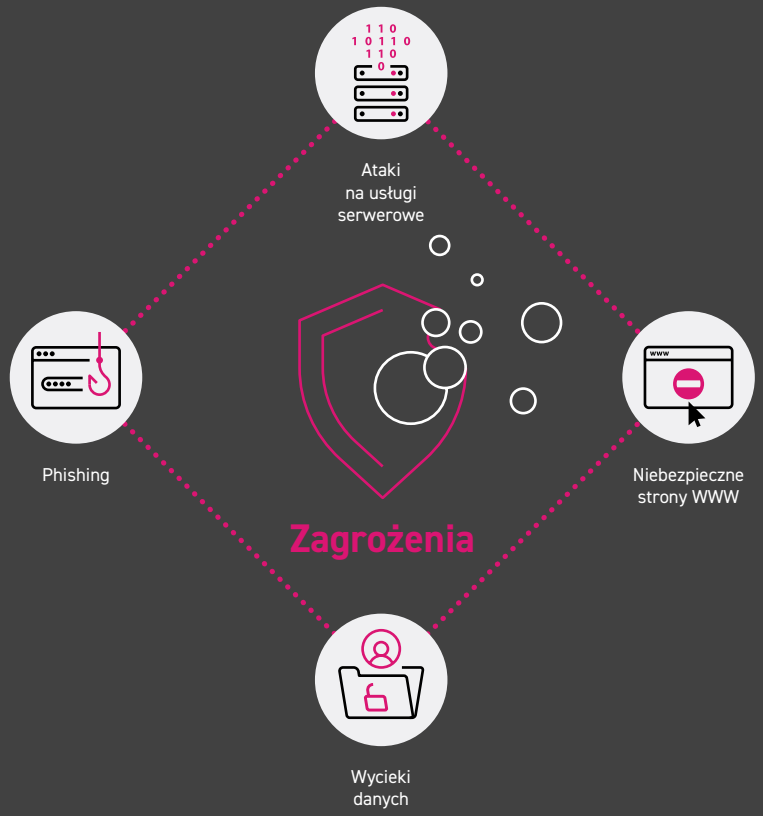
CHECK POINT DLA **SEKTORA FINANSOWEGO**



Jak chroni Check Point

Ataki typu wolumenowego

Dzięki zastosowanej analizie ruchu, firewalle firmy Checkpoint potrafią szybko i skutecznie wykryć atak typu DDoS blokując niepożądane zapytania. Takie działania dają szansę utrzymania działania usług wystawionych dla naszych klientów przy jednoczesnym odfiltrowaniu połączeń, których jedynym celem jest zablokowanie naszej usługi.

Niebezpieczne linki

Najpopularniejszym atakiem w ostatnich latach jest phishing. Atak wykonywany jest za pomocą poczty email, linków przesłanych przez komunikatory czy dostarczonych wraz z plikami. Rozwiązania Check Point potrafią zareagować na przesyłane pliki z zagrożeniami jak i zablokować wykonanie operacji otwarcia połączenia z zainfekowaną stacją, chroniąc nieświadomego użytkownika przed wykradzeniem jego cennych danych.

Wycieki danych i naruszenia RODO w wyniku ataku

Najpopularniejszym atakiem w ostatnich latach jest phishing. Atak wykonywany jest za pomocą poczty email, linków przesłanych przez komunikatory czy dostarczonych wraz z plikami. Rozwiązania Check Point potrafią zareagować na przesyłane pliki z zagrożeniami jak i zablokować wykonanie operacji otwarcia połączenia z zainfekowaną stacją, chroniąc nieświadomego użytkownika przed wykradzeniem jego cennych danych.

Blokowanie niepożądanych witryn

Często spotykamy się z sytuacją gdzie pracownicy, nieświadomie otwierają linki do strony zagrażające ich bezpieczeństwu. Inni pracownicy, już w pełni świadomie, korzystają z internetu celem zapewnienia sobie rozrywki w pracy. Oba problemy w łatwy i wygodny sposób rozwiązuje filtrowanie ruchu WWW oraz kontrola wykorzystywanych aplikacji, dzięki której obniżymy ryzyko ataku oraz zwiększymy produktywność pracowników.

Jakie funkcje Cię chronią?

