Prawda czy fałsz?

Miażdżymy mity o cyberbezpieczeństwie

Kiedy dynamicznie zmienia się krajobraz zagrożeń, a do gry regularnie wchodzą nowe technologie, zarządzanie bezpieczeństwem musi ewoluować co najmniej w tym samym tempie.

Eksperci NTT i CISCO usiedli przy filiżance kawy, aby podzielić się wiedzą: w jaki sposób postawy dostawców technologii, biznesu i klientów wpływają na postrzeganie kwestii bezpieczeństwa w dobie przyspieszonej cyfrowej transformacji? Co jest prawdą, a co fikcją?

Przedstawiamy najważniejsze wnioski z tej inspirującej rozmowy

2 ekspertów ds. bezpieczeństwa

4 pozornie bezsporne tezy

wiele nieoczywistych odpowiedzi

Prawda czy fałsz?:

Tradycyjne zabezpieczenia sieciowe są martwe.

FAŁSZ

Ludzie mają postrzegają kwestiie bezpieczeństwa w tradycyjny sposób. Wystarczy coś ustawić, skonfigurować i można o tym zapomnieć. A takie podejście już nie działa. Trzeba na bieżąco dopasowywać swoje strategie bezpieczeństwa do zmieniającego się otoczenia biznesowego.

Kwestie związane z bezpieczeństwem nieustannie idą do przodu, ewoluują, zmieniają się. Obszar ten jest z pewnością inny, niż nawet jeszcze kilka lat temu. Wszystko dlatego, że krajobraz zagrożeń staje się w pewnym sensie uproszczony, a złośliwe oprogramowanie coraz skuteczniejsze w swojej podstawowej zasadzie działania – kod po prostu ma dostać się do środka sieci, przejąć kontrolę na urządzeniem i zrobić to, do czego zostało stworzony. Jednocześnie bezpieczeństwo sieci musi być coraz bardziej wyrafinowane - trzeba zrozumieć, które systemy ze sobą rozmawiają i co z tego wynika.

Obrona sieci musi być wystarczająco silna, aby poradzić sobie z 95% podstawowych zagrożeń. Identyfikacja i szybka reakcja na pozostałe 5% zagrożeń pochłania zaś połowę budżetów na zabezpieczenia.

Nic dziwnego, że budżety na bezpieczeństwo rosną. Obecnie strategie biznesowe są znacznie ściślej powiązane z bezpieczeństwem, niż kiedykolwiek wcześniej. Na szczęście zarządy firm coraz lepiej rozumieją potrzebę inwestycji w bezpieczeństwo.

> **Dlatego obalamy pierwszy mit i mówimy FAŁSZ. Tradycyjne zabezpieczenia sieciowe są nadal bardzo ważne, choć nie należy zapominać o nieustannej ewolucji sieci. Kiedyś znajdowała się w jednym miejscu, a teraz jest rozproszona po całym świecie. Ewolucja jest fantastyczna, ale firmy muszą nauczyć się iść do przodu w bezpieczny sposób, stosując coraz bardziej wyrafinowane zabezpieczenia.**

Prawda czy fałsz?:

Więcej pieniędzy zainwestowanych w cyberbezpieczeństwo jest lekarstwem na wszystkie nasze problemy

FAŁSZ

Nie ulega wątpliwości, że firmy muszą przeznaczać coraz więcej środków na bezpieczeństwo, ale nie mogą tego robić bez dogłębnych analiz, a później oczekiwać, że wyższe budżety rozwiążą wszystkie ich problemy. Bezpieczeństwo zaczyna się od strategii, technologii i ludzi.

Nakłady na bezpieczeństwo systematycznie rosną. Warto zastanowić się, czy w przeszłości pieniądze były wydawane we właściwy sposób czy dopiero teraz koncentrujemy się na obszarach, które wymagają inwestycji? Zamiast kierować środki głównie na tradycyjne zabezpieczenia, organizacje powinny finansować także rozwiązania, które pozwolą im reagować na zdarzenia już w momencie powstawania incydentów.

