać szczególne obszary działalności cyberprzestępczej, w których pojawiamy się wyżej w niechlubnych statystykach. Takim obszarem jest na przykład rozsyłanie spamu.

Skąd na świecie pochodzi najwięcej cyberataków?

Jeśli spojrzeć na raporty najbardziej rozpoznawanych światowych firm zajmujących się monitorowaniem bezpieczeństwa, wśród których dominują globalni liderzy rynku produktów antywirusowych, jest kilka krajów kandydujących do tytułu źródła internetowego zła. Są to: Stany Zjednoczone, Indie, Rosja, Chiny, Wielka Brytania, Niemcy, Holandia i Korea Południowa. Każdy z tych krajów znajduje się w co najmniej co piątym zestawieniu TOP-3 dla najczęstszych źródeł zagrożeń w internecie, takich jak: rozsyłanie spamu, zlokalizowanie stron phishingowych oraz występowanie stron, które infekują.

Obecność w co piątym zestawieniu to wynik minimum dla wspomnianych krajów, natomiast niekwestionowanym liderem są tu Stany Zjednoczone, które pojawiają się w 9 na 10 zestawień. Na nowego „potentata" wyrastają Indie, które są prawie w co drugim zestawieniu. W przypadku Chin i Rosji jest to wynik na poziomie obecności w co trzecim zestawieniu TOP-3.

Warto przy podawaniu danych zwrócić uwagę na istotne problemy związane z ustalaniem źródła ataku. Fakt, że w zestawieniach pojawiają się poszczególne kraje, świadczy o tym, że ataki są przeprowadzane z komputerów podłączonych do operatorów telekomunikacyjnych w danych krajach. W znacznie mniejszym stopniu świadczy to o tym, że za atakami stoją obywatele danych krajów lub choćby ich mieszkańcy. Bardziej prawdopodobną interpretacją jest to, że obywatele tych krajów, a więc właściciele komputerów, z których ataki są przeprowadzane, niewiele dbają o bezpieczeństwo swoich komputerów, co prowadzi do ich przejęcia przez cyberprzestępców i wykorzystania w atakach. Warto też pamiętać o efekcie skali. Im więcej w danym miejscu

komputerów, tym więcej źródeł ataków – to naturalna korelacja (potwierdzona tym, że listę najczęstszych źródeł ataku otwierają Stany Zjednoczone, Indie, Rosja i Chiny).

Kiedy w 2011 r. dokonano dokładnej analizy ataków DDoS na Koreę Południową i Stany Zjednoczone, okazało się, że istotne elementy infrastruktury atakującej znalazły się w Wielkiej Brytanii i Stanach Zjednoczonych, chociaż powszechnie uznano, że za atakami stoją specjaliści z Korei Północnej.

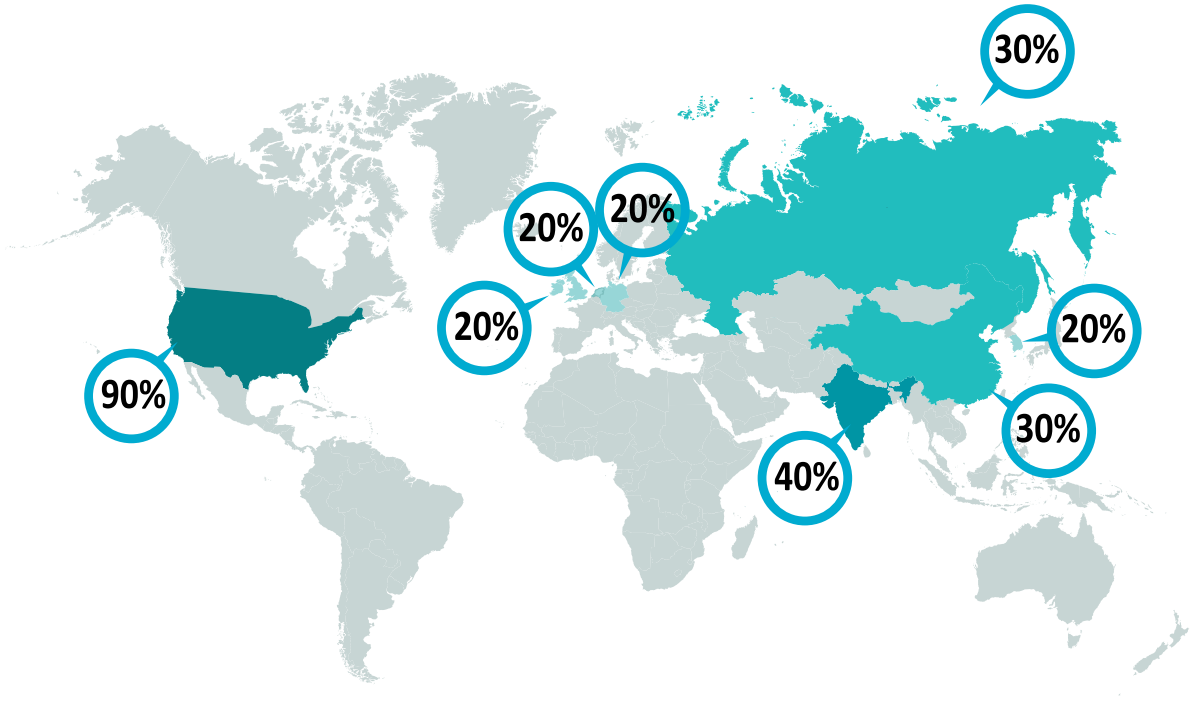
Jak na tym tle wygląda Polska?

W statystykach i raportach bezpieczeństwa nasz kraj pojawia się rzadko. Są to krótkookresowe skoki do TOP-10, a czasami nawet wyżej, choć zazwyczaj na krótko, co widać w trendach długofalowych. Tak jest na przykład w raportach firmy Symantec[2], w których Polska znajduje się w TOP-10 źródeł spamu (w styczniu br.) i źródeł phishingu (w czerwcu).

Ważniejsze są jednak podsumowania roczne albo przynajmniej półroczne. W trzech różnych raportach Polska pojawia w czołowej dziesiątce źródeł zagrożeń. W trzech różnych raportach, ale tylko w dwóch kategoriach: źródło rozsyłania spamu i miejsce instalowania stron z phishingiem.

W raporcie „2012 Cisco Annual Security Report”[3] jesteśmy na dziesiątym miejscu w klasyfikacji krajów, z których wysyłany jest spam, przy okazji na drugim wśród krajów europejskich (po Rosji). Według tego raportu 2,72% światowego spamu jest rozsyłane z Polski. W tej kategorii firma Sophos w swoim raporcie[4] też nas umiejscawia na X miejscu, praktycznie z tym samym wynikiem – 2,8%. Warto zauważyć, że metodyka monitoringu spamu jest chyba jedną z najbardziej dojrzałych, gdyż wyniki poszczególnych ośrodków monitorujących są zbliżone, co nie zawsze jest prawidłowością w innych kategoriach.
Przy okazji rozważań o spamie warto przypomnieć, że polscy operatorzy (a tak naprawdę przede wszystkim Telekomunikacja Polska) w przeszłości bardzo często przewodzili tym listom. Dopiero zmiana portu obsługi poczty elektronicznej, jaką TP wprowadziła 1 stycznia 2009 r., i w konsekwencji zablokowanie masy spamu przechodzącej przez polski internet przyniosła

MAPA NAJCZĘŚCIEJ WYSTĘPUJĄCE KRAJE W ZESTAWIENIACH TOP-3 ŹRÓDEŁ ATAKÓW. PROCENTOWY UDZIAŁ WYSTĘPOWANIA W ZESTAWIENIACH.



OK. 10. MIEJSCE W RANKINGACH

2,8% wg SOPHOS | **2,72%** wg CISCO

LETHIC ODPOWIEDZIALNY ZA ROZSYŁANIE PRAWIE POŁOWY SPAMU

24h

9 MLD E-MAILI ZE SPAMEM, W TM 450 MLN E-MAILI Z POLSKI DZIENNIE

BOTNET LETHIC NR 1 JAKO BOTNETOWE ŹRÓDŁO SPAMU W 2012

znaczącą poprawę statystyk w tej kategorii. To przykład, że odważne posunięcia w dziedzinie bezpieczeństwa są opłacalne.

Drugą sygnalizowaną kategorią, w której się pojawiamy jako źródło, jest phishing. Zdaniem autorów raportu firmy Symantec „Intelligence Security Threat Report – Appendix 2013”[5] Polska jest na 10 miejscu wśród krajów, w których umiejscowione są serwery goszczące strony phishingowe. Mniej więcej co 60. strona z phishingiem znajduje się na polskim serwerze. Co ciekawe, to dokładnie ten sam poziom, jaki mieliśmy w 2011 r. Wtedy dawało to nam 12 pozycję. Jak widać, rynek serwerów z phishingiem się w pewnym stopniu konsoliduje, ograniczając się do mniejszej grupy krajów, do których, niestety, dołączyła Polska. Choć należy zauważyć, że akurat w tej dziedzinie dominacja Stanów Zjednoczonych jest niekwestionowana. Co druga strona z phsihingiem znajduje się na serwerze amerykańskim. I właściwie to tyle, jeśli chodzi o wskazywanie Polski palcem na arenie międzynarodowej jako źródła problemu. Wydaje się, że niewiele, ale aby odnieść się do tego stwierdzenia, należałoby przeprowadzić głębsze badania uwzględniające kilka innych czynników waloryzujących to wrażenie. Na przykład odniesienie do „możliwości” technologicznych poszczególnych krajów. Od pewnego czasu wiadomo, że cyberprzestępcy do lokalizacji swojej „broni” wybierają miejsca, które w sieci mają dobrą charakterystykę dostępności, gdzie jest dużo łączy szerokopasmowych o dużej przepustowości, a serwery obdarzone są dużą mocą.

