Wrzesień 2021

RAPORT

Wokół zarządzania incydentami

Raport opracowany przez:

TREND MICRO

CSO COUNCIL

Spis treści

SZANOWNI PAŃSTWO,

Cyberbezpieczeństwo i bezpieczeństwo informacji to szeroki temat, obejmujący perspektywę technologiczną, organizacyjną, prawną i ludzką. Jeśli trzeba by jednak było wskazać, co stanowi tutaj rdzeń i istotę sprawy oraz probierz tego, jak dana organizacja podchodzi do kwestii cyberbezpieczeństwa, to bez wątpienia jest nią podejście do zarządzania incydentami.

To sprawa kluczowa dla zapewnienia bezpieczeństwa organizacji w świecie cyfrowym. Doskonale obrazuje, czy dana organizacja podchodzi do tego w sposób przemyślany, dojrzały i adekwatny do faktycznego poziomu ryzyk, z jakimi musi się mierzyć. Dlatego temu właśnie tematowi poświęciliśmy ten raport, przygotowany wspólnie przez Trend Micro i CSO Council. Jego kanwą jest badanie przeprowadzone w połowie tego roku wśród menedżerów cyberbezpieczeństwa i członków CSO Council. W badaniu staraliśmy się zebrać informacje o tym, jak ich organizacje podchodzą do kwestii zarządzania incydentami, jakimi zespołami dysponują, a także jak oceniają kluczowe kwestie dotyczące incydentów.

Raport ma dawać także pewien benchmark, możliwość porównania własnej organizacji z innymi. Materiał wzbogacony jest komentarzami praktyków oraz prezentacją najważniejszych wyników z globalnego raportu Trend Micro.

Raport „Wokół zarządzania incydentami" został uzupełniony również rozmowami z szefami cyberbezpieczeństwa znanych, dużych organizacji w Polsce – w których to wywiadach mówią o własnych doświadczeniach i różnorodnych aspektach związanych z zarządzaniem incydentami.

PRZEMYSŁAW GAMDZYK
ORGANIZATOR CSO COUNCIL

Odpowiednio sprawne zarządzanie incydentami jest jedną z podstawowych kwestii związanych z cyberbezpieczeństwem organizacji. Ocena jego skuteczności i wydajności to złożony proces, na który wpływa wiele różnorodnych aspektów, takich jak liczba podjętych działań, czas poświęcony na analizę poszczególnych incydentów czy stosunek obsłużonych alertów bezpieczeństwa do tych niepodjętych. Warto jednak pamiętać, że w całym procesie kluczową rolę odgrywa przede wszystkim człowiek.

To członkowie zespołów SOC, zespołów ds. incydentów, a także działów bezpieczeństwa stoją na pierwszym froncie. Właśnie dlatego jako Trend Micro i CSO Council opracowaliśmy badanie, w którym na podstawie rozmów z CSO pracującymi w polskich organizacjach przeanalizowaliśmy stan zarządzania incydentami w rodzimych przedsiębiorstwach. Jak zmieniła się liczba alertów bezpieczeństwa w ciągu ostatnich 2 lat? Jak pracownicy działów bezpieczeństwa radzą sobie z sytuacjami stresowymi? Jaka jest rola threat intelligence w zarządzaniu incydentami? I w końcu, jak można pomóc zespołom SOC? W poniższym badaniu prezentujemy odpowiedzi na te i inne kluczowe pytania związane z zakresem zarządzania incydentami bezpieczeństwa w polskich organizacjach. Wnioski pomagają zbudować możliwie najbardziej kompletny i holistyczny obraz tematu będącego jedną z najważniejszych kwestii dla zapewnienia wysokiego poziomu cyberbezpieczeństwa w przedsiębiorstwie.

Wynika z niego m.in., że zespoły do spraw cyberbezpieczeństwa zmagają się z nadmierną liczbą alertów bezpieczeństwa, przez co wolniej idzie im wykrywanie i eliminacja zagrożeń. Ponadto skromne możliwości przedsiębiorstw w zakresie korelacji i sortowania alertów często nie pozwalają na odsianie informacji o faktycznym zagrożeniu od fałszywych alarmów. Idąc dalej, usprawnienia procesów zarządzania incydentami upatruje się najczęściej w zwiększeniu zatrudnienia, automatycznej priorytetyzacji zdarzeń, a także centralizacji zarządzania typami danych. Po więcej szczegółów zapraszamy do lektury poniższego raportu „Wokół zarządzania incydentami".

PAWEŁ MALAK,
CEE REGIONAL DIRECTOR,
TREND MICRO

ZAPRASZAMY DO LEKTURY!

GOTOWOŚĆ POLSKICH ORGANIZACJI DO ZARZĄDZANIA INCYDENTAMI

Zarządzanie incydentami to ostatnio jeden z najgorętszych tematów w cyberbezpieczeństwie. Ilość alarmów związanych z bezpieczeństwem, raportowanych incydentów oraz wykrywanych ataków wzrasta z roku na rok. Niestety ewoluują także techniki oraz narzędzia wykorzystywane przez cyberprzestępców, co tym bardziej utrudnia zarządzanie tym obszarem. Wyniki ankiety Trend Micro i CSO Council, przeprowadzonej wśród polskich szefów cyberbezpieczeństwa zatrudnionych w średnich i dużych przedsiębiorstwach w Polsce, pokazują że zaledwie 12 proc. ankietowanych uważa, że obecne procesy zarządzania incydentami w ich firmach są wydajne i ustrukturyzowane. Pozostałe 88 proc. ma mniejsze lub większe zastrzeżenia do obecnego stanu rzeczy. Niemal połowa przyznaje, że proces jest co prawda ustrukturyzowany, ale nie zaspokaja obecnie wszystkich potrzeb lub wymaga przebudowy i zwiększenia nakładów na dodatkowe zasoby. Nasuwa się więc pytanie, jak firmy radzą sobie aktualnie z problemem zarządzania incydentami i jakie są perspektywy na poprawę?

KTO ZA TO ODPOWIADA?

Na pytanie kto jest odpowiedzialny za zarządzanie incydentami w organizacji,

28 %

respondetów wskazało, że posiada własny SOC, który kompleksowo zajmuje się tym tematem.

Niemal

1/4

ankietowanych odpowiedziała z kolei, że wykrywaniem i reagowaniem na incydenty zajmuje się dedykowany zespół ds. incydentów (w dziale bezpieczeństwa lub dziale IT),

a prawie

40 %

podkreśliło, że zarządzanie incydentami jest częścią obowiązków pracowników działu bezpieczeństwa/działu IT.

Oczywiście to czy firma posiada dedykowany zespół do obsługi incydentów, czy zleca to zadanie pracownikom działu IT, czy też korzysta z usługi outsourcingu SOC, zależy w dużej mierze od wielkości przedsiębiorstwa, branży i specyfiki prowadzonego biznesu.

> *„Wyniki przedstawione w raporcie wskazują na poprawę w tym zakresie. Warto jednak mieć na uwadze, że jest to pozorna poprawa, ponieważ członkowie zespołów SOC, zespołów ds. incydentów czy też działów bezpieczeństwa odgrywają kluczową rolę na froncie cyberbezpieczeństwa, zarządzając i reagując na alerty, aby uchronić swoje organizacje przed potencjalnie katastrofalnymi naruszeniami. Jednak jak pokazują badania Trend Micro, presja która na nich ciąży, spotęgowana ilością ataków, czasami wiąże się z ogromnymi kosztami niematerialnymi – tzn. osobistymi"*
>
> mówi **JOANNA DĄBROWSKA, Sales Engineer w Trend Micro**

Problem jest o tyle duży, że w wielu badanych przedsiębiorstwach (ponad 26 proc. ankietowanych) za wyłączną obsługę incydentów odpowiedzialna jest tylko jedna osoba. Niewiele mniej firm, bo niecałe 20 proc., posiada dwa takie stanowiska.

JAKOŚĆ BEZPIECZEŃSTWA

> *„Ocena skuteczności i wydajności działu bezpieczeństwa w organizacji jest procesem złożonym, w którym trzeba wziąć pod uwagę wiele aspektów. Opiera się ona przede wszystkim na rozliczeniu skuteczności działań zespołu. Dobranie odpowiednich KPI zespołu bezpieczeństwa jest niezwykle trudne bo i jak miarodajnie zbadać efekt podjętych działań. Organizacje najczęściej starają się rozliczać per stosunek obsłużonych i nieobsłużonych incydentów lub też średni czas tych działań ale w aspekcie zagrożeń nie jest to najwłaściwsza droga. Z kolei szacowanie zmian ryzyka bazując na powiadomieniach z różnych systemów nie jest trywialną operacją."*
>
> dodaje **JOANNA DĄBROWSKA**

Kwestie skuteczności i wydajności własnego działu bezpieczeństwa ankietowani najczęściej:

52%

oceniają na podstawie ilości podjętych działań.

