Sposoby cyber obrony. Dokumentacja do projektu z przedmiotu WCYB
grupa: CB103

Agnieszka Hermaniuk

Politechnika Warszawska, Wydział Elektroniki i Technik Informacyjnych

19 stycznia 2020

Spis treści

1 Wstęp

Dokument zawiera rozwiązania podpunktu 4. oraz 5. z zadania 3. projetku z przedmiotu wstęp do cyberbezpieczeństwa. Dotyczy podstawowych rozwiązań obrony przed potencjalnym cyberzagrożeniem wdrażanych w firmach i organizacjach. Dzieli się na dwie części:

- Zadanie 4 [roz. 2] - software, czyli narzędzia wykorzystywane do cyberobrony i ich zastosowanie;

- Zadanie 5 [roz. 3] - czynnik ludzki, czyli zespoły profesjoanlistów specjalizujących się w cyberbezpieczeństwie i ich role.

2 Zadanie 4. Narzędzia

2.1 IDS

IDS, czyli Intrusion Detection System, to system monitorujący infrastrukturę sieciową w celu wykrycia podejrzanej aktywności. Jego główną rolą jest detekcja ataku i poinformowanie o nim administratora.[1]

Systemy IDS dzielimy na:

- HIDS
- NIDS
- hybrydowe

Sposoby reakcji na wykryte zagrożenie:

- Wysłanie powiadomienia
- Zebranie dodatkowych informacji
- Zmiana zachowania środowiska sieciowego (np. zerwanie połączenia z IP atakującego)
- Podjęcie akcji przeciw intruzowi

IDS umożliwia wykrycie zagrożenia już na etapie rekonesansu.

2.1.1 HIDS

HIDS, czyli Host-Based IDS, ogranicza monitorowanie do jednego hosta, na którym jest zainstalowany.

Sposób działania:[1]

- Bada integralność systemu np. poprzez liczenie i sprawdzanie sum kontrolnych plików systemowych lub rejestru systemowego
- Bada anomalie w działaniu systemu np. próba logowania w nietypowych godzinach
- Wykrywa sygnatury - ma zapisane ustalone wzorce zachowań, których wystąpienie może oznaczać próbę ataku np. trzy nieudane próby logowania

2.1.2 NIDS

NIDS, czyli Network IDS, służy głównie do analizy ruchu sieciowego w obrębie sieci w celu wykrywania np. ataków DoS czy skanowania portów.

Sposób działania opiera się na dwóch podstawowych metodach:

1. Analiza sygnatur
2. Wykrywanie anomalii

Ze względu na specyfikę swojego działania (tylko pasywna analiza ruchu sieciowego), systemy NIDS nie obciążają infrastruktury, w której działają. Dodatkowo mogą być tak skonfigurowane, że będą praktycznie niewidoczne dla potencjalnych atakujących. Kilka systemów NIDS rozmieszczonych w odpowiednio dobranych węzłach sieci jest w stanie zapewnić monitoring nawet dość rozbudowanym systemom.

1. Bazowanie na sygnaturach

- Analizowanie pakietów na podstawie ustalonych reguł - pakiety niespełniające reguł są zgłaszane administratorowi
- Śledzenie pakietów w dłuższych okresach - ma na celu wykrycie rozłożonych w czasie, wielofazowych ataków, które charakteryzuje np. poprzedzający atak rekonesans
- Dekodowanie protokołów warstw wyższych (np. HTTP, FTP) - umożliwia wykrycie ataków pochodzących z tych warstw

2. Bazowanie na anomaliach

- **analiza heurystyczna** – wykorzystująca algorytmy definiujące pewne zachowania jako anomalie (np. algorytm definiujący, kiedy ruch sieciowy wskazuje np. na skanowanie portów)
- **analiza anomalii** - metoda polegająca na wykrywaniu ruchu sieciowego odbiegającego od normy.[1]

2.2 NNIDS

Istnieją również systemy hybrydowe NNIDS (Network Node IDS), które łączą w sobie cechy HIDS (ochrona pojedynczego hosta) oraz NIDS (analiza ruchu sieciowego skierowanego do tego konkretnego węzła sieci).

Dużą zaletą jest to, że działając bezpośrednio na hoście, są w stanie przeanalizować pakiety pochodzące z ruchu szyfrowanego zanim dotrą do docelowej aplikacji, ale już po rozszyfrowaniu ich przez system operacyjny. To pozwala na wykrywanie ataków np. na aplikacje WWW, które korzystają z szyfrowanego połączenia SSL, czy analizy pakietów z protokołu IPsec.