Niektóre z krajów naszego regionu wyprzedzają nas w klasyfikacji na najszybsze średnie łącze internetowe. Wśród nich są: Czechy, Rumunia, Węgry i Słowacja (wg raportu Akamai „The State of the Internet. 1st Quarter, 2013 Report”[6]). Mimo to żadne z nich nie pojawia się częściej niż Polska w tych niechlubnych statystykach. Z drugiej strony każde z tych państw przewyższamy, jeśli chodzi o liczbę bezwzględną dołączeń do internetu, co wynika chociażby z przewagi populacji krajów. Taka przewaga automatycznie powoduje większe prawdopodobieństwo wystąpienia w ww. statystykach, choć Ukraina też od nas nie pojawia się częściej. I tak można mnożyć uzależnienia i wątpliwości. Niemniej podstawowe problemy widać bez szczególnego uzbrajania oka. Warto się zająć w Polsce likwidacją serwerów służących przestępcom do rozsyłania spamu i umieszczania stron z phishingiem.

A jak nas widzą w szczegółach?

Tak zwany wirus „policja" jest w Polsce dość znany, niestety, głównie poprzez liczbę infekcji i problemów, jakie przyniósł indywidualnym użytkownikom internetu. Ten nasz problem zauważyli również inni. W raporcie firmy F-Secure[7] o zagrożeniach w internecie w pierwszej połowie 2013 r. Polska jest podana jako jeden z krajów, jakich dotyczy problem wirusa „policja", który jest jednym z przypadków tzw. „ransomware" – złośliwego kodu wyłudzającego okup. F-Secure wskazywał nasz kraj również jako jeden z charakterystycznych przykładów haktywizmu politycznego. Tym przykładem były ataki DDoS na polskie serwery rządowe oraz podmiana stron premiera RP, co działo się przy okazji protestów ze stycznia 2012 r. związanych z próbą wprowadzenia ACTA. Natomiast w raporcie za II połowę 2012 r.[8] autorzy zwrócili uwagę, że Polska stała się jednym z krajów poważnie zagrożonych działaniem wirusa Zeus po tym, jak przestępcy dołączyli do kodu wirusa 15 polskich serwisów.

Z kolei Symantec zwrócił na Polskę uwagę przy innej okazji[9]. Firma przeanalizowała, które z botnetów w 2012 r. były w największym stopniu odpowiedzialne za spam. Wśród nich na pierwszym miejscu był botnet Lethic. To jeden z najstarszych botnetów, które systematycznie rozsyłają spam. Mimo że w lipcu 2012 r. odnotowano wyraźny spadek aktywności tego botnetu[10], to i tak jego pozycja nr 1 jako botnetowego źródła spamu w 2012 r. była niekwestionowana. Lethic był odpowiedzialny za prawie co drugi e-mail ze spamem (43,4%). Średnio codziennie rozsyłał ponad 9 mld e-maili. Co to ma wspólnego z Polską? Otóż nasz kraj jest na trzecim miejscu, jeśli chodzi o liczbę komputerów należących do tego botnetu. Co 20 z nich znajduje się właśnie w Polsce.

Jeśli dystrybucja spamu jest rozłożona mniej więcej równomiernie, to można zaryzykować stwierdzenie, że polskie komputery rozsyłają dziennie prawie 0,5 mld e-maili ze spamem – tylko z tego jednego botnetu! Trochę wyjaśnia nam się wysoka pozycja Polski w rankingach dotyczących spamu.

Tak jak wspomniałem wcześniej, bycie źródłem ataku jest w dużym stopniu skorelowane z podatnością na ataki na własny komputer. Dlatego podsumowując ilościowe i jakościowe rozważania dotyczące Polski jako obszaru działalności cyberprzestępczej, trzeba się zgodzić z klasyfikacją, jaką nam przypisała firma Kaspersky Lab.

W swoim raporcie[11] z 2012 r. specjaliści z Kaspersky Lab umieścili nas w grupie średniego ryzyka. To ryzyko określili jako prawdopodobieństwo infekcji w sieci, wartościując ten przedział pomiędzy mniej więcej 20% a 40%. Wygląda na to, że są tego wyraźne skutki i jest się czym zająć. W sieciach polskich operatorów znajdują się miliony komputerów, które „zmieniły swojego właściciela". Nowy właściciel to cyberprzestępca aktywnie wykorzystujący cudze zasoby do prowadzenia działalności niezgodnej z prawem. Zwalczanie tego zjawiska nie jest łatwe. Jest przede wszystkim kosztowne, dlatego trudno przekonać operatorów telekomunikacyjnych. Istotne także, by ofiary tej przestępczej aktywności, zarówno te na końcu łańcucha ataku, jak i te pośrodku, które biernie uczestniczą w procederze, były świadome, co się naprawdę dzieje.

---

1 *Akamai, Arbor, Cisco Systems, Deloitte, Eset, F-Secure, Kaspersky Lab, Lloyds, Neustar, Prolexic, Sophos, Symantec, Trend Micro.*
2 *http://www.symantec.com/security_response/publications/monthlythreatreport.jsp*
3 *https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2013_ASR.pdf*
4 *http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2013.pdf*
5 *http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf*
6 *http://www.akamai.com/dl/documents/akamai_soti_q213.pdf?WT.mc_id=soti_Q213*
7 *http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf*
8 *http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H2_2012.pdf*
9 *http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf*
10 *http://blog.spiderlabs.com/2012/07/spam-down-where-is-lethic.html*
11 *http://www.securelist.com/en/analysis/204792255/*

Włamania nie unikniesz

Z Rikiem Fergusonem, wiceprezesem ds. badań nad bezpieczeństwem w firmie Trend Micro, rozmawia Mirosław Maj.

Czy APT to realne zagrożenie, czy też jedynie marketingowy slogan?

Zjawisko ukierunkowanych ataków jest bez wątpienia realnym zagrożeniem. Ofiary są wybierane z różnych powodów: ze względu na posiadaną własność intelektualną, informacje osobowe lub też po prostu jako część lub etap ataku na inną organizację. Z samego faktu, że ofiary są wybierane, wynika możliwość znacznie bardziej precyzyjnego dopasowania ataku do wybranej ofiary, przez co znacznie trudniej go wykryć i odeprzeć.

Statystyki ataków typu APT wydają się zdumiewające. Z jednej strony mówimy o incydentach, które nie są ujawniane. Z drugiej spotykamy się z informacjami, że – dla przykładu – 75% takich ataków zakończyło się sukcesem. Skąd biorą się tego rodzaju statystyki, jeśli ataki nie są ujawniane?

Tego rodzaju statystyki są efektem analiz prowadzonych przez zespoły informatyki śledczej. Stąd biorą się statystyki dotyczące odsetka skutecznie przeprowadzonych ataków. Gromadzimy informacje, badając ukierunkowane ataki na inne organizacje. Badając sprawy, którymi się zajmujemy, uzyskujemy również dostęp do informacji na temat innych podobnych ataków, co składa się na tego rodzaju statystyki. Trzeba jednak stwierdzić, że w przypadku cyberprzestępczości statystyki są często wzięte z sufitu. Ktoś poślinił palec, podniósł na wiatr i zawyrokował, że 75% będzie właściwą liczbą. Te szacunki to często po prostu zgadywanie. Możemy mówić o dowodach empirycznych, o dowodach pochodzących z ataków, które analizowaliśmy, ale należy ostrożnie podchodzić do wszelkiego rodzaju zbiorczych statystyk.

Od czasu słynnego ataku na RSA, kiedy to ukuto termin APT, zgromadziliśmy jako branża wiele doświadczeń, ale czy opracowaliśmy już spójne, strategiczne rozwiązanie? Jak walczyć z tym problemem?

Kilka rzeczy musimy zacząć robić inaczej. Potrzebujemy fundamentalnej zmiany technologicznej po stronie dostawców systemów bezpieczeństwa. Osoby prywatne i przedsiębiorstwa muszą zacząć zupełnie inaczej budować swoje bezpieczeństwo.

W przeszłości opieraliśmy się na założeniu, że nikogo nie wpuścimy do środka. Wznosiliśmy wysokie mury, kopaliśmy fosy i stawialiśmy strażników wypatrujących nieprzyjaciela. Zakładaliśmy, że uniemożliwimy mu przedostanie się do wnętrza organizacji. Tymczasem musimy przyjąć do wiadomości, że włamania będą się zdarzać.

Przestępcom uda się przekroczyć bramy naszej organizacji. Jeśli haker zechce dostać się do systemów firmy, to się do nich dostanie. Musimy tak zmienić swoją architekturę, procesy i technologie, by jak najszybciej dowiedzieć się o włamaniu i móc przedsięwziąć odpowiednie środki, zamknąć dostęp do systemów i przeanalizować odwrót włamywacza.

