Cyberbezpieczeństwo 2024: Praktyczne podejście do ochrony systemów

Pierwszym błędem w oprogramowaniu, który przeszedł do historii... Była ćma. Grace Hooper pracująca przy komputerze Harvard Mark II znalazła ją niczego nie podejrzewającą, że powoduje... awarię systemu. Był to pierwszy historyczny przypadek znalezienia BUGA. Czyli inaczej w tłumaczeniu pluskwy, robaka. Komputer, w którym znaleziono 9 września 1947 roku sławną ćmę, był elektromechaniczną maszyną do obliczania torów lotów rakiet.

Stopniowo organizacje na całym świecie otrzymują wymaganie zgłaszania luk w zabezpieczeniach. Wymóg ten szczególnie dotyka sektory technologiczne, finansowe oraz instytucje publiczne, gdzie ochrona danych wrażliwych jest priorytetem. Firmy z branży IT, bankowość oraz organizacje rządowe muszą nieustannie monitorować swoje systemy, aby zapobiegać potencjalnym naruszeniom. W Stanach Zjednoczonych wymaganie to zostało formalnie uznane 19 maja 2022 roku, kiedy Departament Sprawiedliwości oficjalnie poinformował, że jeżeli

ktoś w dobrej wierze przeprowadza badanie nad bezpieczeństwem komputerowym, nie będzie ścigany jako przestępca. W 2024 roku senat USA uchwalił ustawę o redukcji podatności na bezpieczeństwo cybernetyczne. Zaleca ona proaktywną identyfikację luk w oprogramowaniu. Postawa ta uległa zmianie między innymi dzięki korzystaniu przez Amerykański Pentagon z programów Bug Bounty. 10 listopada 2017 roku nagłówki amerykańskiej prasy informowały "Pentagon otworzył się na hakerów - i naprawił tysiące błędów". Wówczas jeszcze Ustawa o oszustwach i nadużyciach komputerowych powodowała, że rząd Stanów Zjednoczonych Ameryki nie bardzo dogadywał się z hakerami, a jednak coś uległo zmianie. Musiało się zresztą zmienić, z uwagi na to, że świat coraz bardziej zaczynał rozumieć, jak działa cyberbezpieczeństwo.

Tymczasem w Polsce... Znaleźliśmy się na drugim miejscu w Europie pod względem liczby firm, w których cyfrowe bezpieczeństwo było w jakiś sposób naruszone. Wysoka pozycja Polski w tej statystyce wynika między innymi z dynamicznego rozwoju sektora IT, a także z rosnącej liczby małych i średnich przedsiębiorstw, które często nie dysponują odpowiednimi zasobami na kompleksowe zabezpieczenia. Dodatkowo niski poziom świadomości zagrożeń cybernetycznych wśród pracowników oraz ograniczone budżety na bezpieczeństwo w wielu organizacjach przyczyniają się do zwiększonego ryzyka naruszeń. Pracownicy w sposób naturalny oczekują, że kierownictwo wyższego szczebla będzie świadome zagrożeń. Technologia rozwija się, narzędzia komunikacyjne są coraz istotniejsze z perspektywy zarządzania organizacją. Cyberprzestępcy wykorzystują tę słabość, by ingerować w operacje biznesowe, kraść poufne dane oraz powodować straty pieniężne. Stan niezagrożenia nie oznacza jedynie braku zagrożenia, ale także szereg działań konceptualnych, organizacyjnych i analitycznych w celu przewidzenia i zapobiegania potencjalnym niebezpieczeństwom. Zarządzającym powinno zależeć na poczuciu bezpieczeństwa wśród interesariuszy. Integralność systemów własnościowych w instytucjach międzynarodowych jest coraz bardziej zagrożona. Nie tak dawno najprawdopodobniej chińscy hakerzy wykorzystali lukę w zabezpieczeniach systemów Beyond Trust, zewnętrznego dostawcy usług cyberbezpieczeństwa, celem uzyskania dostępu do niesklasyfikowanych dokumentów skarbowych Departamentu Skarbu USA. Odpowiedzią może być każde ulepszenie w infrastrukturze klucza publicznego (PKI).