W drugiej kolejności

42%

pod uwagę brany jest stosunek obsłużonych i niepodjętych alertów.

38%

z kolei analizuje skuteczność swojego zespołu na podstawie oceny innych jednostek, np. działu audytu wewnętrznego.

JAK USPRAWNIĆ PROCES ZARZĄDZANIA INCYDENTAMI?

Coraz więcej firm przykłada również wagę do zabezpieczeń systemowych, wdrażając odpowiednie rozwiązania i aplikacje automatyzujące część działań związanych z obsługą incydentów oraz korelujące dane z różnych systemów. Dzięki automatyzacji zespoły mogą skupić się na najważniejszych zadaniach, a zwiększenie zatrudnienia nie musi stanowić jedynego rozwiązania na polepszenie sytuacji. Jednak stworzenie własnego SOC, zatrudnienie i przeszkolenie ludzi, wdrożenie odpowiednich rozwiązań i ich bieżąca obsługa, to niełatwe zadanie. Niektóre przedsiębiorstwa powinny zatem rozważyć przeniesienie części zadań związanych z zarządzaniem incydentami , jak np. threat intelligence, na firmę zewnętrzną.

Jak pokazują wyniki badania, polscy CSO widzą potrzebę usprawniania procesów związanych z obsługą incydentów w swoich przedsiębiorstwach. Zdecydowana większość z nich uważa, że działy odpowiedzialne za zarządzanie nimi nie funkcjonują w pełni wydajnie, a aktualne procesy nie zaspokajają w pełni wszystkich potrzeb. Głównym problemem na jaki wskazują, jest przeciążenie personelu, brak odpowiedniej automatyzacji, a także zbyt mało nakładów na dodatkowe zasoby.

Prawie

63%

badanych uznało, że problem przeciążonego personelu chciałoby rozwiązać poprzez zwiększenie zatrudnienia, a także odpowiednie jego przeszkolenie.

Niewiele mniej, bo blisko

62%

chciałoby z kolei postawić na automatyczną priorytetyzację i klasyfikację zdarzeń, która pozwalałaby skupić się w pierwszej kolejności na tych najbardziej istotnych zdarzeniach.

Co jeszcze mogłoby poprawić sytuację?

Nieco ponad

61%

decydentów jako rozwiązanie widzi centralizację zarządzania i korelację wszystkich typów danych, w tym również zmian w rejestrach, aktywności procesów czy aktywności sieciowej.

MIEJSCE I ROLA THREAT INTELLIGENCE W ZARZĄDZANIU INCYDENTAMI

Autorem tekstu jest:

JOANNA DĄBROWSKA,
SALES ENGINEER W TREND MICRO

Dobrze działająca organizacja musi posiadać wiedzę na temat zagrożeń i mapować ją na własne środowisko, tymczasem niemal 3/4 organizacji nie jest jednak zadowolona ze skuteczności monitorowania informacji o nowych zagrożeniach. W większych przedsiębiorstwach operacje związane z tropieniem zagrożeń realizowane są przez dedykowane zespoły Threat Intelligence oraz Threat Hunting, a w tych mniejszych działania te stanowią część obowiązków działu bezpieczeństwa lub IT. Jednak jest to proces czasochłonny i wymaga obecności personelu dysponującego odpowiednią wiedzą i umiejętnościami. Coraz więcej przedsiębiorstw kieruje rozwiązanie tego problemu do zewnętrznych usługodawców.

DLACZEGO TAK ISTOTNE JEST ZDOBYWANIE WIEDZY O ZAGROŻENIACH?

Popatrzmy na proces zarządzania incydentami, to w jaki sposób powinien być zorganizowany, aby osiągnąć jak najwyższą skuteczność. Na tym etapie zapominamy o mechanizmach sygnaturowych i skupiamy się na tym, żeby „nakarmić" nasze środowiska wiedzą pozwalającą na identyfikację ryzykownego zachowania i w razie potrzeby zareagowania na zdarzenie w sposób precyzyjny i kompletny. A jeśli już mowa o apetycie, to ten na wiedzę o aktualnych zagrożeniach powinien być odwrotnie proporcjonalny do apetytu na ryzyko – czyli im niższy ma być poziom ryzyka rezydualnego w naszej organizacji, tym więcej wiedzy o zagrożeniach i kampaniach przestępczych powinniśmy zdobywać. Takie informacje pozwalają nam na odpowiednie przygotowanie się na potencjalny atak bez zbędnych inwestycji w ludzi i narzędzia. Wiedza o zagrożeniach i odniesienie jej do własnego środowiska pozwala również na właściwą priorytetyzacje i klasyfikację zdarzeń, a to ponad 60% organizacji wskazuje jako drogę do usprawnienia procesu zarządzania incydentami.

Duże organizacje posiadają dedykowane zespoły Threat Intelligence, które zbierają informacje o zagrożeniach. Dane te są następnie utylizowane przez zespoły Threat Hunting do śledzenia zagrożeń wewnątrz organizacji a w przypadku wykrycia potencjalnie groźnego zdarzenia uruchamiany jest zespół Incident Response, którego zadaniem jest reakcja na zdarzenie i doprowadzenie organizacji do stanu normalnego. Jednakże niewielka część organizacji jest w stanie pozwolić sobie na tak złożoną strukturę dedykowaną do zarządzania incydentami i w wielu firmach działania te stanowią część obowiązków zespołów odpowiedzialnych za bezpieczeństwo.

Ponad:

65%

organizacji ma problem z procesem zarządzania incydentami i w dużej części problemy te przekładają się na niewystraczające zasoby ludzkie, brak wiedzy i natłok nieustrukturyzowanych danych – jednym słowem zespoły bezpieczeństwa są przeciążone.

Wyjściem z tej sytuacji jest skorzystanie z usług zewnętrznych tam, gdzie to możliwe - jak pokazuje badanie przeprowadzone pośród polskich CSO, jest to rozwiązanie, które zyskuje coraz większą popularność.

Już niemal:

1/3

przyznaje, że ma wykupioną dedykowaną usługę zewnętrzną i otrzymuje bieżące raporty i alerty o zagrożeniach.

PROCES NA PIERWSZY RZUT OKA WYDAJE SIĘ DOŚĆ PROSTY – ZEBRAĆ DANE, PRZESZUKAĆ ŚRODOWISKO, ZAREAGOWAĆ – JEDNAK NIC BARDZIEJ MYLNEGO.

Już samo zbieranie informacji wymaga chociażby wiedzy o wiarygodnych źródłach, z których takie dane można pozyskiwać. Duże organizacje monitorują nie tylko ogólnie dostępne wiadomości, ale również na bieżąco śledzą sytuację w podziemiu przestępczym. Jednakże takim procesem może się pochwalić niewielka część firm w Polsce, co więcej część z organizacji nie jest w stanie monitorować nawet portali specjalistycznych i wiedzy o zagrożeniach nie pozyskuje wcale. Inny aspekt to przekształcenie wiedzy o zagrożenia do formatu, który może zostać wykorzystany w budowaniu reguł w systemach bezpieczeństwa. Co jeśli artykuł mówi o zagrożeniu w sposób bardzo ogólny i nie jesteśmy w stanie zidentyfikować użytych przez przestępców technik, taktyk i procedur (TTP – Techniques, Tactics and Procedures)? Wtedy analityk musi przeszukać inne dostępne źródła. Potem trzeba przeanalizować prawdopodobieństwo wystąpienia zdarzenia w organizacji np. poprzez weryfikację obecności w środowisku

podatności atakowanych w danej kampanii, obecności artefaktów wskazujących na wystąpienie incydentu. Sytuacja komplikuje się, jeśli źródło z którego dostarczono dane jest mało wiarygodne i wszystkie działania były zbędne lub co gorsze niekompletne.

PODSUMOWUJĄC **Threat Intelligence to podstawa budowania skutecznego systemu bezpieczeństwa, ale żeby proces ten był efektywny musi być spełnionych kilka warunków:**

- im więcej danych tym lepiej
- informacje muszą pochodzić z wiarygodnego źródła
- dane muszą być sformatowane w sposób pozwalający na budowanie reguł i identyfikację obszarów ryzyka w organizacji
- personel musi rozumieć i potrafić wykorzystać dostarczone informacje

PRZECIĄŻONE ZESPOŁY DS. BEZPIECZEŃSTWA

Oczywiście takie działania są złożone. Bez właściwych narzędzi mniejsze organizacje mogą więc nie sprostać takiemu zadaniu, z kolei większe mogą mieć duży problem z identyfikacją istotnych zdarzeń, a także z ich właściwą korelacją. Oprócz danych istotne są również umiejętności analityczne i praca zespołowa. Według wyników badania przeprowadzonego przez Trend Micro wśród polskich CSO:

46%
uważa, że specyfika nowych zagrożeń oraz ich liczba sprawiają, że dotarcie do informacji o nowych zagrożeniach w pożądanym czasie jest utrudnione,

28%
uznaje to za bardzo trudne.