Połączenie wykorzystywanych wcześniej rozwiązań czyni je znacznie efektywniejszymi od zwykłych IDS-ów, ale często kosztem spowolnienia ruchu.[1]

2.3 Firewall

Firewall, czyli zapora ogniowa, to usługa, program lub urządzenie zabezpieczające sieć, które monitoruje przychodzący i wychodzący ruch sieciowy i decyduje o jego przepuszczeniu lub zablokowaniu w oparciu o zestaw określonych zasad.

2.3.1 NG Firewall

Firewall nowej generacji ma na celu zatrzymywać zagrożenia, takie jak zaawansowane złośliwe oprogramowania i ataki na poziomie aplikacji.

NG Firewall powinien zawierać:

- Standardowe funkcje firewalla, takie jak kontrola pełnostanowa
- Zapobieganie zintegrowanym włamaniom
- Świadomość i kontrolę aplikacji w celu wychwycenia i zablokowania ryzykownych aplikacji
- Ścieżki aktualizacji, które uwzględniają przyszłe źródła informacji
- Techniki reagowania na zmieniające się zagrożenia[2]

2.3.2 WAF

WAF, czyli Web Application Firewall, skupia swoje działania na ochronie stron WWW. Zapewnia ochronę przed takimi atakami jak np. SQL Injection, Cross Site Scripting, Directory Traversal oraz Command Injection, które w efekcie mogą prowadzić do wycieków danych, podmiany stron WWW, kradzieży tożsamości, umieszczenia stron phishingowych lub rozsyłania spamu za pośrednictwem skryptów.

WAF pozwala kontrolować ruch od i do naszej aplikacji, wykorzystując przy tym wcześniej przygotowane zasady, które mogą być tworzone na dwa sposoby:

- model negatywny (blacklist) – tworzenie listy treści niebezpiecznych;
- model pozytywny (whitelist) – tworzenie listy treści zaakceptowanych.[3]

2.4 DLP

System DLP (Data Loss Prevention) to oprogramowanie służące do ochrony danych przed wyciekiem. Zadaniem systemu DLP jest identyfikowanie krytycznych dokumentów, monitorowanie użytkowników mających do nich dostęp, wykrywanie prób kradzieży oraz zapobieganie wyciekowi informacji, na przykład poprzez natychmiastowe zablokowanie użytkownika (sprawcy incydentu) czy przerwanie jego aktywności.[4]

Metody działania:

- wykrywanie danych wrażliwych w ruchu sieciowym
- klasyfikacja i przypisanie wag plikom
- blokowanie zapisu na nośniki zewnętrzne
- szyfrowanie i deszyfrowanie dokumentów
- przerywanie i blokowanie transmisji danych
- blokowanie użytkownika, który naruszył firmowe bezpieczeństwo IT

2.5 SIEM

SIEM, czyli Security Information and Event Management, to system bezpieczeństwa służący do monitorowania i analizy, którego celem jest pomoc organizacjom w wykrywaniu zagrożeń i łagodzenie skutków ataków.Łączy zarządzanie incydentami bezpieczeństwa z zarządzaniem informacjami o monitorowanym środowisku. [5]

Zasada działania SIEM-ów polega na gromadzeniu logów i zdarzeń generowanych w całej infrastrukturze organizacji, normalizacji tych logów, korelacji zdarzeń i wizualizacji danych.

Systemy SIEM umożliwiają zebranie w całość logów z różnych pojedynczych incydentów, pomagają więc wykryć zdarzenia, które składają się razem na bardziej wyszukany atak. Dodatkowo możliwa jest automatyczna reakcja na trwający już atak i załagodzenie jego skutków.

2.6 Av/Am

Antivirus i antimalware to oprogramowania służące do wykrywania złośliwego oprogramowania, ochrony przed nim oraz jego usuwania. Mogą one powstrzymać infekcję wirusową i usunąć zainfekowane pliki. Obecnie programy te wykorzystują analizę heurystyczną. Analizują strukturę i zachowanie programu w celu wykrycia podejrzanej aktywności, skanują pliki, analizują ogólną strukturę programu, logikę programowania i dane w poszukiwaniu nietypowych instrukcji lub kodu śmieciowego. Mogą też odszukać złośliwe oprogramowanie w plikach i rekordach startowych, a nawet uruchamiać je w piaskownicy (kontrolowanym środowisku)[6].

2.7 EDR

EDR, czyli Endpoint Detection and Response, to narzędzie służące wykrywaniu i reagowaniu na podejrzane aktywności na urządzeniach końcowych. Skupia się na detekcji nieprawidłowych działań, nie malware. EDR analizuje uruchomione procesy, usługi, pojawiające się wpisy w rejestrze czy powiązania między procesami. Po wykryciu nietypowej aktywności generuje alert analitykom bezpieczeństwa.

