Lecția 2: Peisajul amenințărilor și vectorii de atac

Tema: Fundamentele securității informaționale
Universitatea Tehnică a Moldovei
Lector: Maxim Masiutin, Asistent universitar

Introducere

Bine ați revenit. În lecția anterioară, am stabilit conceptele fundamentale ale securității informaționale, inclusiv Triada CID, activele, amenințările, vulnerabilitățile și riscurile. Astăzi vom analiza în profunzime peisajul amenințărilor, examinând cine atacă sistemele noastre, de ce o fac și cum își desfășoară atacurile.

Înțelegerea adversarului este esențială pentru o apărare eficientă. Așa cum a scris Sun Tzu în "Arta Războiului", dacă îl cunoști pe inamic și te cunoști pe tine însuți, nu trebuie să te temi de rezultatul a o sută de bătălii. În securitatea cibernetică, trebuie să înțelegem actorii de amenințare, motivațiile lor, capabilitățile lor și metodele lor.

Peisajul amenințărilor a evoluat dramatic în ultimii ani. Conform Raportului Global de Amenințări CrowdStrike din 2025, publicat de CrowdStrike, o companie de securitate cibernetică, intruziunile în cloud au crescut cu 136 la sută în prima jumătate a anului 2025, comparativ cu întregul an 2024. Intruziunile interactive, în care atacatorii operează direct de la tastatură, au crescut cu 27 la sută de la an la an, iar, în mod remarcabil, 81 la sută dintre aceste intruziuni au fost fără software malițios. Atacatorii devin tot mai sofisticați, bazându-se mai puțin pe software malițios tradițional și mai mult pe tehnici de tip Living off the Land.

Să începem prin clasificarea actorilor care reprezintă amenințări pentru organizațiile noastre.

Partea 1: Clasificarea actorilor de amenințare

Un **actor de amenințare** este orice individ sau grup care reprezintă o amenințare potențială pentru securitatea unei organizații. Actorii de amenințare variază semnificativ în ceea ce privește motivațiile, capabilitățile, resursele și țintele lor. Înțelegerea acestor diferențe ne ajută să anticipăm și să ne apărăm împotriva atacurilor lor.

Actori statali

Actorii statali sunt grupuri sponsorizate de guvern care desfășoară operațiuni cibernetice în scopuri politice, economice sau militare. Aceștia reprezintă cei mai sofisticați și mai bine dotați actori de amenințare.

Caracteristici:

- Resurse practic nelimitate (finanțare, personal, timp)
- Acces la instrumente avansate, inclusiv exploituri de tip zero-day
- Operațiuni pe termen lung, răbdătoare, care durează luni sau ani
- Securitate operațională sofisticată pentru evitarea atribuirii
- Protecție juridică la nivel de stat

Motivații:

- Spionaj (furtul secretelor guvernamentale, proprietății intelectuale)
- Sabotaj (perturbarea infrastructurii critice)
- Operațiuni de influență (manipularea opiniei publice)
- Avantaj economic (furtul secretelor comerciale)

Exemple conform MITRE ATT&CK:

- **APT28 (Fancy Bear)**: Asociat cu serviciile militare de informații ale Rusiei, a vizat alegerile din SUA, comitetele olimpice și țările NATO
- **APT41**: Grup sponsorizat de statul chinez care desfășoară atât operațiuni de spionaj, cât și operațiuni motivate financiar
- **Lazarus Group**: Grup nord-coreean cunoscut pentru atacul asupra Sony Pictures și ransomware-ul WannaCry
- **APT33**: Grup iranian care vizează sectoarele aerospațial și energetic

Termenul APT înseamnă **Amenințare Persistentă Avansată**. Grupurile APT se caracterizează prin capabilitățile lor avansate și persistența în urmărirea obiectivelor pe perioade îndelungate. Adesea mențin accesul la rețelele compromise timp de ani înainte de a fi detectate.