Jak wynika z badania IT security Global Findings, przeprowadzonego przez Sapio research na zlecenie Trend Micro, praca związana z threat intelligence, wykonywana przez SOC, a także zespoły bezpieczeństwa IT, schodzi niestety na dalszy plan w związku z przeciążeniem pracowników i zbyt dużym czasem poświęcanym na zarządzanie alertami bezpieczeństwa.

36%
ankietowanych decydentów IT przyznaje, że proaktywne śledzenie zagrożeń cierpi w związku z tym najmocniej.

Warto pamiętać, że cały proces zarządzania zagrożeniami to nie modny trend, ale wręcz obowiązek wskazywany w wielu regulacjach, np. ustawie o krajowym cyberbezpieczeństwie czy dotyczącej ochrony danych osobowych. Zatem Threat Intelligence to wysiłek i inwestycja, które pozwalają na budowanie skutecznego procesu zarządzania incydentami tym samym pomaga zapobiegać stratom operacyjnym, finansowym i wizerunkowym, oraz pozwala budować odpowiednią odporność organizacji na cyberzagrożenia.

TONĄC W ALERTACH

Autorem tekstu jest:

MICHAŁ PRZYGODA,
SALES ENGINEER W TREND MICRO

Liczba incydentów bezpieczeństwa w polskich organizacjach w ciągu ostatnich 2 lat wzrosła lub utrzymuje się na tym samym poziomie. Obraz wyłaniający się z opublikowanych danych (wg najnowszego badania Trend Micro i CSO Council) jest niepokojący, jednak potwierdza tendencję obserwowaną globalnie w poprzednim roku, kiedy to liczba wykrytych zagrożeń cybernetycznych wzrosła o 20 proc. i przekroczyła 62,6 mld (wyniki raportu: A Constant State of Flux: Trend Micro 2020 Annual Cybersecurity Report).
Skala problemu jest poważna i nie należy jej bagatelizować szczególnie w kontekście takich zagrożeń, jak ataki ransomware, phishing, szara strefa IT czy praca zdalna.
Jak nie utonąć w alertach i zapewnić spokojny sen zespołom SOC?

Z kolei w przeprowadzonym na polskim rynku badaniu (badanie Trend Micro i CSO Council):

45%

ankietowanych

ujawniło, że
w ciągu ostatnich

2 lat

liczba incydentów
bezpieczeństwa
w organizacji

wzrosła lub utrzymuje
się na tym samym
poziomie

Te dane ilustrują, jak duża jest skala problemu i poziom zagrożeń, z którymi borykają się zespoły ds. bezpieczeństwa.

NOWE ZAGROŻENIA

Prawie połowa ankietowanych **(46 proc.)**, badanych przez Trend Micro i CSO Council przyznała, że specyfika nowych zagrożeń oraz ich liczba, sprawia, że dotarcie do informacji o nowych zagrożeniach w pożądanym czasie jest utrudnione. Przegląd „Rocznego raportu na temat stanu bezpieczeństwa Trend Micro 2020" pokazuje złożoność i trudność w wykryciu obecnych ataków. Przy użyciu starych i nowych technik cyberprzestępcy wykorzystywali luki bezpieczeństwa, błędy konfiguracji i inne niedociągnięcia systemów zabezpieczeń, które powstawały podczas pospiesznego wdrażania technologii w reakcji na panującą na świecie sytuację. Oto najważniejsze zagrożenia, spędzające sen z powiek zespołom SOC:

EPIDEMIA OPROGRAMOWANIA RANSOMWARE

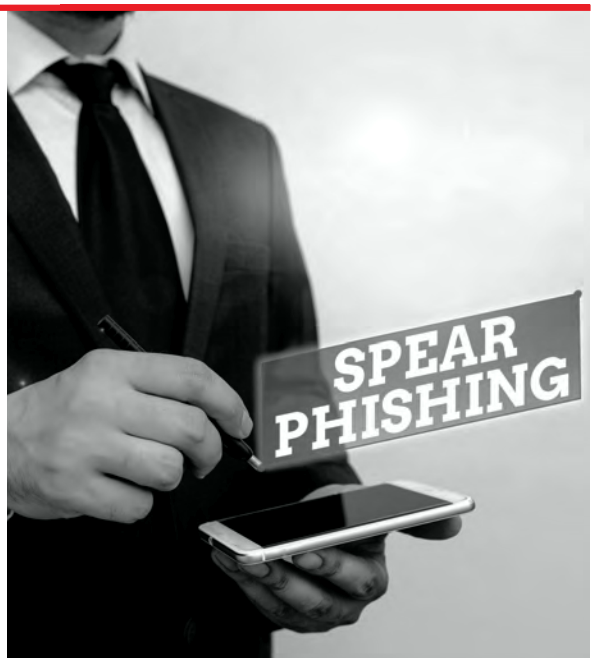
Operatorzy ransomware zmaksymalizowali swoje zyski dzięki zastosowaniu podwójnej strategii. Po pierwsze zarabiali na okupach za przywrócenie ofiarom dostępu do zaszyfrowanych danych (posuwali się nawet do podwyższania stawki za zwłokę), a po drugie grozili ujawnieniem wrażliwych informacji w przypadku braku wpłaty. Zaatakowane w ten sposób organizacje były więc narażone nie tylko na utratę danych, ale również na ryzyko poniesienia strat wizerunkowych. Znaczenia nabiera fakt, że wśród zaatakowanych jednostek znalazły się agencje i firmy z sektorów rządowego, bankowego, produkcyjnego i służby zdrowia — wizja utraty reputacji zwiększała presję na to, by spełnić żądania przestępców.

Oprogramowanie ransomware może dostać się do organizacji na wiele sposobów i skutkiem działania dotknąć wiele różnych zasobów. Dobra polityka tworzenia kopii zapasowych w połączeniu z podejściem wielowarstwowej ochrony może znacznie zmniejszyć skuteczność i wpływ takiego ataku. Firmy i instytucje muszą zabezpieczyć nie tylko fizyczne, ale też wirtualne przestrzenie pracy, czemu nie sprzyjają dynamicznie zmieniające się okoliczności.

PROSTY, ALE SKUTECZNY PHISHING

Rozwój tej techniki w ubiegłym roku zakładał sięgnięcie po nowe elementy, takie jak formularze czy ankiety, za pomocą których dokonywano ataków.

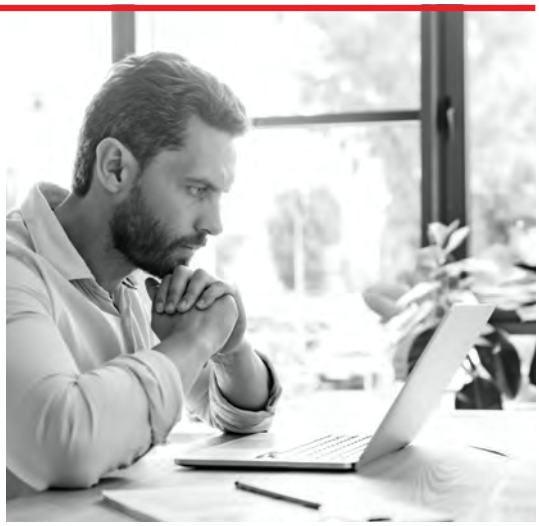
W 2020 r. częściej byliśmy także świadkami najmocniej ukierunkowanej i wyrafinowanej formy phishingu, czyli spear phishingu, polegającego na wysyłaniu niestandardowych, sprofilowanych wiadomości do dobrze zbadanych grup docelowych. Kiedy sprawy dotyczyły tematów związanych z COVID-19, sporów terytorialnych, kwestii dyplomatycznych, a przy okazji poprzedzone były dokładną i wnikliwą analizą, konsekwencje ataków były daleko idące, a same ataki ekstremalnie trudne do wykrycia.



W 2020 roku wciąż bardzo często powtarzały się ataki mające na celu wyłudzenie informacji (tzw. phishing). Według naszych danych 91 proc. spośród 62,6 mld zagrożeń zablokowanych w ubiegłym roku przez Trend Micro zostało zainicjowane za pomocą poczty elektronicznej. Nasi analitycy wykryli w 2020 roku ponad 175 mln adresów URL wykorzystywanych do phishingu (hakerzy atakowali rozproszonych zdalnych pracowników).

NAJSŁABSZE OGNIWO – PRACA ZDALNA

Pracownicy są często określani, jako najsłabsze ogniwo w korporacyjnym łańcuchu bezpieczeństwa. Masowe przejście do pracy zdalnej w 2020 r. wpłynęło również na zwiększenie obciążenia pracą zespołów SOC. Praca w domu doprowadziła pracowników do bardziej ryzykownych zachowań, niż można by sądzić m.in. przesyłanie danych firmowych do niezatwierdzonych aplikacji, korzystanie niezatwierdzonych narzędzi, niezabezpieczone rutery i wiele innych.