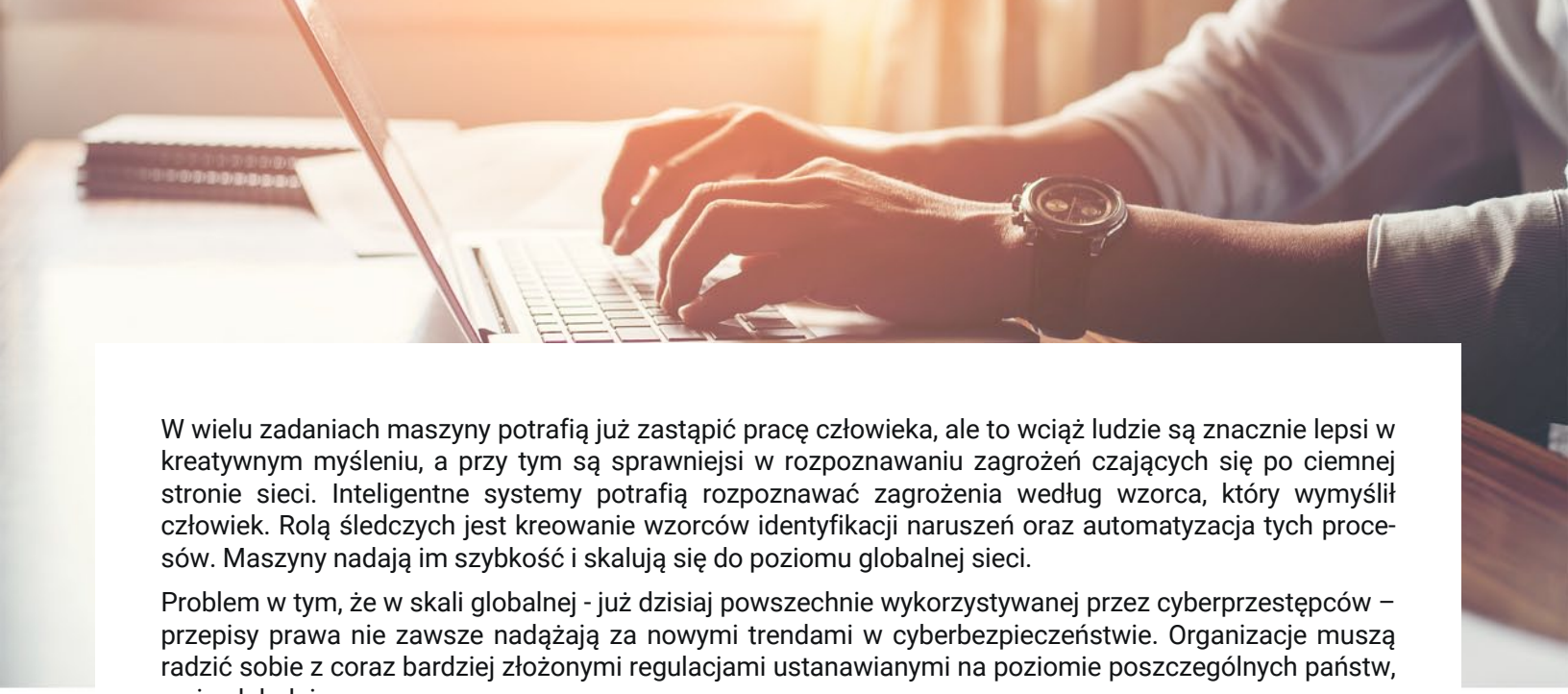
Obecnie, typowe naruszenie zabezpieczeń odkrywane jest przeciętnie dopiero po 160 dniach. To czas, kiedy dajemy atakującemu możliwość wyrządzenia istotnych szkód. W pożądanym scenariuszu, każdy incydent powinien zostać zidentyfikowany i opanowany nie później niż w 24 godziny od momentu jego pojawienia się w sieci.