IPS · Analiza ruchu · AV · Sandbox · Antibot · URL Filtering · SSL Interception · DLP · Content Awareness

Model	1530	1550	1570	1590	1600	1800
Sugerowana ilość użytkowników	5	10	25	50	100	150
Przepustowość Gen V	340Mbps	450Mbps	500Mbps	660Mbps	1.5Gbps	2Gbps
Przepustowość Gen II	1Gbps	1Gbps	2.8Gbps	2.8Gbps	4.8Gbps	7.5Gbps
Ilość interfejsów/WiFi	6x1GB/Opcja	6x1GB/Opcja	10x1GB/Opcja	10x1GB/Opcja	18x1GB/Nie	18x1GB 2x2.5GB

Ransomware – jest to rodzaj ataku, którego głównym celem jest uniemożliwienie dostępu do danych (np. dowolnych plików w komputerze). Dostęp do danych jest niemożliwy z uwagi na to, że w wyniku ataku dane zostają zaszyfrowanie, a atakujący żąda okupu w celu ich odszyfrowania. Najczęściej żądanie okupu dotyczy krypto waluty i jest ograniczone czasem, po którym dane zostają bezpowrotnie utracone, albo upublicznione.

Firewall/UTM – system komputerowy, którego celem jest monitorowanie oraz kontrolowanie połączeń pomiędzy różnymi sieciami komputerowymi (najczęściej wewnętrzną siecią LAN, a zewnętrzną siecią Internet). Typowy firewall składa się z zestawu reguł i polityk, które dają bądź blokują możliwość komunikacji pomiędzy tymi sieciami. Najbardziej zaawansowane firewalle (tzw. NextGen Firewall) posiadają szereg innych funkcji/modułów (np. AntiVirus, AntiBot, URL Filtering, SSL Inspection, IPS, i wiele innych) dlatego też często określa się je mianem Unified Threat Management (UTM).

IT – Informational Technology (IT) skupia się na zapewnieniu komunikacji oraz dostępu do danych pomiędzy aplikacjami, serwerami, komputerami i urządzeniami sieciowymi wraz z zabezpieczeniem tych zasobów z punktu widzenia bezpieczeństwa sieciowego.

OT – Operational Technology (OT) to wszelkie urządzenia, systemy, procesy oraz oprogramowanie związane z zarządzaniem oraz monitorowaniem urządzeń przemysłowych (np. maszyn produkcyjnych, pomp, kontrolerów PLC, urządzeń kolejowych, sygnalizacji świetlej, i wielu innych). Świat OT w odróżnieniu od świata IT rządzi się własnymi normami i protokołami (np. Modbus, Profinet, S7, EtherNet), a zatem potrzebuje innych narzędzi do zapewnienia bezpieczeństwa niż te znane ze świata IT. Odpowiednie zabezpieczenie OT w dużym stopniu jest krytyczne z punktu widzenia funkcjonowania przedsiębiorstwa, miasta, kraju.

Botnet – jest to sieć połączonych ze sobą komputerów, które najczęściej zarządzane są z jednego centralnego miejsca (tzw. C&C - Command and Control), powstała w celu przeprowadzania skoordynowanych ataków sieciowych. Każdy pojedynczy komputer (bot lub też często nazywany zombie) bezwiednie wykonuje zadanie zlecone z C&C. Główną bronią w arsenale botnetu jest liczba botów - im jest ich więcej tym większe oddziaływanie botnetu. Nierzadko sieć botnet składa się z kilkuset, a nawet kilku bądź kilkuset tysięcy komputerów, które niczym jeden organizm atakują ofiarę.

IPS/IDS – Intrusion Prevention Systems (IPS) oraz Intrusion Detection Systems (IDS) są to rozwiązania zarówno sprzętowe, jak i programowe, których głównym celem jest wykrywanie i blokowanie wszelkich anomalii sieciowych i niepożądanych aktywności w sieci, które mogłyby prowadzić do zagrożenia. Systemy IDS służą do wykrycia zagrożenia, a systemy IPS do jego zablokowania.

Cyberatak – jest to atak wycelowany najczęściej na system komputerowy lub sieć komputerową. Tego typu atak wykonują osoby, które nazywamy hakerami. Hakerzy w tym celu stosują wyrafinowane narzędzia oraz aplikacje komputerowe (malware, ransomware, exploit).

Sandboxing – jest to odizolowane środowisko, w którym można uruchomić kod i obserwować jaki będzie miał wpływ na to środowisko. W ten sposób można w bezpieczny sposób zidentyfikować niebezpieczne oprogramowanie, które na przykład będzie wykonywało destrukcyjne zmiany w systemie operacyjnym, zmieniało zawartość plików systemowych, łączyło się z niebezpiecznymi adresami IP, itp. Przez to, że wspomniany kod uruchomiony jest w odizolowanym środowisku, nie ma on wpływu na środowisko produkcyjne, stąd nie ma niekorzystnego impaktu na bezpieczeństwo.