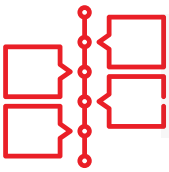


Z raportu podsumowującego stan cyberbezpieczeństwa w 2020 roku wynika, ze sieci domowe były częstym celem cyberprzestepców, którzy za ich pośrednictwem chcieli dostać się do systemów przedsiębiorstw lub przejąć urządzenia IoT i przekształcić je w botnety. Według naszych danych liczba ataków na takie sieci wzrosła o 209% i osiągnęła prawie 2,9 mld, co odpowiada 15,5% wszystkich gospodarstw domowych. W ponad 5% gospodarstw zaatakowane zostały urządzenia podłączone do Internetu. W większości przypadków (74%) hakerzy logowali się do sieci domowych za pomocą algorytmów siłowych (ang. brute force), aby przejąć kontrolę nad routerem lub urządzeniem mobilnym.

ABY USPRAWNIĆ PROCES ZARZĄDZANIA INCYDENTAMI (ALERTAMI) PONAD POŁOWA ANKIETOWANYCH (62-63 PROC.) PRZYZNAŁA, ŻE POTRZEBNA JEST:

Korelacja wszystkich typów danych, nie tylko logów, ale również np. zmian w rejestrach, aktywności procesów, aktywności sieciowej

Automatyczna priorytetyzacja i klasyfikacja, pozwalająca skupić się na zdarzeniach istotnych



Centralizacja zarządzania zdarzeniami

Szybsza i zautomatyzowana reakcja na zdarzenia, pozwalająca na redukcję potencjalnych błędów

Dodatkowa kadra w zespole zarządzania incydentami

Z ROZWOJEM CLOUD COMPUTINGU IDZIE ROZWÓJ SHADOW IT

CZY PRZEDSIĘBIORSTWA SĄ PRZYGOTOWANE NA NOWE ZAGROŻENIA?

W świecie IT jakiś czas temu osiągnięto punkt zwrotny – ponad połowa nowych wydatków była przeznaczana właśnie na chmurę. Trendy na globalnym rynku rozwiązań IT oraz obecna sytuacja, w której zdalny tryb pracy okazał się jedną z głównych opcji na zachowanie ciągłości działań, spowodowały że rozwiązania chmurowe stały się kluczowym dla funkcjonowania organizacji elementem. Warto jednak pamiętać, że to doceniane za elastyczność, skalowalność i efektywność kosztową środowisko, wymaga właściwych zabezpieczeń. Jak jednak pokazują wyniki badania przeprowadzonego przez Trend Micro i CSO Council, **obecnie zaledwie 38 proc. rozwiązań do monitorowania bezpieczeństwa obejmuje obszar chmury**, a aż blisko 70 proc. badanych przyznaje, że tylko częściowo lub w ogóle nie monitoruje tzw. „shadow IT".

Problem jest dobrze widoczny choćby w raporcie Trend Micro podsumowującym 2020 r. na temat stanu bezpieczeństwa. Za główną przyczynę incydentów z ubiegłego roku uznano nieodpowiednią konfigurację chmury, w efekcie czego na liście następstw uwzględniono m.in.: rozprzestrzenianie się złośliwego oprogramowania, kradzież informacji i danych uwierzytelniających czy przeprowadzanie rozproszonych ataków typu DDoS.

CYBERPRZESTĘPCY WYKORZYSTUJĄ BŁĘDY

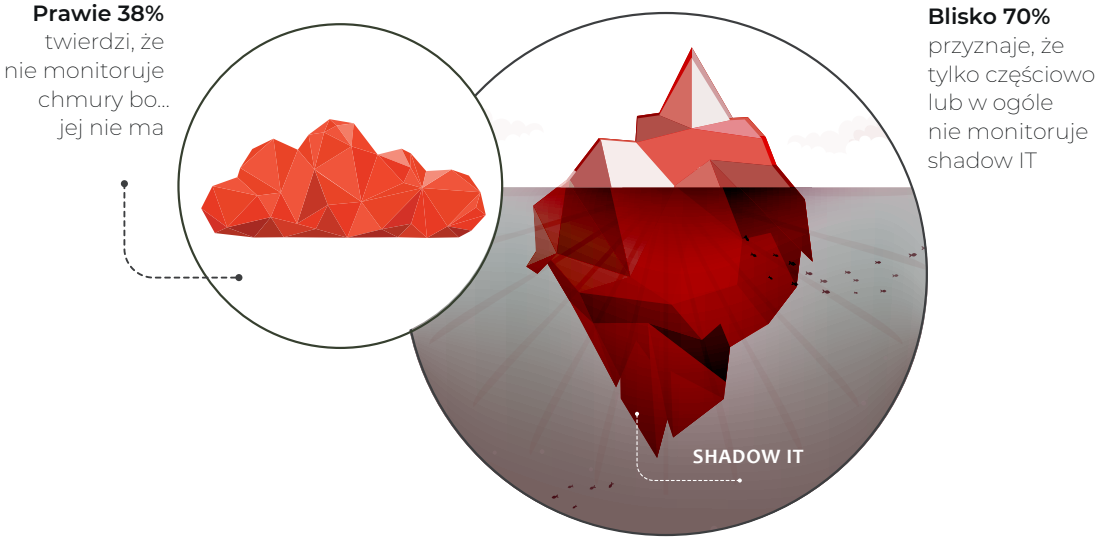
> *„Co ciekawe, środowiska chmurowe nie tylko były i są na celowniku cyberprzestępców, ale zaczęły stanowić dla nich dogodną podziemną infrastrukturę, ułatwiającą działanie, a nawet kooperację. Istnieje obszerna lista rozpowszechnianych w podziemiu usług opartych na chmurze, takich jak usługi hostingowe, mobilne przestrzenie robocze, czy usługi związane z telekomunikacją. Chmura umożliwia im bowiem przetwarzanie ogromnych ilości danych oraz zarządzanie nimi przez złośliwe podmioty bez konieczności posiadania własnej złożonej infrastruktury. Dzięki temu ataki mogą przebiegać szybciej i skuteczniej."*

mówi **JOANNA DĄBROWSKA, Sales Engineer w Trend Micro**

Aktualny obraz zagrożeń przedstawiają wyniki innego raportu Trend Micro - Turning the Tide. Firma oszacowała, że w 2021 r. cyberprzestępcy będą zwracać szczególną uwagę na sieci domowe, jako najważniejszy punkt dostępu i ataku na korporacyjne sieci IoT oraz firmowe dane i systemy informatyczne. Poza tym przewidywania wskazywały właśnie na dużą liczbę ataków ransomware i stosowanie coraz bardziej ukierunkowanych i wyrafinowanych taktyk, ataki na łańcuchy dostaw oraz phishing. Dynamicznie rozwijające się środowiska chmurowe, umożliwiające pracę zdalną i przechowywanie cennych danych firm, znalazły się więc w szczególnym niebezpieczeństwie. Najdotkliwiej odczują je firmy, które rozwiązania chmurowe wprowadzały w reakcji na pandemię, w pośpiechu i w chaotyczny, przypadkowy sposób. Tym bardziej, że działania te bardzo mocno wpłynęły na rozwój zjawiska nazywanego shadow IT.

ROŚNIE PROBLEM ZWIĄZANY Z SHADOW IT

Przeniesienie pracy do środowiska chmurowego i praca zdalna sprawiają również, że coraz większy problem zaczyna stanowić tzw. shadow IT. Jest szerokie pojęcie, które może odnosić się do dowolnego oprogramowania, sprzętu lub innych zasobów, które są nabywane i wykorzystywane bez zgody działu IT.



W przedsiębiorstwie oznacza to, że działy IT często jako ostatnie dowiadują się, że jednostki biznesowe wykorzystują narzędzia, w tym te dostępne w chmurze publicznej, bez należytej staranności i uwagi poświęcanej kontroli zgodności czy bezpieczeństwu. Takie narzędzia są często wykorzystywane jako platformy do współpracy i wymiany informacji między zespołami i nierzadko przetwarzane są tam dość krytyczne dla organizacji dane. Potrzeba optymalizacji biznesowej doprowadza do zmniejszonej widoczności ryzyka i braku świadomości zagrożeń wewnętrznych. Jak wynika z przeprowadzonego badania, prawie 38 proc. badanych twierdzi, że nie monitoruje chmury, bo... jej nie ma, a niemal 3/4 bagatelizuje problem związany z rozwojem shadow IT. Tymczasem negowanie obecności chmury we własnym środowisku należy przyjąć za fikcję, w szczególności w obszarze jakim jest shadow IT.