Prawda czy fałsz?
Miażdżymy mity o cyberbezpieczeństwie.

Remedium na te bolączki jest globalna sieć Cisco, która działa jak gigantyczny sensor. Każdego dnia Cisco zbiera nawet 4 TB danych pochodzących ze 170 krajów, które pozwalają wykryć, że coś niepokojącego dzieje się w sieci, a później odpowiednio zareagować w skali globalnej. Można też skorzystać z gotowych podpowiedzi, na co zwracać uwagę. Np. raz w miesiącu, analitycy NTT przygotowują raport o najnowszych zagrożeniach, metodach ataku czy odkrytych lukacj bezpieczeństwa. Słowem – dają narzędzia pomagające odnaleźć igłę w stogu siana.

Trzy rady, które możesz wdrożyć już dziś

1. Bądź przewidujący. Praca w modelu hybrydowym: trochę z biura, trochę z domu, a trochę z kawiarni będzie nam towarzyszyć w najbliższych latach. Upewnij się, że Twoje systemy są na to gotowe.
2. Projektuj rozwiązania dla ludzi. Jeśli będą intuicyjne i łatwe do zastosowania, użytkownicy nie będą starali się ich omijać.
3. Automatyzuj powtarzalne procesy bezpieczeństwa, a swój czas przeznacz na zajmowanie się niestandardowymi zagrożeniami i ich szybką mitygacją.



W wielu zadaniach maszyny potrafią już zastąpić pracę człowieka, ale to wciąż ludzie są znacznie lepsi w kreatywnym myśleniu, a przy tym są sprawniejsi w rozpoznawaniu zagrożeń czających się po ciemnej stronie sieci. Inteligentne systemy potrafią rozpoznawać zagrożenia według wzorca, który wymyślił człowiek. Rolą śledczych jest kreowanie wzorców identyfikacji naruszeń oraz automatyzacja tych procesów. Maszyny nadają im szybkość i skalują się do poziomu globalnej sieci.

Problem w tym, że w skali globalnej - już dzisiaj powszechnie wykorzystywanej przez cyberprzestępców – przepisy prawa nie zawsze nadążają za nowymi trendami w cyberbezpieczeństwie. Organizacje muszą radzić sobie z coraz bardziej złożonymi regulacjami ustanawianymi na poziomie poszczególnych państw, a nie globalnie.

Przykładem mogą być europejskie regulacje RODO, które okazały się dużym kosztem dla biznesu. RODO dało impuls do skupienia się na kilku dotychczas niedocenianych rzeczach oraz zmianie sposobu myślenia o przepisach związanych z prywatnością. Ich wdrożenie z pewnością ułatwi przygotowanie się do regulacji nadchodzących z innych części świata.

> **Większe inwestycje niekoniecznie więc zapewnią nam większe bezpieczeństwo. Ważniejsze od zwiększania nakładów jest upewnienie się, że środki wydawane są we właściwy sposób. Kultura organizacji i budowanie świadomości w ludziach powinny być częścią dobrej strategii biznesowej i strategii bezpieczeństwa.**

Prawda czy fałsz?:

Zespoły ds. bezpieczeństwa będą musiały zmienić sposób, w jaki pracują

PRAWDA

Technologia cyfrowa wymusza jawność i transparentność, a osoby odpowiedzialne za bezpieczeństwo nabyły nowe umiejętności. Teraz zespoły ds. bezpieczeństwa muszą zmienić styl i sposób pracy.

