

Ofenzivna sigurnost

Metode obrane i zaobilaznje obrane

Tin Lovreković, 8.12.2025.

Pregled predavanja

- Motivacija
- Pitanja za ispit
- EDR
- EPP
- Ostali obrambeni mehanizmi
- Zaobilazeњe obrane
- Zaključak

Motivacija

- Poznavanje obrambenih mehanizama izuzetno je važno za napadača
 - Zadnja linija obrane koja stoji između napadača i njegovog cilja
 - Poznavanje njihovog načina rada omogućuje njihovo izbjegavanje
- Problem: sustav koristi više različitih mehanizama
 - Kakvo je njihovo međudjelovanje?
- Napadači ih također koriste za osiguravanje svojih infrastruktura

Pitanja za ispite

- Zašto je važno da napadač poznaje obrambene mehanizme?
- Navedite 3 obrambena mehanizma.
- Kako EDR otkriva zloćudnu aktivnost (Function Hooking)?
- Koja je razlika između Antivirusa i Next Gen Antivirusa?
- Nabrojite 3 tehnika zaobilaženja obrane.

EDR (Endpoint Detection and Response) (1)

- Alat za obavještavanje sigurnosnih timova o sumnjivim aktivnostima unutar mreže [1, str. 14-15]
 - Prvenstveno cilja sprječavanje napada prije nego što se dogode
- Postavlja agente na sve povezane krajnje uređaje
 - Identificiraju anomalije koje vatrozid previđa, kao što su manipulacije procesima i datotekama
- Tipovi EDR-a [1, str. 20-22]
 - Agent-based, Agentless, Cloud-based, Behavioral, EPP,...

EDR (Endpoint Detection and Response) (2)

- Koriste tehniku zvanu Function hooking [1, str. 20-22]
 - Presretanje sistemskog poziva ili određene funkcije i mijenjanje njihovog standardnog ponašanja
 - Umetanjem kuke koja se nalazi u pozivu funkcije i njenog odredišta omogućuje pregled i izmjenu proslijeđenih informacija
 - Uglavnom se radi o CreateProcess, WriteFile ili CreateFile funkcijama
 - Svakim pozivom, kuka će provjeriti informacije koje se proslijeđuju funkciji i usporediti ih s poznatim zločudnim ponašanjem
 - Ako se aktivnost pokaže zločudna, EDR ju blokira

EDR (Endpoint Detection and Response) (3)

- Glavne mogućnosti EDR-a su [1, str. 20-22]
 - Praćenje svog prometa na krajnjoj točci
 - Mogućnost automatskog odgovora na prijetnje
 - Pretraživanje prijetnji prisutnih na računalu
 - Istraga incidenata i forenzičke sposobnosti
 - Napredno otkrivanje i odgovor na prijetnje
 - Integracija s drugim sigurnosnim mehanizmima

EPP (Endpoint Protection Platform) (1)

- EDR koji uključuje tradicionalna sigurnosna rješenja (antivirus, vatrozid), kao i naprednije značajke u jednoj integriranoj platformi [1, str. 25-26]
 - Dizajniran za zaštitu krajnjih uređaja kao što su stolna računala, prijenosna računala, poslužitelji i mobilni uređaji
 - Kombinira više sigurnosnih tehnologija i funkcionalnosti kako bi zaštitio krajnje uređaje od širokog raspona prijetnji
 - Tipovi: tradicionalni, napredni, integrirani, Cloud-Based i EPP treće strane

EPP (Endpoint Protection Platform) (2)

- Otkrivanje zloćudnih aktivnosti [1, str. 25-26]
 - Na temelju potpisa: održavaju bazu podataka potpisa poznatih zlonamjernih softvera
 - Analiza ponašanja: prate ponašanje krajnjih točaka u potrazi za sumnjivim aktivnostima
 - AI: pomaže identifikaciji novih prijetnji i zero-day napada
 - Heuristike: identificiraju potencijalno zlonamjerni kod na temelju njegove strukture i ponašanja
 - Podatci u oblaku: koriste podatke o prijetnjama iz repozitorija u oblaku za poboljšanje detekcije

Ostali obrambeni mehanizmi (1)

- **Antivirus** [1, str. 16-20]
 - Služe za otkrivanje, sprječavanje i uklanjanje sigurnosnih prijetnji
 - Oslanjaju se na detekciju na temelju potpisa
 - Učinkoviti samo protiv poznatih prijetnji
- **Next Generation Antivirus (NGAV)** [1, str. 16-20]
 - Koriste analizu ponašanja, AI, heurističke metode i sandboxing za poboljšanje mogućnosti otkrivanja prijetnji
 - Praćenjem ponašanja sustava u stvarnom vremenu, NGAV može otkriti prethodno nepoznate prijetnje, uključujući zero-day ranjivosti i napredne uporne prijetnje (APT-ove)