KONIECZNE WSPARCIE DLA DZIAŁÓW DS. BEZPIECZEŃSTWA IT

Największe wyzwania stojące przed wszystkimi działami bezpieczeństwa to niedobór wykwalifikowanych pracowników, brak skuteczniejszej metody wykrywania i reagowania na zagrożenia oraz wciąż rosnąca liczba ataków i incydentów wymagających reakcji. Dla dużych przedsiębiorstw krzyżowanie się tych problemów jest często przytłaczające. Jak pokazuje badanie Trend Micro i Sapio Research, już ponad połowa zespołów zajmujących się bezpieczeństwem SOC/IT jest przytłoczona liczbą alertów generowanych przez systemy.

> *Aby ograniczyć ryzyko firmy powinny korzystać z bardziej zaawansowanych platform do wykrywania zagrożeń i reagowania na nie, co przełoży się na większą wydajność zespołów i poprawi całościowe bezpieczeństwo w organizacji. Wsparciem dla zespołów SOC są systemy klasy XDR analizujące dane z wielu elementów środowiska IT i korzystające z wydajnych mechanizmów uczenia maszynowego oraz AI. Pozwalają one na monitorowanie ryzyka, automatyzację procesów oraz centralne zarządzanie zagrożeniami wykrytymi w poczcie elektronicznej, stacjach roboczych, serwerach, sieci i przede wszystkim w chmurze."*
>
> powiedziała **JOANNA DĄBROWSKA**

„SZARA STREFA INFORMATYCZNA" (SHADOW IT)

Badanie przeprowadzone w pierwszej połowie 2020 roku przez Trend Micro (Head in the Clouds) pokazało, że choć w trakcie lockdownu wielu pracowników zyskało większą świadomość zagrożeń cybernetycznych, złe nawyki nadal się utrzymują. Ponad połowa badanych (56 proc.) przyznała, że używa na firmowych urządzeniach aplikacji niezwiązanych z pracą, a 66 proc. pobrało na te urządzenia dane przedsiębiorstwa. 39 proc. respondentów tego badania „często" lub „zawsze" uzyskiwała dostęp do danych przedsiębiorstwa z urządzeń prywatnych, natomiast 29 proc. uważa, że może bez problemu używać aplikacji niezwiązanych z pracą, ponieważ rozwiązania wspierane przez dział informatyczny są „bez sensu". Taka sytuacja prowadzi prosto do utworzenia „szarej strefy informatycznej" i eskalacji ryzyka. Świadczy również o tym, że obecne metody szkolenia użytkowników w zakresie cyberbezpieczeństwa już nie wystarczają. Wielu pracowników zna najlepsze procedury, ale ich nie przestrzega.

ZESPOŁY SOC NIE WYTRZYMUJĄ PRESJI

Wysoka liczba alertów bezpieczeństwa w przedsiębiorstwach sprawia, że zespoły odpowiedzialne za cyberbezpieczeństwo i obsługujące centra operacji bezpieczeństwa (SOC) są w pracy przeciążone, co przekłada się negatywnie również na życie prywatne pracowników. Jak pokazują wyniki badania IT security Global Findings przeprowadzonego przez Trend Micro, problem ten dotyczy w Polsce już 59 proc. analityków. Wpływ na taki stan rzeczy mogą mieć przede wszystkim braki kadrowe i kompetencyjne, a także brak odpowiedniej integracji infrastruktury.

PRZEPROWADZONE BADANIE WSKAZUJE, ŻE NAWET :

83 %

decydentów zajmujących się bezpieczeństwem IT odczuwa w jakimś stopniu negatywny wpływ emocjonalny pracy związanej z zarządzaniem alertami dot. zagrożeń.

Zbyt duża ilość alertów sprawia, że:

37 %

menadżerów nie potrafi „wyjść z pracy”, co pochłania ich czas wolny.

36%

czuje się zbyt zestresowana, by odpowiednio się zrelaksować.

32%

staje się drażliwych w kontaktach z przyjaciółmi i rodziną.

Jedynie:

17%

respondentów nie myśli o swojej pracy w czasie wolnym.

Z CZEGO MOGĄ WYNIKAĆ WSPOMNIANE PROBLEMY?

Ponad połowa, bo aż **61%** istniejącej infrastruktury bezpieczeństwa, nie jest wykorzystywana.

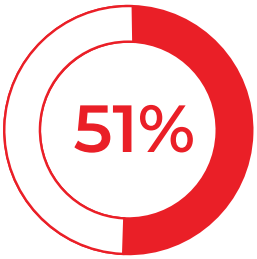
Jak wskazują badani, najczęstszą przyczyną jest brak ludzi lub wystarczających umiejętności, które pozwalałyby na odpowiednie z niej korzystanie **(39 proc.),** a także niewystarczająca integracja infrastruktury **(38 proc.).**

A JAK SIĘ MAJĄ SPRAWY POZA POLSKĄ?

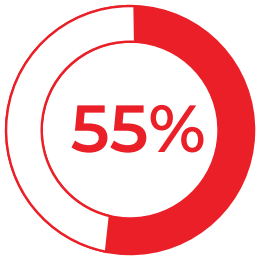
W ramach globalnego badania ankietowano **2303 osoby** podejmujące decyzje związane z bezpieczeństwem IT i SOC w firmach z różnych branż zatrudniających w większości **ponad 250 pracowników.**

Z przeprowadzonej analizy wynika, że praca polegająca na zarządzaniu alertami dotyczącymi zagrożeń wpływa na życie prywatne **70 proc. respondentów.**

Jednocześnie:

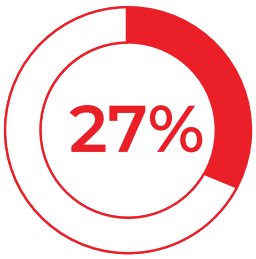


uważa, że ich zespół jest przytłoczony liczbą zagrożeń,



nie ma pewności co do swoich możliwości określania priorytetów alertów i reagowania na nie

Zespoły poświęcają aż:



swojego czasu na obsługę fałszywych alarmów.

Potwierdzeniem tych wyników jest niedawne badanie firmy Forrester, które pokazało, że „zespoły ds. bezpieczeństwa mają zdecydowanie za mało pracowników, aby móc reagować na incydenty – i to mimo coraz liczniejszych ataków. Centra operacji bezpieczeństwa (SOC) potrzebują skuteczniejszej metody wykrywania i reagowania, dlatego potrzebują wielowarstwowych rozwiązań typu XDR (cross detection and response), które działają zupełnie inaczej niż inne narzędzia dostępne obecnie na rynku”.

Jak pokazało badanie przeprowadzone przez Trend Micro, zespoły ds. cyberbezpieczeństwa i obsługujące centra operacji bezpieczeństwa są więc przeciążone przez bardzo dużą liczbę alertów, co wpływa na ich samopoczucie zarówno w pracy, jak i w życiu prywatnym.

Powoduje to, że duża część alertów jest często po prostu zbywana lub wręcz ignorowana. Może to narazić przedsiębiorstwa na ogromne koszty związane z płaceniem kar wynikających z naruszenia przepisów RODO.

Decydenci ds. IT mają jednak w większości świadomość, że zwiększenie nakładów przeznaczanych na personel, automatyzacja priorytetyzacji i klasyfikacji zdarzeń, a także odpowiednia integracja i centralizacja zarządzania mogą znacznie usprawnić zarządzanie incydentami i pozwolić uniknąć niepotrzebnych konsekwencji.

JAK POMÓC ZESPOŁOM SOC?

Zespoły ds. cyberbezpieczeństwa zmagają się z nadmierną liczbą alertów bezpieczeństwa, przez co wolniej idzie im wykrywanie i eliminacja zagrożeń. Przedsiębiorstwa mają coraz większy problem w szczególności z niezintegrowanymi narzędziami, chaotycznymi powiadomieniami i wyrafinowanymi zagrożeniami, bez względu na to, czy posiadają własne SOC, czy też funkcję tą pełni przeciążony dział informatyczny. Na działach zajmujących się cyberbezpieczeństwem spoczywa ogromna odpowiedzialność, ponieważ muszą one szybko identyfikować zagrożenia, aby możliwie jak najbardziej zminimalizować ryzyko i szkody.