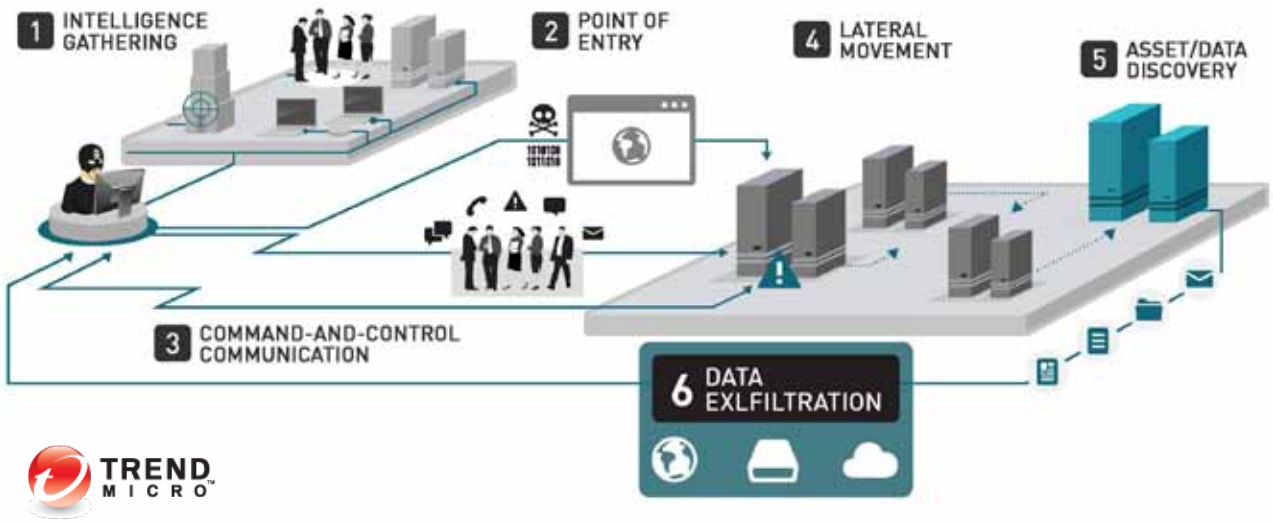
A co ze strategią kill chain? To pojęcie wywodzące się z wojskowości. Czy jest użyteczne w cyberprzestrzeni?

Tak. Tego rodzaju podejście przyjął Lockheed Martin w analizie włamań komputerowych. Lockheed Martin wywodzi się z sektora obrony i przyjęcie strategii kill chain w cyberprzestrzeni było dla nich naturalnym posunięciem. Ta metodologia świetnie się tu sprawdza.

> ***„Im głębiej analizujemy zdarzenia związane z naruszeniami bezpieczeństwa, tym więcej uczymy się od autorów ataku. Atak staje się kluczem do obrony”.***

Zanim kula utkwi w piersi przeciwnika, zachodzi cały łańcuch poprzedzających to wydarzenie zdarzeń. Łańcuch ten określany jest jako kill chain i prowadzi od wyprodukowania kuli w fabryce do ostatecznej eliminacji wroga. Analogicznie, skuteczna kradzież danych należących do przedsiębiorstwa poprzedzona jest całym

SCHEMAT BUDOWA ATAKU



Budowa ataku. Grafika z prezentacji ***Rika Fergusona,*** *Trend Micro*

łańcuchem zdarzeń: od początkowej fazy rozpoznania, która ma na celu rozgryzienie ofiary, przez włamanie, dwustronny przepływ danych w sieci komputerowej, wykorzystanie podatności, po zainfekowaniu systemu i przejęcie nad nim kontroli.

Możemy przeanalizować każde z tych zdarzeń, zdobyć wiedzę i wykorzystać ją, by przerwać ten łańcuch tak wcześnie, jak jest to możliwe. Im głębiej analizujemy te zdarzenia, tym więcej uczymy się od autorów ataku. Atak staje się kluczem do obrony.

Jeśli chcemy zbudować skuteczną obronę przed APT, powinniśmy się skoncentrować na procesach czy technikach?

Potrzebujemy wiedzy, która pozwoli nam działać. Potrzebujemy szerokiego spojrzenia na bezpieczeństwo organizacji. W przeszłości bywało ono bardzo wąskie. Skupialiśmy się na oddzielnych produktach i technologiach, zarządzając nimi niezależnie. Mieliśmy pięć różnych firewalli, system przeciwdziałania włamaniom, system antywirusowy, system zarządzania dostępem. Skłonni byliśmy traktować każdą z tych rzeczy oddzielnie. W ten sposób rezygnujemy z informacji kontekstowej, a ta okazuje się najważniejsza, gdy staramy się przeanalizować mechanizmy ukierunkowanego ataku.

Kontekst jest dziś kluczem do zapewnienia ochrony przed ukierunkowanymi atakami. Musimy być w stanie czerpać informacje z wielu różnych źródeł. Chodzi także o informacje o zdarzeniach, które niezależnie od siebie wydają się nie budzić niepokoju, ale jeśli spojrzymy na nie łącznie, nagle okażą się groźną anomalią wymagającą podjęcia odpowiednich działań. To najważniejsza w tej chwili kwestia. Z punktu widzenia biznesu najważniejsze jest cofnięcie się o kilka kroków, porzucenie dotychczasowych metod i objęcie szerokim spojrzeniem wszystkiego, co dzieje się w firmowej sieci, a nie koncentrowanie się na wybranych zagadnieniach.

Mam wrażenie, że to powtórzenie reguł, którymi kierujemy się od lat. Wiemy, że musimy zarządzać bezpieczeństwem jako całością.

Czy doświadczenie zgromadzone podczas analizy ataków APT podpowiada nam jakieś nowe rozwiązania?

Dostępne są wysokopoziomowe narzędzia, które pozwalają uzyskać spojrzenie w skali makro, o którym wcześniej mówiłem. Jakość narzędzi zależy jednak wprost od jakości informacji, które do nich spływają.

Za ich pomocą szukamy tradycyjnego złośliwego oprogramowania i sygnatur, ale też sprawdzamy, czy na przykład system regularnie łączy się z adresem IP, który wydaje się podejrzany. Nawet jeśli oprogramowanie antywirusowe twierdzi, że nic się nie dzieje, to jeśli adres IP znajduje się w Hongkongu, może jednak należałoby zbadać tę sprawę. Przyglądamy się też zrachowaniom użytkowników. Wielokrotne nieudane logowanie do bazy danych może być sygnałem ostrzegawczym, podobnie jak podejrzane transfery dużej ilości danych.

> ***„Kontekst jest dziś kluczem do zapewnienia ochrony przed ukierunkowanymi atakami. Musimy czerpać informacje z wielu różnych źródeł”.***

APT czasem rozpoczyna się niewielkim włamaniem, po którym następuje legalne, jak mogłoby się wydawać, wykorzystanie danych uprawniających do użytkowania określonych zasobów, a które jest w rzeczywistości wstępem do włamania do kolejnych systemów i kradzieży danych. Szukamy więc nie tylko tradycyjnych znaczników złośliwego oprogramowania, ale też nietypowych zachowań w sieci.

Potrzebujemy narzędzi zdolnych zgromadzić wszystkie te informacje i samodzielnie – do pewnego stopnia – nadać im znaczenie, a następnie przekazać je wyżej, by można było przeanalizować je w szerszym kontekście.

DDoS nasz powszedni

W jaki sposób operatorzy starają się przeciwdziałać atakom Distributed Denial of Service.

Andrzej Maciejewski

Z atakami Distributed Denial of Service (DDoS) powinni liczyć się użytkownicy, którzy przenieśli do sieci znaczną część działalności biznesowej. Celem atakujących stały się bankowe serwisy transakcyjne, serwisy aukcyjne, sklepy internetowe, a także witryny administracji publicznej udostępniające usługi dla ludności. Skutki biznesowe, finansowe i wizerunkowe stają się coraz bardziej widoczne, a straty dotkliwe i przekładające się na realne kwoty. Rośnie prawdopodobieństwo i profesjonalizacja ataków, dlatego firmy i instytucje zaczęły poszukiwać sposobów, jak im zapobiegać i ograniczać ich skutki. Jednym z elementów obrony może być usługa świadczona przez operatora telekomunikacyjnego.

Atak za atakiem

Kilkanaście lat temu dostępność i przepustowość łączy internetowych były nieporównywalnie niższe. *„Przeprowadzanie ataków było bardziej skomplikowane, wymagało posiadania dużej wiedzy i umiejętności technicznych, a przy tym kosztowne – to przekładało się na ich mniejszą powszechność”* – wspomina Krzysztof Białek, kierownik Działu Obsługi Incydentów Bezpieczeństwa (CERT) w Orange Polska.

Do wyraźnego wzrostu liczby i wielkości ataków DDoS przyczyniła się także aktywizacja działalności przestępczego e-podziemia – dziś na czarnym rynku komercyjnie oferuje się usługi ataku DDoS, wykorzystując do tego celu komputery, nad którymi przejęto kontrolę za pomocą złośliwego oprogramowania. Cena takiej usługi znacząco spadła i zaczyna się nawet od kilku dolarów. *„Poza wywołaniem niedostępności usług dochodzi niekiedy do sforsowania zabezpieczeń i, za pomocą złośliwego oprogramowania, kradzieży wrażliwych danych do handlu na czarnym rynku. To wariant, w którym*

za atakiem stoją cyberprzestępcy mający konkretne zamiary" – mówi Michał Śliwiński, kierownik ds. rozwoju oferty w Netii.

Nie bez znaczenia pozostaje coraz częstsze nagłaśnianie kolejnych incydentów. *„Atak DDoS może być także, niestety, narzędziem do zbudowania czarnego PR-u, jeżeli zostanie opisany w mediach"* – dodaje Michał Śliwiński. *„DDoS stał się nieodłącznym elementem towarzyszącym aktywności w internecie. Jest i będzie, musimy się z tym pogodzić"* – stwierdza Marcin Rączkiewicz, dyrektor regionu Europa Centralna i Wschodnia w Tata Communications (hurtowego operatora telekomunikacyjnego).