În MITRE ATT&CK nu există grupuri clasificate în mod explicit ca fiind sponsorizate de guvernele din America de Nord sau Europa de Vest. Această asimetrie există deoarece MITRE ATT&CK este construit pe baza rapoartelor occidentale open-source de informații privind amenințările cibernetice. Furnizorii și guvernele occidentale publică rapoarte extinse care atribuie activitatea adversarilor actorilor statali ruși, chinezi, iranieni și nord-coreeni — adesea susținute de inculpări și sancțiuni. O atribuire publică comparabilă a operațiunilor ofensive ale SUA, Marii Britanii sau ale altor țări din alianța Five Eyes este aproape inexistentă în ecosistemul CTI, în ciuda capacităților bine documentate (scurgerile de informații Shadow Brokers, dezvăluirile lui Snowden, Vault 7 etc.). Prin urmare, framework-ul MITRE ATT&CK

reflectă ceea ce este raportat și atribuit în mod public, nu distribuția reală a operațiunilor cibernetice sponsorizate de state la nivel global.

Printre exemplele neatribuite în mod explicit de MITRE se pot număra următoarele:

- **Equation (G0020)**: atribuită pe scară largă de Kaspersky și alți cercetători către NSA/TAO (Tailored Access Operations) din SUA. Descrierea oferită de MITRE omite în mod deliberat orice atribuire guvernamentală, menționând doar că este „un grup de amenințare sofisticat care folosește multiple instrumente de acces la distanță".
- **Strider / ProjectSauron (G0041)**: suspectată de cercetători că ar fi legată de o agenție de informații occidentală (posibil din SUA sau a unui stat aliat). Din nou, MITRE nu oferă nicio atribuire guvernamentală.

Infractori cibernetici

Infractorii cibernetici sunt motivați în principal de câștigul financiar. Aceștia variază de la hackeri individuali la sindicate de crimă organizată cu structuri de tip corporativ.

Caracteristici:

- Motivați financiar
- Selecție oportunistă a țintelor (ținte ușor de atacat)
- Utilizarea infrastructurii criminale (găzduire protejată, spălare de bani)
- Operațiuni din ce în ce mai profesionale
- Pot achiziționa instrumente și servicii de la alți infractori

Activități comune:

- **Ransomware**: Criptarea datelor victimei și solicitarea unei plăți
- **Compromiterea e-mailului de afaceri**: Păcălirea angajaților pentru a transfera fonduri
- **Furtul cardurilor de credit**: Furtul și vânzarea datelor de pe carduri de plată
- **Recoltarea credențialelor**: Furtul și vânzarea datelor de autentificare
- **Cryptojacking**: Utilizarea sistemelor victimei pentru minarea criptomonedelor

Economia criminalității cibernetice a devenit puternic organizată. Există piețe unde infractorii cumpără și vând date furate, instrumente de hacking și chiar acces la sisteme compromise. Operațiunile de tip Ransomware ca Serviciu furnizează ransomware către afiliați care efectuează atacurile, împărțind profiturile.

Hacktiviști

Hacktiviștii sunt indivizi sau grupuri care utilizează hacking-ul pentru a promova cauze politice sau sociale. Termenul combină "hacker" și "activist".

Caracteristici:

- Motivați ideologic
- Caută publicitate pentru cauza lor
- Capabilități tehnice variabile
- Adesea organizați în mod lax
- Pot avea o selecție largă a țintelor

Activități comune:

- Vandalizarea site-urilor web pentru răspândirea mesajelor
- Atacuri DDoS pentru perturbarea operațiunilor
- Scurgeri de date pentru a pune în dificultate țintele
- Doxing (dezvăluirea informațiilor private despre indivizi)

Exemple:

- **Anonymous**: Colectiv descentralizat cunoscut pentru atacuri asupra guvernelor și corporațiilor
- **LulzSec**: Grup care a vizat Sony, CIA și alte organizații
- Diverse grupuri active în timpul conflictelor geopolitice

Amenințări interne

Amenințările interne provin de la indivizi din cadrul organizației care utilizează în mod abuziv accesul lor autorizat. Aceștia pot fi angajați actuali sau foști, contractori sau parteneri de afaceri.

Tipuri de amenințări interne:

- **Persoane din interior rău intenționate**: Cauzează în mod deliberat daune din răzbunare, câștig financiar sau ideologie
- **Persoane din interior neglijente**: Cauzează accidental daune prin lipsa de atenție sau de conștientizare
- **Persoane din interior compromise**: Au credențialele furate de atacatori externi

Caracteristici:

- Dețin deja acces autorizat
- Cunosc sistemele și procesele organizaționale
- Pot ocoli multe controale de securitate
- Acțiunile lor pot părea legitime
- Greu de detectat

Conform Raportului Verizon Data Breach Investigations Report (DBIR) din 2024, amenințările interne sunt implicate în aproximativ 20-30 la sută din brețele de securitate, dar adesea

cauzează cele mai mari daune deoarece persoanele din interior știu unde se află activele valoroase.