WYZWANIA ZWIĄZANE Z ZARZĄDZANIEM ALERTAMI

> *„W firmie zatrudniającej średnio 1000 osób, na wejściu do systemu SIEM, co sekundę w szczytowych momentach może mieć miejsce nawet 22 000 różnych zdarzeń. Łącznie może to dać nawet 2 mln zdarzeń dziennie. Biorąc pod uwagę ilość powiadomień, które generują różne rozwiązania oraz w związku z przepracowaniem odpowiedzialnych za ich monitorowanie zespołów, aż 45 proc. analityków zdarzyło się chociaż raz zignorować informację o zagrożeniu i zająć się w tym czasie innymi zadaniami."*
>
> mówi **MICHAŁ PRZYGODA, Sales Engineer w Trend Micro**

Skromne możliwości w zakresie korelacji i sortowania alertów nie pozwalają na efektywne odsianie informacji o faktycznym zagrożeniu od fałszywych alarmów i szumu. Jak pokazuje badanie IT security Global Findings przeprowadzone przez Trend Micro, ponad połowa, bo aż 61 proc. istniejącej infrastruktury bezpieczeństwa, nie jest wykorzystywana. Jak wskazują badania, najczęstszą przyczyną jest brak ludzi lub wystarczających umiejętności, które pozwalałyby na odpowiednie z niej korzystanie (takiej odpowiedzi udzieliło 39 proc. ankietowanych decydentów ds. IT), a także niewystarczająca integracja infrastruktury (38 proc.).

Potwierdzają to także wyniki raportu ***Innovation Insight for Extended Detection and Response Gartnera***, które pokazują, że dwa największe wyzwania stojące przed wszystkimi działami ds. cyberbezpieczeństwa to właśnie zatrudnianie i utrzymanie personelu z kwalifikacjami technicznymi oraz wypracowanie systemu zabezpieczeń, który pozwoli sprawnie konfigurować i serwisować mechanizmy obronne oraz szybko wykrywać zagrożenia i na nie reagować. Nawet dla dużych przedsiębiorstw nakładanie się obu problemów może być często zwyczajnie przytłaczające.

AUTOMATYZACJA PROCESÓW

Duża liczba alertów bez wyraźnych wskaźników powoduje, że trudno jest określić, na co właściwie należy zwracać uwagę. Nawet jeśli uda się już zidentyfikować zagrożenie, trudno jest prześledzić jego realny wpływ na organizację. Śledzenie tego może okazać się czasochłonnym zadaniem, na które często po prostu zwyczajnie brakuje środków. XDR pozwala na automatyzację procesów oraz dostarcza bogaty zestaw danych i narzędzi, które w innym wypadku byłyby trudne do uzyskania. Przykładem może być automatyczna analiza przyczyn, dzięki której analityk uzyskuje dokładne informacje na temat przebiegu ataku w czasie, który może obejmować pocztę elektroniczną, punkty końcowe, serwery, chmurę i sieć. Pozwala to na szczegółowe zbadanie każdego kroku ataku, co umożliwia podjęcie odpowiednich przeciwdziałań.

> *„Rozwiązania XDR, takie jak opracowane przez Trend Micro Vision One, pomogły już do tej pory setkom organizacji w odpowiednio sprawnej identyfikacji i ograniczeniu cyberzagrożeń poprzez korelowanie danych z całego środowiska informatycznego, a nie tylko endpointów, jak ma to miejsce w przypadku rozwiązań EDR. Rozszerzone wykrywanie gromadzi i automatycznie koreluje dane z różnych warstw zabezpieczeń – poczty elektronicznej, wspomnianych punktów końcowych, serwerów, systemów chmurowych i sieci, co umożliwia szybsze wykrywanie zagrożeń oraz ich skuteczniejszą i szybszą analizę.”*

mówi **MICHAŁ PRZYGODA**

Tego rodzaju rozwiązanie pozwala przede wszystkim zwiększyć wydajność, ponieważ nawet mniej zaawansowane i doświadczone zespoły będą mogły dzięki niemu wejść na wyższy poziom skuteczności. Szybsza analiza incydentów związanych z bezpieczeństwem, identyfikacja wzorców krytycznych zagrożeń i złożonych ataków, lepsze zapoznanie się ze swoim stanem zabezpieczeń – to wszystko daje możliwość proaktywnej identyfikacji i oceny potencjalnych zagrożeń bezpieczeństwa.

Wprowadzenie holistycznej platformy do obrony przed zagrożeniami, takiej jak Trend Micro Vision One, pozwala zapewnić większą widoczność zagrożeń i dostarcza kompleksowych informacji o nich. Dzięki wielowarstwowym modelom wykrywania zagrożeń wzbogacanych informacjami *threat intelligence*, przedsiębiorstwa mogą dostrzec złożone ataki i słabe punkty zabezpieczeń, które na co dzień umykają rozwiązaniom wyspowym. Platformę można łatwo połączyć nie tylko z systemami bezpieczeństwa Trend Micro, ale także z innymi technologiami zabezpieczającymi. Dostępne są integracje z rozwiązaniami takich producentów, jak m.in. Check Point, Palo Alto, Microsoft, czySplunk.

Świetne efekty wdrożenia holistycznego, zautomatyzowanego rozwiązania, pokazują na przykład wyniki badania ***The XDR Payoff: Better Security Posture***. Przebadane przedsiębiorstwa, które postawiły na automatyzację agregacji, korelacji i analityki wskazują, że aby zastąpić zautomatyzowane systemy, potrzeba byłoby zatrudnić aż 8 pełnoetatowych, wykwalifikowanych pracowników. Dochodzi w nich również do ignorowania ponad dwukrotnie mniejszej liczby alertów bezpieczeństwa.

TONĄC W ALERTACH – JAK USPRAWNIĆ OBSŁUGĘ ALERTÓW

W wyniku rosnącej cyberprzestępczości i zwiększonej liczby narzędzi, a także braku technologii do korelowania i ustalania priorytetów alertów, zespoły SOC są przytłoczone coraz większą liczbą incydentów.

Według:

45%

ankietowanych (badania przeprowadzonego przez Trend Micro i CSO Council), alerty nie są poddawane dalszej analizie z powodu niewystarczających zasobów.

Prawie:

25%

przyznaje, że dostaje zbyt dużą ilość alertów,

a ponad:

14%

wskazuje na brak odpowiedniej wiedzy w zespole.

WYWIADY

Okiem CSO

TREND MICRO CSO COUNCIL

W KWESTII CYBERBEZPIECZEŃSTWA NALEŻY WYCHODZIĆ POZA SCHEMATY

Bezpieczeństwo organizacji to sprawa najwyższej wagi. O automatyzacji, elastyczności i wyzwaniach, z jakimi zmagają się zespoły odpowiedzialne za cyberbezpieczeństwo, rozmawiamy z Robertem Kanigowskim, Kierownik ds. Bezpieczeństwa Informacji i Zarządzania Ciągłością Biznesu w Provident.

PRZEMYSŁAW GAMDZYK
ORGANIZATOR CSO COUNCIL

PRACUJE PAN NA STANOWISKU KIEROWNIKA DS. BEZPIECZEŃSTWA INFORMACJI I ZARZĄDZANIA CIĄGŁOŚCIĄ BIZNESU. JAK WYGLĄDA OBSZAR ZADAŃ, ZA KTÓRY PAN ODPOWIADA?

ROBERT KANIGOWSKI

Odpowiadam za szeroko pojęte bezpieczeństwo informacji, które opiera się na dwóch filarach. Pierwszy z nich to bezpieczeństwo technologii, rozumiane jako wszystko to, co dzieje się z informacją w systemach IT. Drugi to bezpieczeństwo biznesu, czyli to, w jaki sposób biznes współdzieli informacje, co z nimi robi. Moim zadaniem, jako Kierownika ds. Bezpieczeństwa Informacji i Zarządzania Ciągłością Biznesu, jest kompleksowa opieka nad tymi obszarami.

PG: CZY TO, W JAKI SPOSÓB FIRMA DEFINIUJE INCYDENTY, WYNIKA Z JAKIEGOŚ UNIWERSALNEGO SYSTEMU LUB MIARY?

RK: Jest wiele czynników, które mają na to wpływ. W pierwszej kolejności to kwestia wielkości firmy i rodzaju branży. Niektóre obszary są narażone bardziej od innych, czego przykładem jest branża finansowa. Jest też wiele czynników, które trudno sklasyfikować, a które obserwujemy np. w przypadku ataków ukierunkowanych, kiedy organizacja z jakiegoś powodu znajduje się na celowniku cyberprzestępców.

PG: CZY ROSNĄCA LICZBA INCYDENTÓW WYNIKA ZE WZMOŻONEJ LICZBY ATAKÓW, CZY Z TEGO, ŻE POTRAFIMY JE CORAZ SPRAWNIEJ WYKRYWAĆ?