Bezpieczeństwo to pasjonujący obszar. Można więc oczekiwać, że ludzie, którzy się nim zajmują, będą bardzo otwarci i chętnie będą dzielili się pomysłami z resztą organizacji, aby pozwolić firmie dynamicznie się rozwijać. Konieczne jest jednak zmotywowanie zespołów ds. bezpieczeństwa, aby były gotowe na zmiany, chciały dostosowywać się do biznesu i innych pracowników. W przeszłości można było dostrzec niechęć do dzielenia się wiedzą na temat bezpieczeństwa, dzisiaj jest to krytyczny czynnik dla zdolności organizacji do wejścia w cyfrowy świat. Przejawem kultury bezpieczeństwa jest również przekazywanie najlepszych praktyk i aktualizowanych instrukcji działania.

Co więcej, zespoły ds. bezpieczeństwa muszą pozyskać nowe umiejętności (np. w dziedzinie programowania), aby pomóc w budowie systemów i aplikacji, z których ludzie będą mogli w pełni bezpiecznie korzystać.

Ważną rzeczą jest również sposób, w jaki budujemy partnerstwa wewnątrz i na zewnątrz firmy. Współpraca Cisco i NTT stanowi doskonały przykład partnerstwa, w którym obie organizacje dostrzegają wyzwania i wymieniają się wiedzą i kompetencjami oraz potrafią czerpać inspiracje z różnorodności doświadczeń i punktów widzenia swoich pracowników. Z perspektywy bezpieczeństwa podejście to wzmacnia wszystkich, zaś samo partnerstwo jest kluczowe dla sukcesu biznesowego i korzyści dla klientów.

> **Nie tylko zespoły ds. bezpieczeństwa, ale wszyscy pracownicy organizacji muszą zmienić podejście do bezpieczeństwa. Dział bezpieczeństwa musi dzielić się wiedzą, zdobywać nowe umiejętności oraz ściślej integrować się z modelem biznesowym danej organizacji.**

Prawda czy fałsz?:

Możemy przyzwyczaić wszystkich użytkowników do stosowania się do tych samych procedur bezpieczeństwa.

FAŁSZ

Kiedy zmienia się krajobraz zagrożeń, modele biznesowe wymagają szybkiego dostosowania się do otoczenia, a zmiany te zachodzą prawdopodobnie szybciej, niż kiedykolwiek wcześniej. Transformacji musi podlegać również nasze podejście do bezpieczeństwa.

Na przestrzeni lat bezpieczeństwo stało się tematem dyskusji na poziomie najwyższego kierownictwa organizacji, częścią krótko- i długoterminowych strategicznych planów, a w rezultacie zaczęło wpływać na sukces biznesowy firm. Problem w tym, że bezpieczeństwo musi zmieniać się w tym samym tempie, a może nawet trochę szybciej, niż modele biznesowe. Z uwagi na szybko ewoluujące technologie, próba zdefiniowania długoterminowej strategii bezpieczeństwa może spełznąć na niczym.

Zadaniem dobrego lidera ds. bezpieczeństwa jest stworzenie różnorodnego zespołu złożonego z młodych i starszych pracowników. Tak jak w gotowaniu, posiłek smakuje naprawdę dobrze dopiero, gdy uda nam się połączyć wszystkie właściwe składniki. Łącząc różne perspektywy i umiejętności pracowników, stworzymy najlepszy zespół do walki z obecnymi i przyszłymi zagrożeniami.

Przykład: coraz większy wpływ na funkcjonowanie organizacji mają millenialsi. Młodzi ludzie wnoszą do firmy świeży sposób myślenia, inny sposób współpracy, a nawet odmienne podejście do biznesu. Millenialsi mają fantastyczne umiejętności współpracy, są bardziej inkluzywni i chętniej dzielą się informacjami.

> **Zmiana krajobrazu zagrożeń i modeli biznesowych wymusza nieustanną zmianę w podejściu do spraw bezpieczeństwa. Jeśli oczekujemy poprawy bezpieczeństwa musimy nieustannie zmieniać sposób w jaki nad nim pracujemy, również przez pozyskiwanie umiejętności ludzi młodego pokolenia.**

NTT | CISCO