Infrastruktura ta jest w istocie rzeczy układem, który wiąże klucze z odpowiednimi tożsamościami podmiotów. Powiązaniami tymi zarządza organ certyfikacji, rejestrując i wydając certyfikaty. Całość

odbywa się albo przy udziale ludzi, albo w sposób zautomatyzowany. W przypadku sieci komputerowej niezbędny jest odpowiedni CMP, czyli protokół zarządzania certyfikatami. Całość musi być odpowiednio zarządzana również w Internecie Rzeczy (IoT). Protokół Zarządzania Certyfikatami jest standaryzowany przez IETF – organizację normalizującą dla Internetu, odpowiadającą za standardy techniczne tworzące pakiet protokołów TCP/IP. Najnowsza wersja CMP, to CMP2021 (3). Odpowiednie informacje można znaleźć w dokumencie RFC 9480 z listopada 2023 roku. Z kolei w RFC 9481 znajduje się opis algorytmów dla tego protokołu. Natomiast RFC 9482 opisuje protokół klient-serwer podobny do HTTP, używany przez różne urządzenia w przestrzeni Internetu Rzeczy w powiązaniu z dwoma poprzednimi dokumentami.

Po co taka otwartość i czy nie jest to kuszenie losu? Interfejsy systemu powinny funkcjonować w pełnej zgodności, współpracując z innymi produktami lub systemami, które już istnieją, bez ograniczania możliwości implementacji lub dostępu. Z jednej strony pozwalają to na szybsze wprowadzanie innowacji, łatwiejszą współpracę między różnymi systemami i zwiększenie przejrzystości, co wzmacnia zaufanie do stosowanych technologii. Z drugiej jednak, niesie za sobą ryzyko nadużyć przez osoby o złych intencjach, które mogą wykorzystać publicznie dostępne specyfikacje do identyfikacji słabych punktów w zabezpieczeniach.

Dlatego konieczne jest znalezienie równowagi między otwartością a bezpieczeństwem. Transparentność powinna być wspierana przez rygorystyczne procedury testowania, monitorowania i aktualizowania standardów oraz systemów. Odpowiednie mechanizmy takie jak programy Bug Bounty, wsparcie społeczności badaczy i inwestycje w edukację użytkowników mogą skutecznie ograniczyć ryzyko, jednocześnie korzystając z zalet otwartych rozwiązań. Składniki systemu muszą móc wymieniać się informacjami, wykorzystywać dane oraz wykonywać programy i przesyłać dane między jednostkami. Korzystać z nich mają osoby, również takie, które posiadają jedynie małą lub żadną wiedzę techniczną. Otwarte standardy są fundamentem współczesnej technologii, umożliwiając interoperacyjność i dynamiczny rozwój globalnych systemów.

Powszechnie dostępne standardy to fundament globalnej sieci. Z jednej strony prowadzenie transparentnej polityki pozwala na analizę i weryfikację, zwiększając tym samym bezpieczeństwo i niezawodność. Z drugiej jednak zapewnia dostęp dla potencjalnych atakujących. Publicznie dostępna specyfikacja może ułatwić osobom o złych intencjach identyfikację oraz użycie luk bezpieczeństwa. Niedawny atak

na Departament Skarbu USA mógł wiązać się z kradzieżą klucza używanego przez dostawcę do zabezpieczenia usługi opartej na chmurze, wykorzystywanej do zdalnego zapewnienia wsparcia technicznego pracownikom. W ten sposób hakerzy obeszli zabezpieczenia usługi, uzyskując dostęp do stacji roboczych pracowników.

W 1995 roku firma Netscape wdrożyła program bug bounty, oferując nagrody finansowe programistom, którzy znaleźli i zgłosili błędy bezpieczeństwa. Dotyczy to sytuacji zgoła odmiennej od opisanej przed chwilą, ponieważ problem Departamentu Skarbu USA dotyczył błędu ludzkiego. Nawet jeśli jednak wszyscy pracownicy bezustannie spisywaliby się na medal pod względem stosowania zasad bezpieczeństwa, może to po prostu nic nie dać, jeśli system sam w sobie posiada wady związane z bezpieczeństwem.

W roku 2024 komputer stał się nieodłącznym elementem naszej codzienności. Tradycyjne narzędzia pracy, takie jak segregatory, maszyny do pisania czy nawet notatniki, powoli odchodzą w zapomnienie. Współczesny pracownik jest swoistą maszyną biurową, w której centrum znajduje się komputer – narzędzie produktywności, ale również potencjalne źródło zagrożeń. Jednak relacja między użytkownikami a technologią, choć niezbędna, nie jest wolna od problemów.