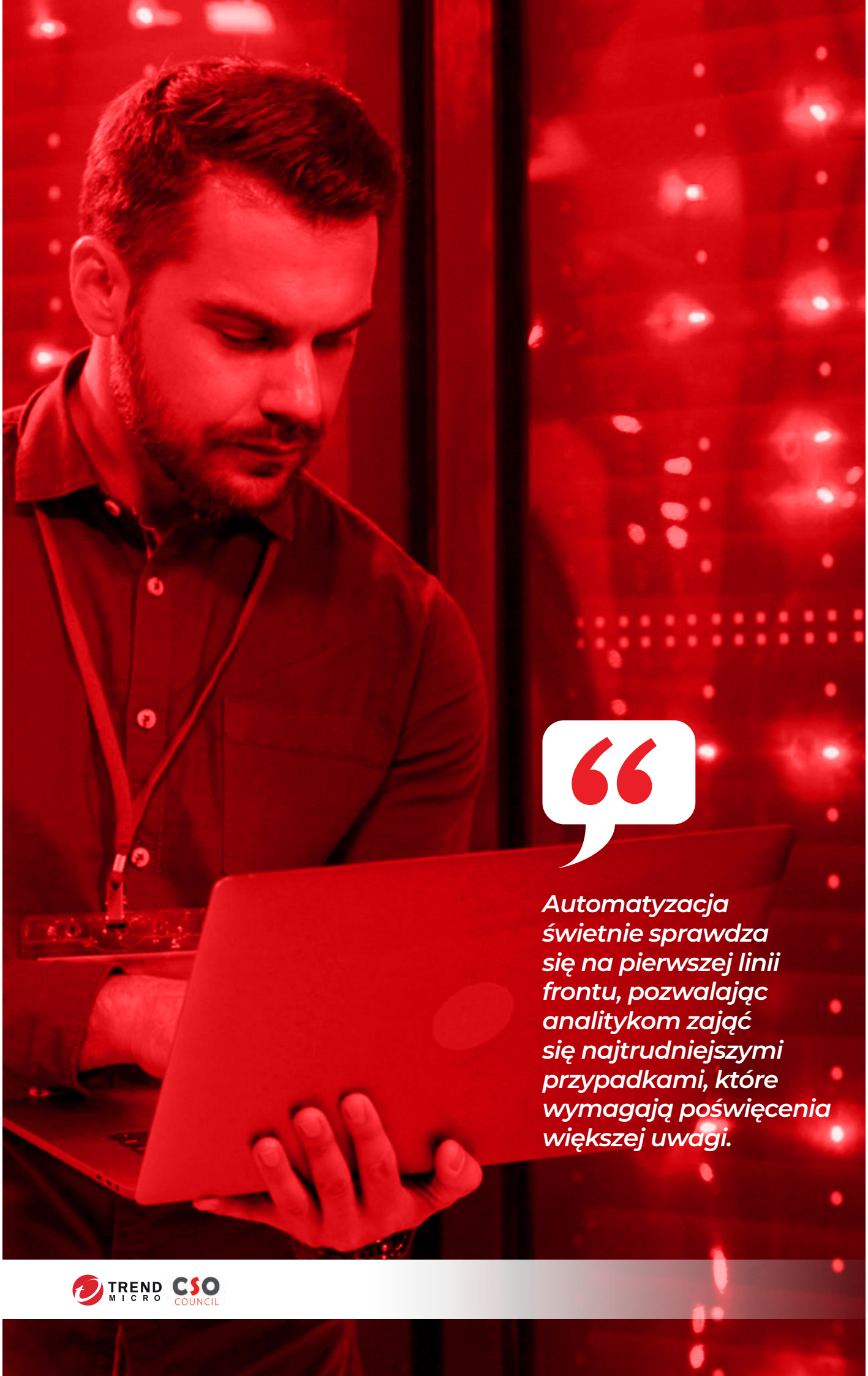
RK: Myślę, że i jedno i drugie. Z jednej strony potrafimy szybciej i skuteczniej wykrywać incydenty, z drugiej cyberprzestępcy dynamicznie rozwijają swoją działalność. Wszystkie dostępne na rynku raporty dowodzą, że ich aktywność się zwiększa. Coraz chętniej korzystają też z opcji automatyzacji ataków - wyrafinowanych rozwiązań, które w krótkim czasie pozwalają im atakować dziesiątki tysięcy organizacji na całym świecie. Znacząco wpływa to na wzrost wolumenu incydentów.

PG: WOBEC OGROMU RÓŻNEGO RODZAJU ALERTÓW, TYCH BŁAHYCH, JAK I BARDZO POWAŻNYCH, JAK WYKRYWAĆ TE, KTÓRYM TAK NAPRAWDĘ NALEŻY POŚWIĘCIĆ UWAGĘ?

RK: Odpowiedź na to pytanie warto zacząć od zwrócenia uwagi na ilość zasobów, jakimi dysponuje organizacja. Często wraz ze wzrostem obserwowanych incydentów zasoby pozostają na niezmienionym poziomie - zarówno pod względem liczby analityków, jak i systemów, które mają im pomagać. Ja osobiście jestem zwolennikiem automatyzacji w procesie wykrywania incydentów. Uważam, że aspekt ludzki jest potrzebny i konieczny, ale dopiero na etapie, kiedy pojawia się konkretny alert i wiemy, że coś istotnego zagraża organizacji. Automatyzacja świetnie sprawdza się na pierwszej linii frontu, pozwalając analitykom zająć się najtrudniejszymi przypadkami, które wymagają poświęcenia większej uwagi. Oczywiście nie jest bez wad. Idealnie byłoby gdyby alerty generowane przez systemy służące do wykrywania incydentów były odpowiednio skorelowane i trafiały do dalszego opracowania.

PG: JAK DEFINIUJE PAN SUKCES W WYKRYWANIU INCYDENTÓW W ORGANIZACJI?

RK: W mojej organizacji nie posiadamy własnego SOC, korzystamy z usługi zewnętrznej, która stanowi dla nas pierwszą linię obrony. Nie mamy też sztywnych kryteriów oceny, dajemy analitykom dużą swobodę. Są to osoby doświadczone, które dobrze znają organizację, dlatego ufamy ich decyzjom. Dużo rozmawiamy, analizujemy, staramy się wykazywać otwartością i elastycznością, by nic nam nie umknęło. Sytuacja ta wydaje mi się optymalna do rozwoju organizacji, pracujących w niej ludzi, a także do realizacji naszego podstawowego celu - ochrony przed incydentami.



Automatyzacja świetnie sprawdza się na pierwszej linii frontu, pozwalając analitykom zająć się najtrudniejszymi przypadkami, które wymagają poświęcenia większej uwagi.

TREND MICRO CSO COUNCIL

PRACA Z INCYDENTAMI TO NIEUSTANNE ZASKOCZENIA I NAUKA, KTÓRA PRZYCHODZI RAZEM Z NIMI

W tak dużej firmie jak Grupa Allegro incydenty bezpieczeństwa zdarzają się non stop. O tym, ile osób czuwa nad bezpieczeństwem użytkowników, jak testuje się czujność pracowników, a także o specyfice pracy z incydentami rozmawiamy z Michałem Wieruckim, CSO Grupy Allegro.

PRZEMYSŁAW GAMDZYK
ORGANIZATOR CSO COUNCIL

CHCIAŁEM ZAPYTAĆ CZY JAKO CSO W GRUPIE ALLEGRO ŻYJESZ INCYDENTAMI IT NA CO DZIEŃ, CZY TRAFIAJĄ DO CIEBIE TYLKO TE NAJPOWAŻNIEJSZE SPRAWY?

MICHAŁ WIERUCKI

Mówi się, że dzień bez incydentu to dzień stracony (śmiech). Chciałbym podkreślić, że to nie jest tak, że wystarczy mieć dobry dział bezpieczeństwa, aby ich uniknąć. Pewne rzeczy i tak będą się działy, nie mamy wpływu na wszystko. Na co dzień nie zajmuję się już bezpośrednio incydentami, chyba że są naprawdę poważne. Poświęcam im za to dużo uwagi w szerszej perspektywie, m.in. podczas miesięcznych czy kwartalnych statusów, kiedy omawiamy trendy w zakresie zagrożeń.

PG: JAK WIELE OSÓB ZAJMUJE SIĘ INCYDENTAMI W TAK DUŻYM PODMIOCIE, JAKIM JEST ALLEGRO?

MW: W Grupie Allegro nie mamy jednego zespołu, który stricte zajmowałby się incydentami bezpieczeństwa. Mamy dział IT Security który liczy kilkanaście osób i odpowiada za techniczne kwestie w zakresie incydentów. Osobno funkcjonują kilku osobowy zespół skupiony wokół ochrony danych osobowych oraz dodatkowy zespół specjalny, który zajmuje się fraudami, czyli incydentami dziejącymi się na platformie. W organizacji działa również zespół CERT (Computer Emergency Response Team), współtworzony przez wytypowanych specjalistów z wymienionych wcześniej działów, który zajmuje się najbardziej złożonymi, połączonymi incydentami.

PG: PATRZĄC NA TO JAK WIELE MACIE INCYDENTÓW, CZY MOŻNA POWIEDZIEĆ, ŻE LICZBA INCYDENTÓW STALE, GLOBALNIE ROŚNIE?