> ***„Operator globalny 'widzi' w sieci znacznie więcej i może reagować niemal u źródła ataku".***

Marcin Rączkiewicz, *dyrektor regionu Europa Centralna i Wschodnia, Tata Communications*

Zbudować obronę

Arsenał środków zaradczych operatora zależy od jego wielkości i profilu klientów, ich oczekiwań oraz związanych z tym inwestycji w sprzęt i oprogramowanie zabezpieczające przed atakami DDoS. Po pierwsze, każdy operator buduje nadmiarową infrastrukturę, aby w razie potrzeby „zmieścić" nagły wzrost ruchu. Po drugie, niezbędne są narzędzia do filtrowania ruchu. To oczywiście elementarz operatorskiej działalności.

> ***„Podmioty potrzebujące zabezpieczeń DDoS Protection wybiorą operatora, który może je zaoferować".***

Michał Śliwiński, *kierownik ds. rozwoju oferty, Netia*

Krajowi operatorzy, nawet najwięksi, powinni współpracować z regionalnym czy globalnymi partnerami. W polskich warunkach najczęściej atak DDoS nadchodzi z zagranicy. Operator globalny „widzi" w sieci znacznie więcej i może reagować na brzegu swojej infrastruktury, co pozwala na powstrzymanie zdarzenia przed rozprzestrzenieniem się na inne kontynenty, regiony czy kraje. To najbliższe możliwe miejsca zduszenia ataku, gdyż jego źródła są zazwyczaj bardzo liczne. Dotarcie i neutralizacja samego serwera Command-and-Control (C&C) ataku są oczywiście dużo trudniejsze. Ponadto przepustowość sieci globalnego operatora jest liczona już w terabitach, co znacznie ułatwia opanowanie nagłego wzrostu ruchu.

„W 2010 r. największy pojedynczy atak zużywał przepływności 100 GB/s, podczas gdy jeszcze w 2007 r. była to pięciokrotnie mniejsza wartość. Takich możliwości nie ma na ogół operator lokalny, a tym bardziej klient" – mówi Marcin Rączkiewicz. Z tego powodu globalni operatorzy pracują bezpośrednio z największymi podmiotami, takimi jak Amazon. *„W razie ataku jesteśmy w stanie przejąć i odfiltrować cały ruch, choć klient ma także innych dostawców łączności. Współpraca z lokalnymi operatorami jest jednak kluczowa, ponieważ to zwykle w ich sieciach zaczyna się atak.*

Jesteśmy w stanie to wychwycić i poinformować o nagłym podejrzanym wzroście ruchu" – podkreśla Marcin Rączkiewicz.

Przewaga informacji

Obok dbałości o nowoczesną technologię i jakość usług operator musi przewidywać rozwój zagrożeń i skutecznie im przeciwdziałać. Wdrożyć rozwiązanie, zbudować dedykowany zespół, opracować procedury. Tata Communications dysponuje własnym rozwiązaniem do ochrony przed atakami DDoS i posiada globalne centrum nadzoru sieci. W Orange Polska od 2006 r. działa CERT, a także SOC (Security Operations Center). Członkowie tych zespołów zajmują się identyfikacją i ograniczaniem zagrożeń występujących w internecie, w tym ochroną przed atakami DDoS oraz świadczeniem klientom operatora usług doradczych.

„Jeszcze kilka lat temu w ramach CERT nie obserwowaliśmy dużego zainteresowania usługami ochrony wśród klientów. Ostatnie ataki, o których donosiły media, w znaczący sposób wpłynęły na podniesienie poziomu świadomości zagrożeń płynących z internetu – ciągła dostępność usług jest jednym z kluczowych czynników prowadzenia biznesu" – mówi Krzysztof Białek.

> ***„Klienci są już świadomi, jak wiele może zależeć od dostępności w internecie".***

Krzysztof Białek, *kierownik Działu Obsługi Incydentów Bezpieczeństwa, Orange Polska*

„Odpowiednio wczesne wykrycie i natychmiastowa reakcja są niezbędne, ponieważ klient na ogół nie zdaje sobie sprawy z trwającego ataku, dopóki jego witryny czy usługi nie zostaną całkowicie zablokowane" – mówi Michał Śliwiński. Netia do walki z atakami DDoS wdrożyła platformę firmy Arbor Networks i powołała zespół specjalistów. *„Platforma Arbor posiada główną bazę o nazwie Atlas, która zawiera dziś 47 TB danych dotyczących ataków DDoS, jakie już wystąpiły. Mają dostęp do niej wszyscy użytkownicy tej platformy. Dzięki temu operator, który korzysta z tego narzędzia, ma wgląd w aktualną sytuację w czasie rzeczywistym"* – opisuje Michał Śliwiński.

Operatorska ochrona

Niezbędna jest także wiedza i doświadczenie, w jaki sposób filtrować ruch, uniemożliwiając lub mitygując atak. *„Trudno odróżnić atak od wzmożonego ruchu wywołanego atrakcyjną ofertą, którego firmowe serwery nie są w stanie obsłużyć"* – zaznacza Michał Śliwiński. *„W przypadku wykrycia anomalii podejmujemy natychmiastowe działania. Identyfikujemy rodzaj zagrożenia, błyskawicznie weryfikujemy, z jakim zagrożeniem mamy do czynienia, dobieramy adekwatne środki zaradcze"* – potwierdza Krzysztof Białek.

Jeżeli rozpoznano faktyczny atak, zaczyna się etap minimalizacji jego wpływu na infrastrukturę i usługi zaatakowanej firmy. Klient jest szczegółowo informowany o przebiegu sytuacji, działaniach podjętych przez operatora, otrzymuje raporty dotyczące incydentu. *„Bieżąca komunikacja i współpraca są kluczowe. W trakcie obsługi zdarzenia proponujemy klientom prowadzenie konkretnych działań, ale jesteśmy również otwarci na sugestie płynące z ich strony. Klienci często pozostawiają operatorowi swobodę doboru środków zaradczych, czasem też oczekują możliwości podejmowania decyzji na bazie naszych sugestii, na przykład filtrowania na czas incydentów całego zagranicznego ruchu lub konkretnych adresów atakujących maszyn"* – opisuje Krzysztof Białek.

Cenne bezpieczeństwo

Jak przyznają sami operatorzy, inwestycja w rozwiązanie chroniące przed atakami DDoS bywa dla nich kosztowna, ale zwraca się, ponieważ może pracować jednocześnie dla wszystkich klientów. Firmy i instytucje rzadko decydują się na własne systemy ochrony, dlatego że nie mają możliwości technicznych czy finansowych ich wdrożenia. *„Od operatora kupują wówczas 'polisę ubezpieczeniową', minimalizując ryzyko udanego ataku"* – mówi Krzysztof Białek. To tańsze

i prostsze rozwiązanie, ale nie powinno całkowicie wykluczać własnych inwestycji, które są wskazane choćby w najmniejszym zakresie. Michał Śliwiński dodaje, że największe firmy z branży finansowej czy e-commerce mają środki na inwestycje we własne zabezpieczenia. Sytuacja wygląda inaczej w przypadku instytucji publicznych, które przy wyborze rozwiązań kierują się ceną. *„W budżetach nie przewidziały tego typu wydatków na relatywnie nowe dla nich zjawisko. A podmioty publiczne coraz częściej stają się celem ataków”* – przypomina Michał Śliwiński. *„Z biegiem czasu będą dysponować odpowiednimi środkami. Rolą operatora jest zbudowanie takiego modelu współpracy, aby wspomóc administrację publiczną w walce z atakami DDoS”* – dodaje.

Ataki na wznoszącej

„Popularność i dostępność ataków DDoS w internetowym podziemiu będzie wzrastać wraz z dalszym wzrostem przepustowości oraz z coraz większą liczbą urządzeń podłączonych do sieci. Kto wie, być może ten największy atak DDoS jest dopiero przed nami” – zastanawia się Marcin Rączkiewicz. Czy problem ataku DDoS już zawitał już do świata mobilnego? Eksperci twierdzą, że tak. Mobilne terminale pod kontrolą cyberprzestępców instalujących odpowiedni malware stały się narzędziem ataku. Celem ataku może być infrastruktura odpowiedzialna za firmowe mobilne urządzenia, które coraz częściej stanowią ważny element realizacji codziennych procesów biznesowych.

Świadczenie usług zabezpieczających będzie narzędziem w walce o klienta między operatorami. Usługi tego typu mogą z czasem zostać włączone do abonamentu za pakiet usług telekomunikacyjnych dla biznesu. Tym samym staną się osiągalne dla mniejszych firm prowadzących działalność w internecie.

Według Krzysztofa Białka nie można wykluczyć, że dodatkowe rozwiązania DDoS Protection upowszechnią się i staną się częścią ochrony infrastruktury – podobnie jak dziś systemy IPS i firewalle.

Obserwujemy lawinowy wzrost ataków DDoS. Jednocześnie widzimy, że firmy nie zawsze potrafią sobie z nimi radzić. Dotychczas dostępne narzędzia pozwalały „wycinać” cały zły ruch zmierzający na daną stronę, co oznacza, że zwykli użytkownicy banku internetowego czy serwisu aukcyjnego w czasie usuwania awarii byli pozbawieni możliwości korzystania z usług. Dlatego też, jako pierwsi w Polsce, przystąpiliśmy do programu Cloud Signaling koordynowanego przez ArborNetworks, który skupia międzynarodową społeczność bezpieczeństwa operacyjnego. Ta współpraca zaowocowała wdrożeniem ochrony przeciw atakom DDoS w jednym z największych banków w Polsce. Dzięki niej bank jest natychmiast powiadamiany o zagrożeniu, a siły Orange niezwłocznie przystępują do jego zwalczenia. Natomiast klienci mają wciąż niezakłócony odbiór usług.