Centra operacyjne bezpieczeństwa jako tarcza ochronna

W obliczu rosnącej liczby zagrożeń cybernetycznych organizacje wdrażają rozwiązania, które mają na celu ochronę ich infrastruktury IT. Kluczową rolę odgrywają tu SOC (Security Operations Centers) – centra operacyjne bezpieczeństwa, które monitorują, analizują i reagują na incydenty bezpieczeństwa w czasie rzeczywistym. Ich celem jest zapewnienie ciągłości działania systemów informatycznych oraz minimalizowanie skutków potencjalnych ataków. Wiele rządów również aktywnie angażuje się w inicjatywy mające na celu ochronę obywateli i instytucji przed zagrożeniami cybernetycznymi.

Nowe zagrożenia – infostealery na celowniku

Jednym z bardziej popularnych rodzajów zagrożeń w 2024 roku jest oprogramowanie typu infostealer. Jego celem jest kradzież danych, takich jak hasła, dane kart płatniczych czy poufne informacje przechowywane w systemach użytkowników. Jednym z najczęściej wykorzystywanych wektorów ataku są wiadomości e-mail, w szczególności te, które zawierają złośliwe załączniki lub linki. Użytkownicy systemu Windows, z racji jego popularności, są szczególnie narażeni na tego typu zagrożenia.

Przykłady znanych infostealerów

Jednym z przykładów infostealerów jest Lumma, oprogramowanie, które skutecznie wykrada dane z zainfekowanych systemów. Na szczęście wiele tego typu programów może zostać zablokowanych przez aktualizowane na bieżąco oprogramowanie antywirusowe lub system operacyjny. Jednakże cyberprzestępcy nieustannie dostosowują swoje metody, aby obejść zabezpieczenia. Dlatego tak ważne jest monitorowanie aktywności sieciowej i analiza logów systemowych.

Dlaczego logi są kluczowe?

Logi sieciowe są jednym z najważniejszych narzędzi w walce z zagrożeniami. Pozwalają one na śledzenie ruchu w sieci, identyfikowanie nietypowych zdarzeń oraz reagowanie na potencjalne ataki. Rozpocząłem pracę nad rejestracją logów sieciowych w systemie Windows 11, aby lepiej zrozumieć, jak można wykorzystać te dane do ochrony przed zagrożeniami.

Jak skonfigurować logowanie zdarzeń zapory w systemie Windows 11?

Oto kroki, które podjąłem, aby włączyć rejestrowanie logów zapory w systemie Windows 11:

1. Włącz rejestrowanie zdarzeń zapory

Otwórz ustawienia zapory systemu Windows: wyszukaj "Zapora systemu Windows" w menu startowym i uruchom narzędzie.

Przejdź do właściwości zapory: kliknij prawym przyciskiem na "Zapora systemu Windows z zaawansowanym zabezpieczeniem (lokalne)" i wybierz Właściwości.

W zakładkach Profil domeny, Profil prywatny i Profil publiczny w sekcji Logowanie ustaw:

- Logowanie odrzuconych pakietów: Tak.
- Logowanie dozwolonych połączeń: Tak (opcjonalnie).
  - Kliknij Przeglądaj, aby określić lokalizację pliku logów (np. `%SystemRoot%\System32\LogFiles\Firewall\pfirewall.log`).

Kliknij OK.

2. Upewnij się, że usługa zapory działa

Otwórz Menedżer usług: naciśnij Win + R, wpisz `services.msc` i naciśnij Enter.

Znajdź usługę Zapora systemu Windows Defender.

Upewnij się, że jej stan to "Uruchomiona", a typ uruchamiania ustawiony na "Automatyczny".

3. Sprawdź uprawnienia w Podglądzie zdarzeń

Otwórz Podgląd zdarzeń.

Kliknij prawym przyciskiem myszy na dziennik, który chcesz włączyć (np. "Zabezpieczenia połączeń").

Wybierz Właściwości i upewnij się, że dziennik nie jest wyłączony.

Kliknij Włącz dziennik, jeśli opcja jest dostępna.

4. Sprawdź logi w pliku dziennika zapory

Przejdź do lokalizacji pliku logów zapory, którą ustawiłeś wcześniej (np. `C:\Windows\System32\LogFiles\Firewall\pfirewall.log`).

Otwórz plik za pomocą dowolnego edytora tekstu, aby zobaczyć zarejestrowane zdarzenia.