EDR pozwala na:

- Efektywne zapobieganie incydentom
- Automatyczne wykrywanie zagrożeń
- Detekcję ukrytych zagrożeń
- Automatyczną reakcję na zdarzenia
- Gromadzenie informacji koniecznych do dalszej analizy[7]

2.8 SOAR

SOAR, czyli Security Orchestration, Automation and Response, ma na celu wspomaganie zespołów SOC w zarządzaniu i reagowaniu na alarmy dotyczące bezpieczeństwa. SOAR łączy wszystkie systemy, narzędzia i aplikacje wykorzystywane do cyberobrony organizacji. Umożliwia zbieranie danych i alertów bezpieczeństwa z różnych źródeł, zapewnia przeprowadzanie analizy incydentów oraz ich sortowanie i kategoryzację, eskalację, wzbogacanie, ograniczanie i usuwanie skutków.

Celem wdrożenia technologii SOAR jest skrócenie czasu od wykrycia naruszenia do rozwiązania problemu oraz zminimalizowanie ryzyka związanego z incydentami bezpieczeństwa.[8]

2.9 Przykłady

Narzędzie	Nazwa	Link
HIDS	SolarWinds Security Event Manager	SolarWinds
HIDS	OSSECC	OSSEC
NIDS	Snort	Snort
NIDS	Suricata	Suricata
Firewall	ZoneAlarm	ZoneAlarm
Firewall	ComodoFirewall	ComodoFirewall
DLP	SolarWinds DLP	SolarWinds
DLP	Symantec DLP	Symantec
SIEM	SolarWinds Security Event Manager	SolarWinds
SIEM	Splunk	Splunk
Av	BitDefender Total Security 2020	BitDefender
Av	ESET Internet Security	ESET
EDR	Cynet 360 Security Platform	Cytnet
EDR	Symantec Endpoint Protection	Symantec
SOAR	LogRhythm	LogRhythm
SOAR	RSA	RSA

2.10 Kill Chain

Etapy modelu Kill Chain, na których pomocne mogą być wspomniane rozwiązania:

Etap	Narzędzia
Reconnaissance	IDS, FW, SIEM, DLP
Weaponization	IDS, AM
Delivery	IDS, FW, AV, AM, DLP
Exploitation	HIDS, AM
Installation	HIDS, AV, DLP, FW, SIEM
Command and Control	IDS, SIEM, SOAR, FW
Actions on Objective	DLP, AM

Rys. 1: Etapy Kill Chain wraz z metodami prewencji[9]

3 Zadanie 5. Ludzie i zespoły

3.1 SOC

SOC, czyli Security Operation Center, to zespół odpowiedzialny za cyberbezpieczeństwo w firmie. Do głównych zadań każdego takiego zespołu należą:

- Utrzymywanie narzędzi do ochrony systemów - SOC odpowiada za utrzymywanie i aktualizowanie wszystkich narzędzi związanych z ochroną infrastruktury sieci organizacji, m.in. systemów SIEM
- Analizowanie podejrzanych aktywności - na podstawie stosowanych narzędzi pracownicy analizują otrzymane alerty, sortują je według wagi i zasięgu oraz wyciągają wnioski.

Każdy zespół SOC rozdziela odpowiedzialność na kilka głównych ról wśród członków.[10]

3.1.1 Security Analyst

Ich zadaniem jest detekcja zagrożeń, zbadanie ich oraz odpowiednia reakcja na nie. Mogą mieć także dodatkowe obowiązki, takie jak udział w planach odnowy czy też wdrażanie środków ochrony.

Kill Chain: wszystkie etapy

3.1.2 Security Engineer

Jego głównym zadaniem jest utrzymywanie narzędzi do ochrony systemów organizacji, poszukiwanie nowych rozwiązań, aktualizacja systemów. Są odpowiedzialni za architekturę systemów bezpieczeństwa w firmie oraz dbanie o to, by budowane systemy były aktualne.

Kill Chain: właściwie wszystkie etapy

3.1.3 Security Manager

Zarządza członkami SOC. Jest także odpowiedzialny za tworzenie polityki i protokołów do zatrudniania nowych pracowników i ustanawiania procedur. Jest bezpośrednim szefem całego zespołu SOC.

Kill Chain: *Reconnaissance, Delivery*

3.1.4 Chief Information Security Officer

Jest odpowiedzialny za określenie operacji firmy związanych z bezpieczeństwem. Mają ostatnie słowo w sprawie polityki, strategii i procedur w zakresie cyberbezpieczeństwa.

Musi posiadać też umiejętności interpersonalne, ponieważ ma bezpośredni kontakt z zarządem, gdzie wyjaśnia kwestie związane z technicznymi aspektami bezpieczeństwa firmy.