Marcin Sokołowski, *dyrektor wsparcia sprzedaży, Integrated Solutions*

Stanisław Dałek, *kierownik produktu ATMAN EcoSerwer w ATM SA*

Działania ochrony przed atakami DDoS to dobra praktyka operatorów czy komercyjna usługa dodatkowa?

– **Stanisław Dałek**, kierownik produktu ATMAN EcoSerwer w ATM SA: Operatorzy muszą chronić szkielet swoich sieci, aby zapewnić sprawne funkcjonowanie usług. Do dobrej praktyki należy także udostępnianie mechanizmów organizacyjnych i technicznych umożliwiających innym operatorom blokowanie źródeł ataku znajdujących się w obrębie sieci danego operatora. Ochrona usług poszczególnych klientów zwykle traktowana jest przez operatorów jako usługa dodatkowa. Wynika to m.in. z wysokiego kosztu sprzętu i usług administracyjnych niezbędnych dla świadczenia usługi oraz tego, że nie jest ona potrzebna wszystkim klientom.

W jaki sposób DDoS zagraża operatorom?

– Operatorowi zależy przede wszystkim na utrzymaniu sprawności działania szkieletu sieci, czyli tych elementów, których zablokowanie lub wysycenie zagraża funkcjonowaniu usług wielu klientów. Zabezpieczenia na poziomie operatora pozwalają wykrywać i eliminować ataki o dużym wolumenie, które zagrażają szkieletowi sieci. Warto zaznaczyć, że często mechanizmy na poziomie operatorskim muszą uporać się z bardzo dużym ruchem, rzędu dziesiątek lub setek Gb/s.

A jak zagraża ich klientom?

– Klientom zależy na utrzymaniu ciągłości działania swoich usług. Ataki DDoS są kierowane na konkretną usługę klienta – np. portal internetowy – i mogą wykorzystywać słabe punkty tej usługi, m.in. potrzebę rezerwowania określonej ilości pamięci przez każdą otwartą sesję użytkownika. Wolumen takich ataków bywa niewielki i niezauważalny dla „grubych" filtrów operatora, jedyną możliwością ich wykrywania są mechanizmy badające ruch konkretnego klienta, dostosowane do potrzeb i profilu ruchu właściwego dla jego usługi. Mechanizmy eliminowania ataków na poziomie klienta muszą być bardziej finezyjne, tak by umożliwić bardzo selektywne wycinanie ataków, bez zakłócania funkcjonowania usługi. Nie muszą one obsługiwać tak dużego ruchu jak mechanizmy operatorskie, co umożliwia dogłębną analizę. W idealnym przypadku mechanizmy ochrony klienckiej i operatorskiej powinny ze sobą współpracować. Analizator zainstalowany blisko klienta powinien móc zlecić zablokowanie ruchu na wejściu do sieci operatora. Mechanizmy takie jak blackholing BGP pozwalają nawet na zablokowanie ruchu u operatora, w którego sieci zlokalizowane jest źródło ataku.

Bezpieczeństwo o dużej skali

Paweł Chwiećko, Citi

Pracując dla tak dużej organizacji, jaką jest Citi, trzeba myśleć i działać globalnie. Rozwiązania opracowywane przez mój zespół mają za zadanie zapewniać bezpieczeństwo dla całej grupy finansowej Citi.

Do naszych obowiązków należy opracowywanie wewnętrznych standardów w obszarze bezpieczeństwa infrastruktury teleinformatycznej, ocena nowych zagrożeń oraz przygotowywanie na nie odpowiedzi. Wliczamy w to zarówno techniczne, jak i organizacyjne rozwiązania. W przypadku rozwiązań technicznych dużo czasu poświęcamy na dogłębną analizę zagadnienia, a następnie na badania rozwiązań dostępnych na rynku. Sprawdzamy także, czy istniejące obecnie w naszej korporacji rozwiązania są wystarczające, czy też należy je zmodyfikować.

> ***„Zagrożenia ciągle są te same, ale zmienia się ich postrzeganie i prawdopodobieństwo ich występowania”.***

Jeśli chodzi o bezpieczeństwo, rozwiązania, które były wystarczające rok czy dwa lata temu, mogą być obecnie nieadekwatne do istniejących, ciągle ewaluujących zagrożeń. Zdarza się, że na rynku nie ma rozwiązań, które spełniałyby nasze oczekiwania. Czasami jest to pochodną skali działalności naszej organizacji. Biznesowo jesteśmy obecni w ponad 100 krajach, co sprawia, że nasza infrastruktura jest rozległa i złożona. Współpracując bezpośrednio z twórcami rozwiązań, zlecamy w takich przypadkach modyfikacje ich produktów, aby mogły obsłużyć nasze potrzeby. Taka współpraca owocuje umieszczaniem przygotowanych dla nas rozwiązań w standardowych wersjach produktów.

Czas i pomysł

Dostawców znacznie różnicuje czas przygotowania odpowiedzi na nowe zagrożenia. Tylko najlepiej przygotowani, posiadający odpowiednie zaplecze techniczno-badawcze są w stanie robić to szybko. Podobnie jak w innych obszarach, tak i w branży bezpieczeństwa IT widzimy sporą innowacyjność. Obserwujemy dużo przykładów przedsięwzięć typu start-up, które swoimi rozwiązaniami napędzają rozwój rynku. To wszystko tworzy interesujący ekosystem pomysłów i nowych idei, istotnych także z punktu widzenia korporacji.

Sam paradygmat bezpieczeństwa IT zbytnio się nie zmienia. W dalszym ciągu mamy po jednej stronie tych, którzy chcą przełamać zabezpieczenia, a po drugiej tych, którzy strzegą, aby nie zostały one przełamane. Uogólniając, zagrożenia ciągle są te same, ale zmieniają się prawdopodobieństwa ich wystąpienia. Zmienia się świadomość tych zagrożeń, a także sposób patrzenia na nie. Coś, co do niedawna było mało prawdopodobne, obecnie jest na porządku dziennym. Jako przykład podam atak DDoS, przez wielu postrzegany jako nowe zjawisko. Pojawił się on jednak ponad dekadę temu. Oryginalnie wymyślony jako narzędzie szantażu i wymuszeń („zapłać, to przestaniemy robić ci krzywdę”) na dostawcach kasyn internetowych. Obecnie szeroko wykorzystywany jako element tzw. hacktywizmu, rozgrywek politycznych i warfare. W świecie finansów bywa też stosowany jako przykrywka do ukrycia innych działań.

Na szerokiej planszy

Bezpieczeństwo IT przypomina grę w szachy – trzeba mieć strategię i planować wiele ruchów naprzód. Tylko takie podejście zapewnia zwycięstwo. Oczywiście, mam na myśli świat korporacji, gdzie istnieją odpowiednie zasoby, aby móc to zrealizować. Jednakże bezpieczeństwo IT to temat także dla użytkowników prywatnych, którzy bardzo często nie zdają sobie sprawy z jego powagi. Wynika to z braku świadomości i odpowiednich programów mogących poprawić obecny stan rzeczy. Należałoby się zastanowić, jak można to zmienić.

Paweł Chwiećko, Vice President, od 12 lat pracuje w różnych obszarach bezpieczeństwa IT w grupie finansowej Citi. Obecnie jako Senior Engineer w zespole Network Threat Defense Engineering. Jest też szefem polskiego oddziału międzynarodowej organizacji ISC(2), zrzeszającej profesjonalistów środowiska bezpieczeństwa IT. Członek organizacji ISSA, ISACA oraz ISC(2).

Analiza wyników badania przeprowadzonego podczas konferencji Atak i Obrona 2013

Mirosław Maj

Metodologia badania

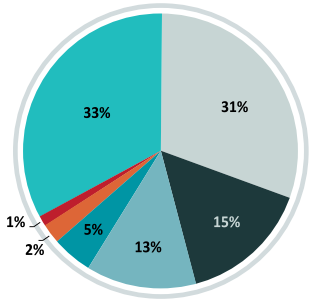
Dane zaprezentowane w tym raporcie są wynikiem badania przeprowadzonego w czasie konferencji „Atak i obrona 2013 – DDoS/APT" w dniu 26 listopada 2013 r. wśród uczestników. Przeprowadzono je z wykorzystaniem systemu elektronicznego głosowania (e-voting). W badaniu wzięło udział 85 osób. Nie każda z tych osób odpowiedziała na wszystkie pytania. Średnia liczba odpowiedzi na pytanie wyniosła 54.

Temat badania

Badanie dotyczyło zebrania informacji na temat bezpieczeństwa teleinformatycznego w polskich firmach i organizacjach. Ankietowani odpowiadali na pytania dotyczące używanych i preferowanych technik bezpieczeństwa, technicznych i organizacyjnych aspektów zapewnienia bezpieczeństwa teleinformatycznego w ich firmach i organizacjach oraz przypadków naruszenia bezpieczeństwa teleinformatycznego i sposobów reagowania na nie.