MW: Dział bezpieczeństwa nie ma wpływu na pojawianie się incydentów - maili phishingowych, malware'u przychodzącego pocztą, fałszywych stron. To na co mamy wpływ to podnoszenie świadomości ludzi - klientów i naszych pracowników. Mając to na uwadze prowadzimy działania edukacyjne i budujemy odpowiednie narzędzia. Robimy wszystko, żeby te podejrzane treści wyłapać, tak by nie trafiały do użytkowników. Wiadomo jednak, że druga strona czasu nie marnuje, stale pojawiają się nowe zagrożenia, przed którymi szukamy ochrony i staramy się ją automatyzować - to ciągła, niekończąca się walka lub, jak kto woli "zabawa". Z naszych obserwacji wynika jednak, że coraz mniej ludzi klika w dziwne maile, co z pewnością jest efektem tych edukacyjnych kampanii.

PG: ZAUWAŻACIE INCYDENTY BARDZIEJ WYRAFINOWANE?

MW: Zdarzają się superphishingi. Szczególnie w dziale finansów, który dostaje maile z prośbą o wykonanie przelewu w imieniu prezesa. Widać, że ktoś sobie zadaje dużo trudu, żeby zbadać nasza strukturę organizacyjną. Ostatnio zauważyliśmy, że na Linkedin zaczęły pojawiać się fałszywe profile związane z Grupą. Niestety część pracowników przyjmowała zaproszenia do sieci znajomych, przez co je uwierzytelniała, jako osoby faktycznie będące w organizacji. Potem profile te wysyłały różne wiadomości i informacje do naszych pracowników. Na szczęście udało nam się wyłapać i zgłosić wszystkie te profile do LI i zostały one usunięte. Widać jednak pewien trend. Pojawia się bardzo dużo działań phishingowych u naszych klientów, szczególnie w zakresie wyłudzania danych do logowania i przejmowania konta, w celu dokonania transakcji. Takie rzeczy cały czas się zdarzają, dlatego staramy się edukować użytkowników i zachęcać do stosowania dwuskładnikowego logowania. Jak mówiłem, to ciągła walka.

PG: WSPOMNIAŁEŚ, ŻE ŚWIADOMOŚĆ UŻYTKOWNIKÓW ROŚNIE. JEŚLI TAK, CZEMU PHISHINGI NADAL SIĘ UDAJĄ?

MW: Obie strony się uczą i podnoszą swój poziom. Z jednej strony zespoły bezpieczeństwa prowadzą działania edukacyjne i pracują nad mechanizmami, a z drugiej odpowiedzialni za ataki, doskonalą siebie i swoje działania. Zadajemy sobie pytanie nie czy, ale kiedy ktoś się złapie. Mi samemu też niestety kiedyś udało się być złapanym, bo wydawało mi się że wszystko jest ok. Czasami, szczególnie w pośpiechu, łatwo uśpić czujność. Przykład? Robiliśmy kiedyś testy wewnętrzne, dzień przed wejściem na giełdę. Część pracowników dostała maila, że może otrzymać bonifikatę na zakupy akcji. Kiedy w grę wchodzą emocje, człowiek jest między jednym a drugim spotkaniem, instynkt samozachowawczy się zagłusza, łatwiej wpaść w pułapkę. Natomiast to jest praca po stronie security - zabezpieczyć w taki sposób, żeby ten mail nie dotarł do odbiorcy. Co istotne, w Allegro staramy się nie karać za to, że ktoś kliknie niebezpieczny link, tylko nagradzać, kiedy tego nie zrobi. Doceniamy drobne kroki w zakresie rosnącej świadomości pracowników i motywujemy do dalszej uważności.

W BEZPIECZEŃSTWIE NIC NIE JEST WAŻNIEJSZE NIŻ CZŁOWIEK

Tysiące klientów biznesowych korzysta z usług cyberbezpieczeństwa Orange Polska. Wśród nich znajdują się największe polskie banki, firmy ubezpieczeniowe, uczelnie oraz samorządy i instytucje publiczne. Zespół cyberbezpieczeństwa Orange Polska odpowiedzialny jest zatem nie tylko za bezpieczeństwo organizacji, ale też dostarczanie usług bezpieczeństwa w kraju i na świecie. Ilu osób potrzeba do realizacji tych działań, kiedy warto pomyśleć o własnej komórce SOC oraz dlaczego maszyny jeszcze długo nie zastąpią ludzi w zakresie zapewniania bezpieczeństwa informatycznego - na te i inne pytania, w rozmowie z Przemysławem Gamdzykiem, Organizatorem CSO Council, odpowiada Przemysław Dęba, Dyrektor Cyberbezpieczeństwa Orange Polska.

PRZEMYSŁAW GAMDZYK
ORGANIZATOR CSO COUNCIL

ZARZĄDZASZ JEDNĄ Z NAJWIĘKSZYCH ORGANIZACJI CYBERSECURITY W POLSCE. ILE OSÓB LICZY TWÓJ ZESPÓŁ?

PRZEMYSŁAW DĘBA

Zacznijmy od tego, że mój zespół odpowiada nie tylko za bezpieczeństwo Orange Polska, ale też za dostarczanie usług do innych firm, także do spółek Grupy poza Polską. Dużą jego część stanowi także rozbudowany CERT. To wszystko wpływa na sporą liczebność naszego teamu. Pracujemy w trybie hybrydowym, co oznacza, że połowę zespołu stanowią etatowi pracownicy Orange Polska, a druga połowa to outsourcing i różnego rodzaju usługi. Łącznie to około stu osób. Jak na polskie realia to dużo, choć są u nas i więksi.

PG: A JEŻELI CHODZI O INCYDENTY - CZY SAMA ICH LICZBA COŚ OZNACZA? CZY JEST TO WSKAŹNIK, KTÓRY MOŻEMY OCENIAĆ SAM W SOBIE I NA JEGO PODSTAWIE MÓWIĆ O POZIOMIE CYBERBEZPIECZEŃSTWA ORGANIZACJI?

PD: Sama liczba incydentów nie świadczy o niczym szczególnym. Może jedynie o tym, jak dużo pracy cała organizacja, nie tylko jednostka bezpieczeństwa, wkłada w ten proces. Nie jest to jednak żadna miara do wykonywania porównań między firmami. Liczba ta jest bowiem uzależniona od tego co chcemy monitorować (czyli od definicji incydentu) i na co chcemy reagować (na jakie zdarzenia, czy tylko zewnętrzne, czy również nieprawidłowe zachowania pracowników itp.).

Drugim czynnikiem jest to, co możemy monitorować - jakimi dysponujemy środkami technicznymi, możliwościami kreatywnego wykrywania incydentów, jaka jest dostępność logów czy systemów, które mogą te logi generować. Z mojego doświadczenia wynika, że organizacje operacji bezpieczeństwa dość intensywnie rozwijają swoje możliwości, co wpływa na generowanie większej liczby alertów, ale jednocześnie optymalizują, zmieniają zakres monitorowania. Reasumując - sama liczba incydentów nie jest dobrą miarą, jeżeli nie ma jakiejś formy klasyfikacji, czy sztywnego punktu odniesienia, na przykład porównania rok do roku.

PG: PRZY ZARZĄDZANIU INCYDENTAMI BARDZO WAŻNE JEST SECURITY OPERATION CENTER. WIEMY JUŻ, ŻE MACIE JEDEN Z NAJWIĘKSZYCH SOC W POLSCE. KIEDY ORGANIZACJA POTRZEBUJE SOC, A KIEDY MOŻE PORADZIĆ SOBIE BEZ NIEGO?

PD: Warto w tym miejscu zarysować potencjalny zakres działania SOC. Przeważnie jest to proaktywne wykrywania zagrożeń, budowanie ich wewnętrznej i zewnętrznej świadomości, często również zarządzanie podatnościami. Działania te są silnie skorelowane ze świadomością posiadanych i chronionych środków, w zakresie infrastruktury i software oraz źródeł danych, czyli z log managementem (red: kolekcjonowanie i przetwarzanie logów z systemów). Warto zauważyć, że w zasadzie każda organizacja, która jakkolwiek zarządza swoją infrastrukturą i aplikacjami, również realizuje te funkcje. Przeważnie są to działania rozproszone, niewidoczne i nie współpracujące ze sobą w odpowiedni sposób.

Kluczowy jest moment, kiedy organizacja zaczyna być świadoma ryzyk związanych cyberbezpieczeństwem dla swojego biznesu. Jeśli chce nimi zarządzać w bardziej transparentny sposób, poprzez scentralizowanie wiedzy i kompetencji oraz operacjonalizację procesów, wówczas tworzy się odrębną, własną jednostkę operacji bezpieczeństwa SOC. Jest to kwestia decyzji biznesowej podejmowanej przez organizację.

TREND MICRO

CSO COUNCIL