Phishing – jest to zagrożenie polegające na podszywaniu się pod inną osobę bądź organizację w celu wyłudzenia poufnych informacji (np. danych osobowych, numerów kart kredytowych, danych autoryzacyjnych, itp.). Pod tym pojęciem można zaklasyfikować wszelkie czynności, które służą do nakłonienia do udostępnienia tych danych. Najczęściej z tego typu atakami można się spotkać na stronach internetowych, które do złudzenia przypominają inne popularne strony (np. banki, portale aukcyjne, portale społecznościowe).

VPN – Virtual Private Network (VPN) jest to tunel sieciowy, który w bezpieczny sposób zapewnia komunikację pomiędzy nadawcą i odbiorcą za pomocą publicznych środków komunikacji (np. Internet). Najczęściej tego typu rozwiązanie stosuje się w celu połączenia ze sobą odległych od siebie oddziałów firmy, albo zapewnienia dostępy do wewnętrznych sieci pracownikom zdalnym. Komunikacja wewnątrz VPN gwarantuje poufność, integralność oraz dostępność - czyli główne filary bezpieczeństwa informacji wg normy ISO27001.

Adware/Malware/Trojan/Wirus/Worm – najczęściej pod tymi terminami określamy niebezpieczne bądź niepożądane oprogramowanie komputerowe. Głównym celem Adware jest wyświetlanie niepożądanych treści, wykonywanie przekierowań na niepożądane witryny internetowe, zbieranie danych. Malware to szerokorozumiane oprogramowanie charakteryzujące się niebezpiecznym zachowaniem. Trojan to oprogramowanie, które pomimo tego, że wygląda na użyteczne, ma ukryte często niebezpieczne inne funkcjonalności i mechanizmy. Wirus to oprogramowanie komputerowe, które jest ukryte i replikuje się na komputerze ofiary w celu zaatakowania innych programów. Worm (robak) jest bardzo podobny do wirusa. Główną różnicą pomiędzy nimi jest to, że wirus wymaga nosiciela (np. plik wykonywalny), którego uruchomienie aktywuje wirusa. Robak jest pod tym względem samodzielny (nie potrzebuje nosiciela) i jest niejako ewolucją wirusa. Często robaki rozprzestrzeniają się poza komputer, wysyłając swoje kopie do innych komputerów w sieci poprzez pocztę elektroniczną.

Exploit – jest to fragment oprogramowania komputerowego, fragment danych, zestaw komend, itp. gdzie głównym celem jest wykorzystanie błędu w oprogramowaniu (tzw. bug). Atakujący wiedząc o błędzie w oprogramowaniu wykorzystuje go w celu uzyskania dostępu do danych, kontroli nad komputerem, podniesienia uprawnień, itp.

DoS/DDoS – Denial-of-Service (DoS) jest to atak, którego głównym celem jest uniemożliwienie dostępu do zasobów. Atak polega na wykonywaniu wielu połączeń sieciowych (flood) najczęściej z wielu różnych źródeł (Distributed DoS - DDoS) w tym samym czasie do komputera ofiary. W ten sposób atakujący może skutecznie uniemożliwić dostęp do zasobów innym użytkownikom wskutek wysycenia zasobów, co może skutkować realnymi stratami finansowymi.

URL Filtering/Application Control – wiele ataków sieciowych rozprzestrzenia się na stronach internetowych. Poza tym w obecnych czasach istnieje wiele różnych stron internetowych oraz aplikacji sieciowych, które mogą mieć niekorzystny wpływ na organizację, nie tylko z punktu widzenia bezpieczeństwa, ale również np. produktywności pracowników. Dzięki filtrowaniu tego do jakich stron internetowych oraz aplikacji sieciowych ma być dostęp, a do jakich takiego dostępu nie ma być organizacje mogą sobie poradzić z tego typu zagrożeniami. To zapewniają mechanizmy URL Filteringu oraz Application Control, które uwzględniają zarówno komunikację niezaszyfrowaną, jak i tą zaszyfrowaną.

CLICO Sp. z o.o.
ul. Oleandry 2, 30-063 Kraków
Informacje i pomoc techniczna: ps@clico.pl
www.clico.pl, **www.checkpoint.clico.pl**