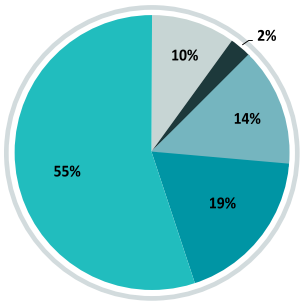
Uczestnicy badania pochodzili z dużych organizacji

W badaniu wzięło udział 85 uczestników. Najliczniej reprezentowany był sektor bankowy (31%). Dwoma innymi istotnie reprezentowanymi sektorami były sektor handlu i usług (15%) oraz sektor publiczny (13%). Uczestnicy w większości wywodzili się z dużych organizacji. Aż 74% reprezentowało organizacje, które zatrudniają więcej niż 250 osób, z czego aż 55% zatrudnia ponad 1000 osób. Potwierdza to odnotowaną reprezentację sektorową, a w szczególności uczestnictwo w badaniu przedstawicieli banków, które są dużymi organizacjami.



SEKTORY REPREZENTOWANE W BADANIU

- BANKOWOŚĆ
- HANDEL I USŁUGI
- SEKTOR PUBLICZNY
- DOSTAWA MEDIÓW
- PRZEMYSŁ
- UBEZPIECZENIA
- INNY



WIELKOŚĆ ORGANIZACJI

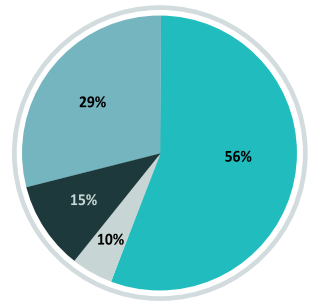
- 1-20 PRACOWNIKÓW
- 21-49 PRACOWNIKÓW
- OD 50 DO 250 PRACOWNIKÓW
- OD 250 DO 1000 PRACOWNIKÓW
- PONAD 1000 PRACOWNIKÓW

„Bezpieczniacy" nadal głównie w działach IT

Spytaliśmy uczestników badania, gdzie w ich organizacjach umiejscowione są zadania związane z zapewnieniem bezpieczeństwa teleinformatycznego. Okazuje się, że tylko w 29% przypadków zadania te realizowane są przez wydzielone komórki bezpieczeństwa IT. Nadal w większości przypadków (56%) zadania realizowane są przez działy IT. Jak widać, separacja zadań związanych z utrzymaniem infrastruktury IT i zapewnieniem jej bezpieczeństwa nadal nie jest standardem. Biorąc pod uwagę, że w badaniu mieliśmy do czynienia raczej z dużymi, rozwiniętymi strukturami organizacyjnymi, które powinny być związane z odpowiednio wysokim poziomem dojrzałości organizacji, to raczej fakt zaskakujący in minus. Świadczy on o tym, że w większości priorytety biznesowe w niewielkim stopniu są „audytowane" w kontekście ryzyka związanego z cyberzagrożeniami. To fakt, który powinien być poddany szczegółowej analizie.

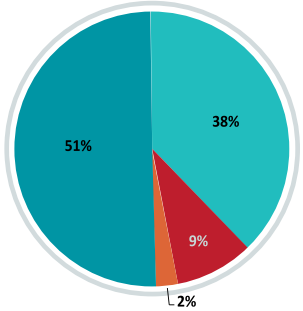
Budżet na bezpieczeństwo raczej nieznany

Choć minimalnie ponad połowa odpowiadających (51%) stwierdziła, że nie wie, jaki jest budżet na bezpieczeństwo w ich organizacjach, lub nie jest to po prostu liczone, to warto zwrócić uwagę, że wielu z respondentów jednak potrafiło podać dane na ten temat. To stosunkowo optymistyczny fakt, który wskazuje, że pieniądze wydawane na bezpieczeństwo w wielu miejscach zaczęto liczyć. Należy mieć nadzieję, że nie jest to tylko liczenie mające ograniczyć wydatki, ale je zoptymalizować. W blisko 40% przypadków budżet ten nie przekracza 5% wydatków na całe IT, choć niemała jest liczba podmiotów, które swoje wydatki mieszczą w przedziale 6–10%, a to już jest dużo. Mimo optymistycznych sygnałów wniosek jest jeden: trzeba te budżety wydzielać, liczyć i optymalizować poprzez analizę ryzyka, a przede wszystkim wyeliminowanie potencjalnych strat wynikających z ograniczania lub „przedawkowania" budżetu.



UMIEJSCOWIENIE ZADAŃ IT SECURITY W STRUKTURZE ORGANIZACYJNEJ

- DZIAŁ IT
- ZARZĄDZANIE RYZYKIEM
- DZIAŁ BEZPIECZEŃSTWA ORGANIZACJI
- WYDZIELONA KOMÓRKA BEZPIECZEŃSTWA

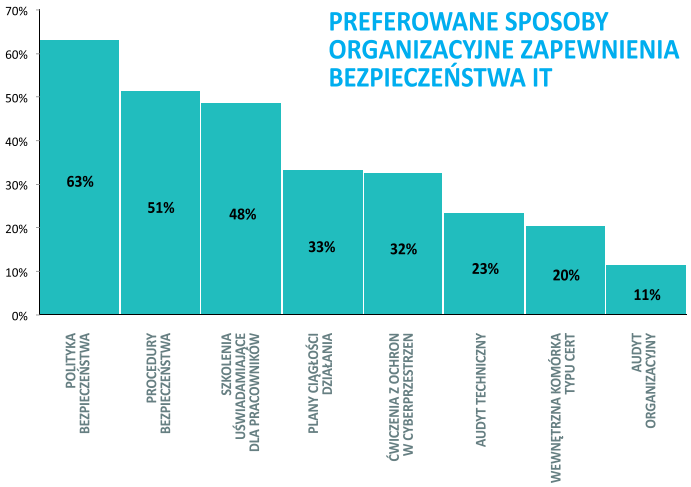


WIELKOŚĆ BUDŻETU IT SECURITY W CAŁYM BUDŻECIE IT

- 0-5%
- 6-10%
- Więcej niż 10%
- Nie jest to liczone/nie wiem

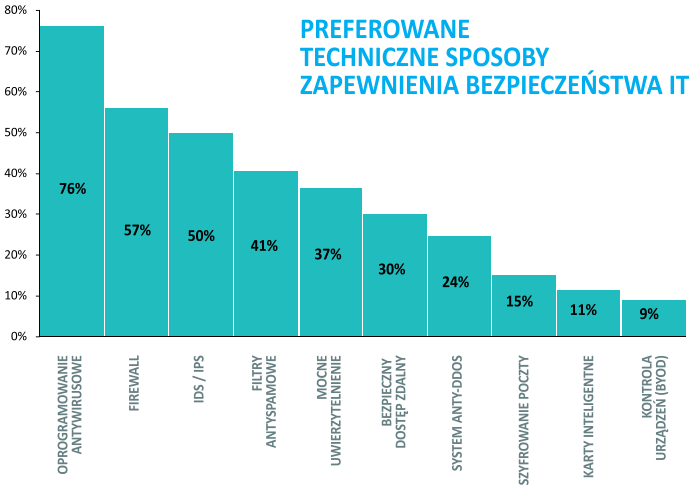
Polityka bezpieczeństwa być musi, ale wiara w nią jest ograniczona

Biorąc pod uwagę profil organizacji, z jakimi mieliśmy do czynienia w badaniu, można zaryzykować stwierdzenie, że w zdecydowanej większości z nich istnieją polityki i procedury bezpieczeństwa. Dla większości podmiotów jest to chociażby wynik obowiązującego prawa. Dlatego przy tej domniemanej powszechnej obecności polityki i procedur skromnie wygląda fakt, że dla specjalistów wywodzących się z tych organizacji takie dokumenty jak polityka bezpieczeństwa i procedury w ograniczonym stopniu są preferowanymi rozwiązaniami. Można się pokusić o interpretację mówiącą o ograniczonym zaufaniu i wierze w skuteczność tych instrumentów. Trudno się z tym nie zgodzić. Po kilkunastu już latach systematycznego wprowadzania bezpieczeństwa „na papierze" specjaliści z tej dziedziny wiedzą o tej konieczności, ale również o ograniczonej skuteczności spisanych zasad. Cyberbezpieczeństwo jest na tyle skomplikowanym i dynamicznym zagadnieniem, że papier za nim nie nadąży. Dlatego rozwiązania upatruje się w praktycznym podejściu do problemu. Blisko połowa (48%) odpowiadających wskazała na szkolenia uświadamiające dla pracowników jako na skuteczną formę budowania bezpieczeństwa IT w organizacji. Jeszcze ciekawszy jest chyba fakt upatrywania podwyższania zdolności do cyberobrony w organizacji poprzez przeprowadzanie ćwiczeń z ochrony przed zagrożeniami w cyberprzestrzeni (32%). Strategia organizacyjnego bezpieczeństwa rysuje się więc następująco: pamiętaj o polityce i procedurach, szkól pracowników firmy z podstaw bezpieczeństwa, a dla specjalistów organizuj specjalistyczne szkolenia i ćwiczenia symulujące zdarzenia kryzysowe.