Script kiddies

Script kiddies sunt atacatori fără experiență care utilizează instrumente pre-construite fără a înțelege cum funcționează. În ciuda abilităților lor limitate, pot cauza totuși daune semnificative.

Caracteristici:

- Sofisticare tehnică redusă
- Utilizează instrumente disponibile pe scară largă
- Adesea motivați de curiozitate sau de dorința de recunoaștere
- Selecție oportunistă a țintelor
- Pot cauza accidental mai multe daune decât au intenționat

Deși fiecare script kiddie individual reprezintă o amenințare limitată, numărul lor mare înseamnă că, în mod colectiv, desfășoară multe atacuri. Adesea servesc drept poartă de intrare pentru dezvoltarea unor atacatori mai sofisticați.

Competitori

Spionajul competitiv implică afaceri care își spionează rivalii pentru a obține un avantaj concurențial.

Activități:

- Furtul secretelor comerciale și al proprietății intelectuale
- Obținerea listelor de clienți și a informațiilor despre prețuri
- Monitorizarea planurilor strategice
- Angajarea de personal pentru a extrage cunoștințe

Această amenințare este adesea subestimată, dar poate cauza prejudicii comerciale semnificative.

Partea 2: Vectorii de atac

Un **vector de atac** este calea sau metoda pe care un atacator o utilizează pentru a obține acces la un sistem țintă. Înțelegerea vectorilor de atac ne ajută să implementăm apărări adecvate.

Atacuri bazate pe rețea

Atacurile de rețea vizează infrastructura de comunicații care conectează sistemele.

Atacuri de rețea externe:

- Scanarea porturilor pentru identificarea serviciilor active
- Exploatarea serviciilor de rețea vulnerabile
- Atacuri de tip man-in-the-middle asupra traficului de rețea
- Atacuri DNS (spoofing, otrăvirea cache-ului)
- Atacuri DDoS pentru a copleși resursele rețelei

Atacuri de rețea interne:

- Spoofing ARP pentru redirecționarea traficului
- VLAN hopping pentru accesarea rețelelor segmentate
- Dispozitive neautorizate în rețea
- Interceptarea neautorizată a traficului de rețea

Atacuri wireless:

- Puncte de acces de tip evil twin
- Încercări de spargere WPA2/WPA3
- Atacuri Bluetooth
- Bruiaj RF

Atacuri bazate pe aplicații

Atacurile asupra aplicațiilor vizează vulnerabilitățile software.

Atacuri asupra aplicațiilor web:

- Injecție SQL: Inserarea de interogări malițioase în baza de date
- Cross-site scripting (XSS): Injectarea de scripturi malițioase
- Cross-site request forgery (CSRF): Forțarea utilizatorilor autentificați să efectueze acțiuni
- Execuție de cod la distanță: Exploatarea defectelor pentru a rula cod arbitrar
- Traversarea căilor: Accesarea neautorizată a fișierelor

Atacuri asupra API-urilor:

- Autentificare defectuoasă
- Expunerea excesivă a datelor
- Vulnerabilități de atribuire în masă
- Atacuri de injecție

Vulnerabilități software:

- Depășiri de buffer
- Erori de tip use-after-free
- Depășiri de numere întregi
- Condiții de cursă

Atacuri fizice

Atacurile fizice necesită prezența fizică la sau în apropierea țintei.

Exemple:

- Furtul dispozitivelor (laptopuri, telefoane, memorii USB)
- Supravegherea vizuală pentru a observa parolele (shoulder surfing)
- Căutarea în gunoi pentru documente aruncate
- Tailgating prin ușile securizate
- Instalarea de keyloggere hardware
- Atacuri cu dispozitive USB abandonate (lăsarea de dispozitive USB malițioase)

Securitatea fizică este adesea neglijată, dar rămâne critică.

Atacuri de inginerie socială

Ingineria socială exploatează psihologia umană, nu vulnerabilitățile tehnice. Vom acoperi acest subiect în detaliu într-o lecție ulterioară, dar vectorii principali includ:

- E-mailuri de phishing
- Phishing vocal (vishing)
- Phishing prin SMS (smishing)
- Pretexting și impersonare
- Momeală (baiting)

Atacuri pe lanțul de aprovizionare

Atacurile pe lanțul de aprovizionare compromit o organizație prin atacarea furnizorilor, vânzătorilor sau furnizorilor de software ai acesteia. Aceste atacuri au crescut dramatic în ultimii ani.