Analiza logów przy pomocy PowerShell

Podczas pracy nad analizą logów i konfiguracją sieci PowerShell był kluczowym narzędziem. Dzięki jego poleceniom mogłem monitorować ruch sieciowy, weryfikować aktywne połączenia oraz identyfikować potencjalne zagrożenia. Na przykład, aby sprawdzić, jakie procesy nasłuchują na otwartych portach, użyłem następującego polecenia:

```
Get-NetTCPConnection | Where-Object { $_.State -eq "Listen" } | Format-Table LocalAddress, LocalPort, OwningProcess
```

Wynik pozwolił mi zidentyfikować procesy odpowiedzialne za nasłuchiwanie na porcie 22 (SSH) oraz innych otwartych portach. W przypadku portu 22, wykorzystując PowerShell, ograniczyłem dostęp tylko do zaufanych adresów IP:

```
New-NetFirewallRule -DisplayName "Allow SSH from Specific IPs" -Direction Inbound -LocalPort 22 -Protocol TCP -Action Allow -RemoteAddress 192.168.1.100, 192.168.1.101
```

Wsparcie przy analizie plików logów

Kolejnym istotnym etapem było analizowanie plików logów, które eksportowałem z różnych narzędzi systemowych. Dzięki wskazówkom AI przesyłając logi, które wymagały analizy w promptach, przejrzałem zawartość plików zapory w celu identyfikacji nietypowych zdarzeń,

takich jak próby dostępu z nieznanych adresów IP. Korzystając z PowerShell, filtrowałem logi, aby znaleźć istotne wpisy:

```
Select-String -Path "C:\Windows\System32\LogFiles\Firewall\pfirewall.log" -Pattern "Deny"
```

To polecenie pozwoliło szybko wychwycić blokowane połączenia, które mogły wskazywać na potencjalne próby ataków.

Konfiguracja sieci w PowerShell

Podczas pracy z konfiguracją sieci PowerShell był nieoceniony. Kilka przydatnych komend, które wykorzystałem:

Wyświetlenie szczegółów konfiguracji sieci:

```
Get-NetIPAddress
```

Ta komenda pozwoliła mi szybko sprawdzić przypisane adresy IP oraz interfejsy sieciowe.

Monitorowanie aktywnych połączeń:

```
Get-NetTCPConnection | Format-Table LocalAddress, LocalPort, RemoteAddress, State
```

Dzięki tej komendzie mogłem obserwować bieżący ruch sieciowy i identyfikować potencjalne zagrożenia.

Tworzenie reguły zapory:

```
New-NetFirewallRule -DisplayName "Block SMB Traffic" -Direction Inbound -LocalPort 445 -Protocol TCP -Action Block
```

W ten sposób ograniczyłem dostęp do portu SMB (445), aby zabezpieczyć system przed potencjalnymi exploitami.

Wnioski i dalsze kroki

Analiza logów oraz wykorzystanie narzędzi takich jak PowerShell umożliwiły mi dokładniejsze zrozumienie zagrożeń oraz skuteczną reakcję na nie. Dzięki systematycznemu monitorowaniu i szybkiej identyfikacji podejrzanej aktywności mogłem zapobiec potencjalnym atakom.

Podsumowując, w erze cyfrowej nieustanne monitorowanie i identyfikacja podatności są kluczowe dla utrzymania bezpieczeństwa systemów. Historia bugów, od przypadkowej ćmy w Harvard Mark II po współczesne infostealery, ukazuje, jak różnorodne mogą być wyzwania stojące przed specjalistami IT. Kluczem do skutecznej ochrony jest umiejętność szybkiego reagowania na incydenty, współpraca

międzynarodowa oraz proaktywne podejście do edukacji i testowania zabezpieczeń.

Technologia, która umożliwia nam rozwój i poprawę jakości życia, jednocześnie stawia nas przed coraz większymi wyzwaniami. Dlatego transparentność, wsparcie społeczności i otwarte standardy, w połączeniu z zaawansowanymi metodami analizy, takimi jak logi sieciowe i programy Bug Bounty, stają się fundamentem nowoczesnego cyberbezpieczeństwa. Tylko dzięki stałej ewolucji narzędzi i strategii możemy sprostać dynamicznie zmieniającym się zagrożeniom i zabezpieczyć przyszłość cyfrową na globalną skalę.