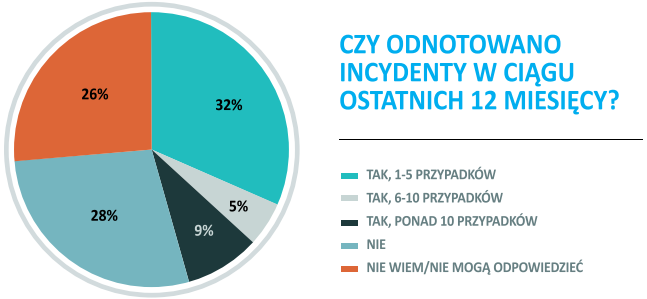
W obronie technicznej nic nowego. Kontrola urządzeń przenośnych fikcją

Na pytanie o preferowane techniczne środki ochrony uczestnicy badania odpowiedzieli w sposób raczej łatwy do przewidzenia. Oprogramowanie antywirusowe jest zdecydowanym minimum. To, że w odpowiedziach ta opcja nie osiągnęła minimum 90%, to chyba tylko i wyłącznie wynik dojrzałego spojrzenia i świadomości odpowiadających, którzy doskonale zdają sobie sprawę z niedoskonałości tego typu rozwiązania. Mniej więcej 3/4 komputerowych wirusów pojawia się w sieci tylko raz. Reszta to ich kolejne mutacje. Szczepionka przygotowana na podstawie ich wzorca jest w niewielkim stopniu skuteczna, dlatego tradycyjne metody działania programów AV stają się niewystarczające.
Producenci już od dawna to wiedzą i proponują coraz to nowe podejścia. Trzeba z nich korzystać – bez oprogramowania antywirusowego lub jeszcze szerzej: anty-malware ani rusz. W kolejce za nim stoją firewall i programy typu IDS/IPS (Intrusion Detection System/ Intrudsion Protection System). Natomiast absolutną niespodzianką jest bardzo niska pozycja dedykowanych rozwiązań ograniczających zagrożenia wynikające z powszechnego stosowania w firmach urządzeń przenośnych. Laptop, tablet czy smartfon to praktycznie narzędzia większości pracowników firm.
Nie wiadomo, jak wobec tego zinterpretować fakt, że tylko 9% odpowiadających wśród preferowanych technicznych metod bezpieczeństwa stawia na zabezpieczenia przed zagrożeniami związanymi z powszechnie używanym terminem BYOD (Bring Your Own Device). Może to wynikać z braku zaufania do podobnych rozwiązań lub z wiary w to, że ryzyko jest pod kontrolą w związku z korzystaniem z już dostępnych narzędzi zabezpieczających. Trudno byłoby uwierzyć, że ktoś liczy, iż nad zagrożeniem zapanuje poprzez odpowiednie regulacje i procedury.



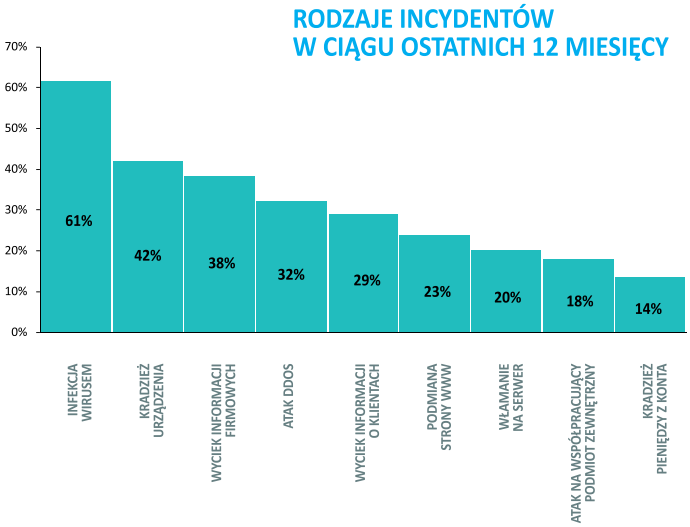
Chyba czujemy się zbyt bezpiecznie

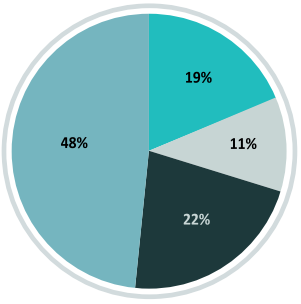
Jeśli popatrzeć na wyniki podobnych raportów, a właściwie na statystyki związane z odnotowaniem incydentów naruszających bezpieczeństwo, to może się wydawać, że nasi respondenci czują się dość bezpiecznie. W najróżniejszych raportach zazwyczaj 80–90% odpowiadających przyznaje, że ich organizacja doświadczyła incydentu. Dlatego odpowiedź: „w ciągu ostatnich 12 miesięcy nie odnotowano incydentu", podana przez 28% uczestników, badania jest zaskakująca. Dalsze 26% nic na ten temat nie wie lub nie chce powiedzieć. Wielu specjalistów od cyberbezpieczeństwa twierdzi, że organizacje dzielą się na te, które już zostały skutecznie zaatakowane i wiedzą o tym, i na te, które jeszcze tego nie wiedzą. Biorąc pod uwagę, że wśród największych ze świecą szukać tych, którzy uniknęli skutecznego ataku, trzeba się z taką opinią zgodzić. Tym samym można stwierdzić, że odsetek przyznających się do incydentu na poziomie 46% to wynik niechęci do przyznania się do problemu lub brak wiedzy na ten temat. Trudno powiedzieć, która opcja jest lepsza.



Wirusy – problem nr 1. Ataki głównie z zewnątrz

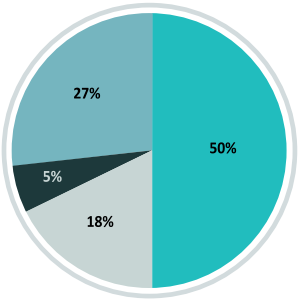
Skoro jednak incydenty mimo wszystko są, to przyjrzyjmy się ich rodzajom. Zaskoczenia nie ma – problem nr 1 to wirusowe infekcje komputerów. Swoją drogą to potwierdzenie niedoskonałości programów antywirusowych. Wśród przyznających się do incydentu 61% wskazało właśnie na problem z wirusem. Powszechny stał się wyciek informacji, który w 32% dotyczy informacji firmowych, a w 29% informacji na temat klientów. Nie lepiej jest z atakami DDoS. 32% doświadczających incydentów stwierdziło, że miało właśnie taki problem. Te właśnie dane potwierdzają słuszność doboru tematyki konferencji „Atak i obrona", czyli APT i DDoS. W odpowiedziach na pytanie o źródło ataku uczestnicy wskazali przede wszystkim otoczenie zewnętrzne organizacji. Było ich 68%, a 50% stwierdziło że atak był istotny. Na źródło wewnętrzne wskazało znacznie mniej – 30%. Choć przy tej opcji nie sposób pominąć faktu, że blisko połowa (48%) udzieliła odpowiedzi: „nie wiem / nie mogę powiedzieć". Zapewne dominowała ta druga opcja. Ataki z wnętrza organizacji zazwyczaj obwarowane są wyższą klauzulą poufności i są większym ryzykiem dla utraty wizerunku. Dowiadujemy się o nich rzadziej, również dlatego że zazwyczaj nikt inny oprócz samych zainteresowanych nie wynosi tych informacji na światło dzienne.





CZY ODNOTOWANO ATAK Z WNĘTRZA ORGANIZACJI?

- TAK, BYŁ TO ISTOTNY ATAK
- TAK, BYŁ TO MAŁO ISTOTNY ATAK
- NIE
- NIE WIEM / NIE MOGĘ POWIEDZIĆ



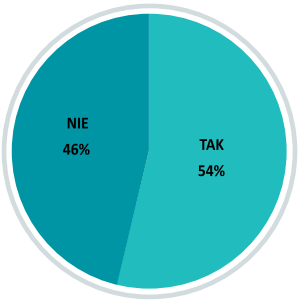
CZY ODNOTOWANO ATAK Z ZEWNĄTRZ ORGANIZACJI?

- TAK, BYŁ TO ISTOTNY ATAK
- TAK, BYŁ TO MAŁO ISTOTNY ATAK
- NIE
- NIE WIEM / NIE MOGĘ POWIEDZIĆ

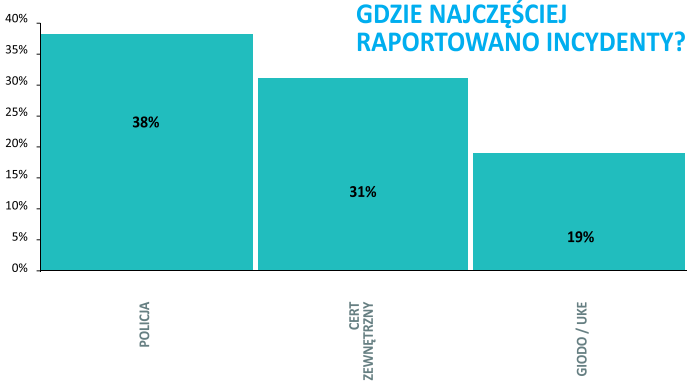
Trochę rzadziej do GIODO i UKE. Powodem, dla którego nie decydujemy się raportować, jest fakt, że przypadek nie był wart większego zainteresowania (tak stwierdziło 56% wśród nieraportujących), ale już na drugim miejscu (32%) jest brak wiary w skuteczność zgłoszenia. Regulacje wewnętrzne i obawy o utratę wizerunku organizacji to dalsze pozycje – odpowiednio 12% i 8%. Co gorsza, brak wiary w skuteczność zgłoszenia to nie wynik uprzedzenia, ale przykrych doświadczeń. Blisko 3/4 odpowiadających (73%) negatywnie ocenia wynik swojego zgłoszenia do incydentu do podmiotu zewnętrznego. 33% twierdzi po prostu, że zgłoszenie nie miało pozytywnego skutku, a co gorsza, przyniosło więcej złego niż dobrego. 40% zaś w ogóle nie uzyskało odpowiedzi czy informacji zwrotnej na swoje zgłoszenie. O ile brak pozytywnego skutku w kontekście trudności ze ściganiem przestępstw komputerowych w jakiś sposób jest zrozumiały, o tyle tak wysoki odsetek zgłoszeń pozostawionych bez odpowiedzi jest nie do zaakceptowania.