Ostali obrambeni mehanizmi (2)

- Vatrozid (engl. Firewall) [1, str. 16-20]
 - Osiguravaju mrežu provjerom svog ulaznog prometa
 - Koriste filtriranje paketa i analize stanja veza
 - Postavljaju se na mrežu (network tip) ili na pojedino računalo (host-based tip)
- IDS/IPS (Intrusion Detection/Prevention System) [1, str. 16-20]
 - Služe za otkrivanje (IDS) i sprječavanje (IPS) neovlaštenog ulaza
 - Često se koriste zajedno i s drugim mehanizmima
 - Prate mrežni promet (network tip) ili ponašanje na određenom računalu (host-based tip)

Ostali obrambeni mehanizmi (3)

- XDR (Extended Detection and Response) [1, str. 16-20]
 - Ujedinjena platforma koja omogućuje vidljivost u više tokova podataka, obuhvaćajući krajnje točke, mreže i okruženja u oblaku
 - Predstavlja evoluciju EDR-a
- MDR (Managed Detection and Response) [1, str. 16-20]
 - Kombinira naprednu tehnologiju s ljudskim znanjem
 - MDR timovi provode temeljite istrage sigurnosnih incidenata, nudeći praktične uvide za jačanje organizacijske obrane

Ostali obrambeni mehanizmi (4)

- NDR (Network Detection and Response) [1, str. 16-20]
 - Ističu se u praćenju mrežnih ranjivosti (poznatih ili nepoznatih) i pojednostavljaju upravljanje mrežom
 - Koriste AI i priručnike kako bi autonomno provoditi korektivne mjere i rješavati različite prijetnje u stvarnom vremenu
- DLP (Data Loss Prevention) [1, str. 16-20]
 - Osmišljen kako bi se spriječio gubitak, krađa ili zlouporaba osjetljivih podataka (šifriranje podataka, nadgledanje i blokiranje prijenosa, ...)
 - Kombinacija softvera, hardvera i politika

Ostali obrambeni mehanizmi (5)

- SIEM (Security Information Event Management) [1, str. 16-20]
 - Specijalizirani softver ili hardver koji omogućuje organizacijama prikupljanje i analizu podataka povezanih sa sigurnošću
 - Sastoji se od 2 dijela: SIM (Security Information Management) koji prikuplja podatke i ECA (Event Correlation and Analysis) koji ih analizira
- SOAR (Security Orchestration, Automation and Response) [1, str. 16-20]
 - Sveobuhvatno rješenje za poboljšanje, pojednostavljenje i ubrzavanje postupaka odgovora na incidente
 - Automatizira jednostavne, ponavljajuće zadatke

Zaobilaženje obrane

- Tehnike zaobilaženje DLP-a [2]
 - Šifriranje podataka
 - Kompresija podataka
 - Steganografija (tehnika skrivanja osjetljivih podataka unutar naizgled bezopasnih datoteka ili slika)
 - Fragmentacija (rastavljanje podataka na manje dijelove koje je teže otkriti)
 - Korištenje nestandardnih protokola
 - Korištenje alternativnih komunikacijskih kanala koje DLP ne provjerava (npr. osobni email, servis u oblaku)

Zaključak

- Zaobilazeње obrambenih mehanizama je ključno za postizanje cilja
 - To je moguće samo dobrim poznavanjem načina njihovog rada i međudjelovanja
- Često ih se koristi više istodobno
 - Značajno otežava posao napadaču, no često i oni imaju ranjivosti koje je moguće iskoristiti za izbjegavanje detekcije

Literatura

- [1] A Comprehensive Analysis of EDR (Endpoint Detection & Response), EPP (Endpoint Protection Platform), and Antivirus Security Technologies
https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/16751/Cappello_mpked21016.pdf?sequence=5&isAllowed=y
- [2] BYPASS DLP POLICIES
<https://www.linkedin.com/pulse/bypass-dlp-policies-jitu-mani-das-cism-cissp--oikrf/>

Dodatna Literatura

- What is Endpoint Detection and Response (EDR)?, IBM Technology
<https://www.youtube.com/watch?v=55GaloVVql>
- EDR vs. EPP vs. NGAV, IBM Technology
<https://www.youtube.com/watch?v=8ZIHOZINIkk>

Hvala!