Kill Chain: *Reconnaissance, Delivery, Actions on Objective, Exploitation*

3.2 CERT

CERT, czyli Community Emergency Response Team, to organizacja utworzona w 1988 r. przez DARPA, po incydencie z robakiem Morrisa.

Zadaniem CERT jest:

- całodobowe nadzorowanie ruchu internetowego
- podejmowanie natychmiastowych akcji w razie pojawienia się zagrożeń
- działalność badawcza z zakresu metod wykrywania incydentów bezpieczeństwa
- analiza złośliwego oprogramowania i systemów wymiany informacji o zagrożeniach
- rozwijanie własnych narzędzi do wykrywania, monitorowania, analizy i korelacji zagrożeń
- regularne publikowanie raportów o bezpieczeństwie zasobów Internetu
- publikowanie materiałów edukacyjno-szkoleniowych.[11]

Kill Chain

- nadzorowanie ruchu - głównie *Reconnaissance, Delivery*
- działalność badawcza - wszystkie etpay
- analiza złośliwego oprogramowania - *Weaponization, Exploitation, Delivery, CnC, Actions on Objective*
- materiały szkoleniowe - wszystkie etapy
- raporty o bezpieczeństwie - *Delivery, Reconnaissance*

3.3 CSIRT

CSIRT, czyli Computer Security Incident Response Team, to zespół pracowników IT, którzy zapewniają organizacjom usługi i wsparcie związane z jej zabezpieczeniem przed potencjalnymi cyberatakami oraz reakcją na nie.

Podstawowe zadania zespołów CSIRT:

- odbieranie alertów o incydentach
- analizowanie alertów o incydentach - muszą sprawdzać wiarygodność alertu, a także przygotować odpowiedni plan reakcji (IRP) w danej sytuacji w celu odzyskania kontroli i zminimalizowanie skutków wydarzenia
- reagowanie na incydenty
- prewencja zagrożeń - dbanie o infrastrukturę sieci organizacji, aktualizowanie oprogrmowania, detekcja podatności
- edukacja innych pracowników organizacji

- proponowanie nowych rozwiązań, technologii, protokołów bezpieczeństwa

Kill Chain

- tworzenie IRP ma wpływ właściwie na wszystkich etapach kill chaina
- detekcja podatności, aktualizacje - etap *Exploitation* i *Delivery*
- Edukacja pracowników ma głównie wpływ na etapie *Delivery* i *Exploitation*. Z kolei dbanie o wprowadzanie nowych technologii ma wpływ na wszystkich etapach kill chaina.

Przykładowe role:[12]

- Manager
- Incident Manager
- Help Desk
- Incident Handlers
- Vulnerability Handlers
- Artifact Analysis Staff
- Platform Specialists
- Trainers
- Technology Watch

Bibliografia

[1] R. Janicki. (2015) Wprowadzenie do systemów ids. [Online]. Available: https://sekurak.pl/wprowadzenie-do-systemow-ids/

[2] Cisco. Co to jest zapora sieciowa?

[3] M. Szopa. (2018) Zapora sieciowa, czyli co to jest firewall? [Online]. Available: https://www.kei.pl/blog/zapora-sieciowa-czyli-co-to-jest-firewall/

[4] E. System. (2018) Co to jest dlp (data loss prevention) i komu się to przyda? [Online]. Available: https://www.ekransystem.com/pl/blogpolska/co-jest-dlp-data-loss-prevention-i-komu-sie-przyda

[5] K. Hack. (2019) Co to jest siem? [Online]. Available: https://kapitanhack.pl/2019/06/26/akronimy/czym-jest-siem/

[6] Malwarebytes. Ochrona antywirusowa. [Online]. Available: https://pl.malwarebytes.com/antivirus/

[7] B. Stryczek. Co to jest edr (endpoint detection and response)? [Online]. Available: https://www.vida.pl/edr-endpoint-detection-and-response/

[8] E. Kirtley. (2019) What is siem? what is soar? how are they different? [Online]. Available: https://swimlane.com/blog/siem-soar/

[9] Briskinfosec. (2019) What do you need to know about cyber kill chain? [Online]. Available: https://medium.com/@briskinfosec/what-do-you-need-to-know-about-cyber-kill-chain-4dfff57e0e72

[10] A. Stern. (2017) Understanding the soc team roles and responsibilities. [Online]. Available: https://www.siemplify.co/blog/understanding-the-soc-team-roles-and-responsibilities/

[11] C. Polska. O nas. [Online]. Available: https://www.cert.pl/o-nas/

[12] V. Henri. (2018) Incident response planning in a nutshell: Roles and responsibilities. [Online]. Available: https://www.hitachi-systems-security.com/blog/roles-responsibilities-incident-response-team/