Incydenty są rzadko raportowane. Brak wiary w sens raportowania, niestety, potwierdzony doświadczeniami

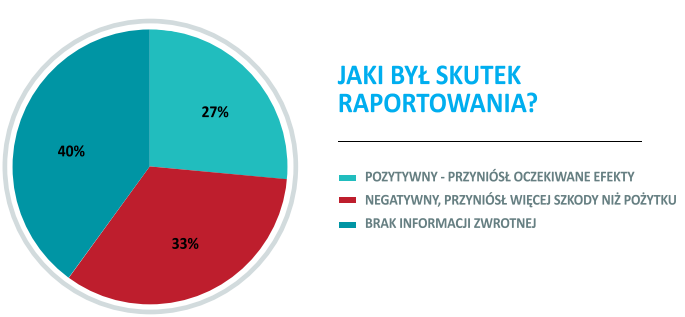
Jeśli spojrzeć na podstawowe ustalenie dotyczące raportowania incydentów, sytuacja nie wydaje się beznadziejna. Według ankiety nieznaczna większość uczestników (54%) odpowiedziała na to pytanie twierdząco, że firmy raportują. Jednak jeśli spojrzeć na dalsze informacje dotyczące raportowania, to zapala się czerwona lampka i przekonanie, że jeśli nawet nie najgorzej jest z samym raportowaniem, to negatywne doświadczenia z nim związane sprawią, że możemy się spodziewać, że będzie raczej gorzej. Gdzie najczęściej raportujemy? Na Policję – 38%, do zewnętrznego zespołu typu CERT (Computer Emergency Response Team) – 31%.

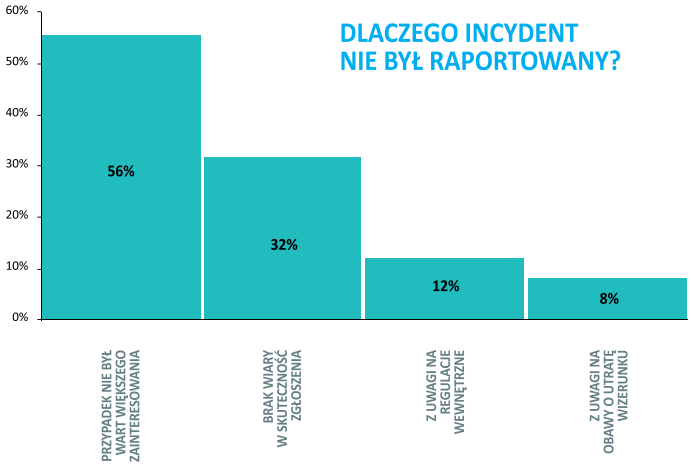


CZY INCYDENT RAPORTOWANO DO PODMIOTU ZEWNĘTRZNEGO?



GDZIE NAJCZĘŚCIEJ RAPORTOWANO INCYDENTY?





Podsumowanie badania – główne wnioski

Nie uzurpujemy sobie prawa, aby uznać badania przeprowadzone w czasie konferencji „Atak i obrona 2013 – DDoS/APT" za w pełni reprezentatywne dla całego środowiska teleinformatycznego w Polsce. Niemniej jednak grupa respondentów w sposób wyraźny reprezentowała jedne z najważniejszych sektorów, których bezpieczne funkcjonowanie w wyraźny sposób wpływa na postrzeganie ogólnego poziomu bezpieczeństwa polskiego internetu. Dlatego warto zauważyć kilka najważniejszych wniosków wynikających z odpowiedzi specjalistów do spraw bezpieczeństwa uczestniczących w badaniu.

Oto one:

1. Komórki bezpieczeństwa w organizacjach powinny w większym stopniu uzyskać niezależność w stosunku do działów IT. Tylko to pozwoli na prawidłowo funkcjonujący organizm, w którym zasady bezpieczeństwa nie będą spychane na dalszy plan. Tworzenie wewnętrznych, niezależnych komórek CERT-owych wydaje się optymalnym działaniem na rzecz poprawy bezpieczeństwa.

2. Odpowiedzialni za zarządzanie bezpieczeństwem powinni zacząć liczyć koszty swojego funkcjonowania i wykorzystywać te obliczania w zarządzaniu ryzykiem oraz optymalizacji ilościowych i jakościowych wydatków na bezpieczeństwo. W zależności od poziomu ryzyka wydatki na bezpieczeństwo powinny się wahać od kilku do 10%.

3. Warto postawić na praktyczne kształcenie pracowników organizacji. Wobec wszystkich pracowników powinny być stosowane atrakcyjne i nowoczesne programy uświadamiające zagrożenia sieciowe, zaś specjaliści powinni się udoskonalać w ramach praktycznych ćwiczeń z ochrony przed zagrożeniami z cyberprzestrzeni i zarządzania kryzysowego wynikającego z ataków sieciowych.

4. Konieczne są programy wdrażające odpowiednie zarządzanie incydentami sieciowymi od momentu ich wykrycia, poprzez odpowiednią ich obsługę prowadzącą do wyjaśnienia, często przy współpracy z podmiotami trzecimi, takimi jak zewnętrzne CERT-y i organy ścigania.

Konferencja **ATAK I OBRONA** 2013
DDoS/APT

Fotorelacja

„Atak i Obrona 2013. DDoS / APT" to pierwsza w Polsce konferencja dedykowana w całości problemowi APT (ang. Advanced Persistent Threat – zaawansowany rodzaj ataku ukierunkowego) oraz DDoS (ang. Distributed Denial of Service – rozproszona odmowa usługi). Patronat honorowy nad wydarzeniem objęły: Rządowe Centrum Bezpieczeństwa, Ministerstwo Administracji i Cyfryzacji, Biuro Bezpieczeństwa Narodowego i Generalny Inspektor Ochrony Danych Osobowych.

W konferencji wzięło udział ponad 130 osób, które zawodowo zajmują się bezpieczeństwem IT. Swoją wiedzą podzieliło się z nimi aż 18 uznanych ekspertów w dziedzinie cyberbezpieczeństwa, znanych w Polsce i na świecie. Formuła spotkania zainteresowała praktycznie wszystkie branże, co pokazuje, jak dużym problemem, niezależnie od sektora i stopnia wielkości danej organizacji, są ataki typu DDoS oraz APT.

Program konferencji został podzielony na dwa bloki tematyczne. W sesji przedpołudniowej skupiono się na DDoS, a po południu na APT. Każda sesja rozpoczynała się od wstępu, następnie dyskutowano nad konkretnymi przypadkami, a na jej zakończenie odbywało się podsumowanie i przedstawiana była lista kontrolna.

Przedstawiamy w fotograficznym skrócie relację z wydarzenia.

Poranna sesja networkingowa, zorganizowana przez profesjonalistów networkingu, umożliwiła już na samym starcie wzajemne poznanie się uczestników i przełamanie pierwszych lodów.

***Przemysław Gamdzyk**, prezes Evention, oraz **Mirosław Maj**, prezes Fundacji Bezpieczna Cyberprzestrzeń, oficjalnie otwierają konferencję.*

***David Monnier** z dobrze znanego w branży Team Cymru opowiada o tym, co ciekawego można znaleźć w internetowym podziemiu.*

Wnętrza Klubu Loft44 znakomicie współgrały z tematyką konferencji. Miejscami tajemniczo i w lekkich ciemnościach jak w czasie ataku, po czym w pełni świateł reflektorów, niczym w czasie skutecznej obrony.

***Carl Froggett**, główny inżynier w zakresie bezpieczeństwa sieci i analizy bezpieczeństwa w Citi, mówi o pouczających doświadczeniach tej globalnej korporacji finansowej.*

*Wystąpienie **Jakuba Masłowskiego** z Allegro spotkało się z ogromnym zainteresowaniem uczestników. Nie bez powodu, bo było to studium przypadku w najlepszym wydaniu. Prelegent w szczegółach i z dużą dawką praktycznych porad omówił kwietniowe ataki DDoS na największy polski portal aukcyjny.*

*Sesję przewodnią na temat APT otworzyło wystąpienie **Rika Fergusona** z Trend Micro. Znakomicie uświadomił wszystkim, jakim wyzwaniem jest ten rodzaj ataku.*

***Michał Sajdak** z Sekurak.pl przykuł uwagę uczestników, na żywo demonstrując wybrane etapy ataku APT. Pokaz prelegenta nie pozostawił złudzeń co do realności ataku.*

*Sesję na temat APT zakończyła świetna „Prezentacja podsumowująca APT. Twoja lista kontrolna“ **Borysa Łąckiego** z Bothunters.pl.*

Konferencja ATAK I OBRONA 2013
DDoS/APT

ATAK I OBRONA to nowa formuła spotkania profesjonalistów bezpieczeństwa IT. To konferencja w całości poświęcona cyberbezpieczeństwu – skupiona na najważniejszych i aktualnych zagrożeniach, której celem jest pokazanie i przekazanie istotnych zagadnień w najbardziej przystępnej i praktycznej formule, zakładającej aktywny udział wszystkich uczestników. Tematyka wydarzenia odnosi się do bieżących i istotnych cyberzagrożeń, które zgłaszają sami uczestnicy oraz praktycy, pragnący podzielić się swoimi doświadczeniami. Każdy z tematów, który pojawi się na konferencji, jest przedstawiony w postaci prezentacji praktycznego problemu (atak) i praktycznego rozwiązania (obrona).

W roku 2013 tematem przewodnim były zagrożenia DDoS (Distributed Denial of Service) i APT (Advanced Persistant Threat).

FUNDACJA bezpieczna cyberprzestrzeń

EVENTION
CZAS ZAANGAŻOWANY