Tipuri:

- **Lanțul de aprovizionare software**: Compromiterea software-ului în timpul dezvoltării sau distribuției
- **Lanțul de aprovizionare hardware**: Implantarea de componente malițioase în hardware

- **Atacuri asupra furnizorilor de servicii**: Compromiterea furnizorilor de servicii gestionate pentru a ajunge la clienții lor

Exemple celebre:

- **SolarWinds (2020)**: Atacatorii au compromis actualizarea software-ului Orion de la SolarWinds, o companie de gestionare a infrastructurii IT, afectând 18.000 de organizații, inclusiv agenții guvernamentale ale SUA
- **Kaseya (2021)**: Ransomware distribuit prin software de administrare la distanță compromis de la Kaseya, un furnizor de software de gestionare IT
- **Log4Shell (2021)**: Vulnerabilitate într-o bibliotecă de jurnalizare larg utilizată, care a afectat nenumărate aplicații

Un nou cadru denumit **OSC&R (Open Software Supply Chain Attack Reference)** a fost creat special pentru a aborda amenințările de securitate ale lanțului de aprovizionare software. Acesta oferă o abordare similară cu MITRE ATT&CK pentru înțelegerea comportamentelor atacatorilor în contextele lanțului de aprovizionare.

Vectori de atac bazați pe cloud

Pe măsură ce organizațiile migrează către cloud, apar noi vectori de atac.

Atacuri specifice cloud-ului:

- Configurare greșită a stocării cloud (bucket-uri S3 expuse)
- Credențiale cloud compromise
- API-uri nesecurizate
- Atacuri cross-tenant în medii multi-tenant
- Vulnerabilități ale funcțiilor serverless
- Evadări din containere

Intruziunile în cloud au crescut dramatic. Multe secvențe de atac se desfășoară acum în planurile de control cloud, nu pe punctele terminale tradiționale, necesitând noi abordări defensive.

Partea 3: Ciclul de viață al vulnerabilităților

Înțelegerea modului în care vulnerabilitățile sunt descoperite, divulgate și exploatate ne ajută să gestionăm riscul în mod eficient.

Descoperirea vulnerabilităților

Vulnerabilitățile pot fi descoperite de:

- Cercetători de securitate (etici)
- Producătorii de produse
- Agenții guvernamentale
- Infractori cibernetici
- Participanți la programe bug bounty

Divulgarea responsabilă

Când cercetătorii descoperă vulnerabilități, practicile de divulgare responsabilă sugerează:

1. Raportarea vulnerabilității în mod privat către producător
2. Acordarea unui timp rezonabil producătorului pentru a dezvolta un patch (de obicei 90 de zile)
3. Coordonarea divulgării publice după ce un patch este disponibil
4. Dacă producătorul nu acționează, divulgarea pentru a proteja publicul

Vulnerabilități de tip zero-day

O **vulnerabilitate de tip zero-day** este un defect necunoscut producătorului sau publicului. Exploiturile de tip zero-day vizează aceste vulnerabilități înainte ca patch-urile să existe.

Vulnerabilitățile zero-day sunt foarte valoroase:

- Statele le acumulează pentru operațiuni ofensive
- Infractorii cibernetici plătesc sute de mii de dolari pentru ele
- Programele bug bounty oferă recompense substanțiale

Odată ce o vulnerabilitate zero-day este descoperită și utilizată, aceasta devine cunoscută și în cele din urmă este remediată, pierzându-și valoarea.

Sistemul CVE

Sistemul **CVE (Common Vulnerabilities and Exposures)** oferă identificatori standardizați pentru vulnerabilitățile cunoscute.

Format: CVE-AN-NUMAR (de ex., CVE-2024-12345)

Înregistrările CVE includ:

- Descrierea vulnerabilității
- Produsele și versiunile afectate
- Referințe la avize și patch-uri

Baza de date CVE este menținută de MITRE Corporation și este accesibilă gratuit la cve.org.

Evaluarea CVSS

Sistemul comun de evaluare a vulnerabilităților (CVSS) oferă scoruri numerice care indică severitatea vulnerabilităților.

Scorurile CVSS 3.1 variază de la 0,0 la 10,0:

- 0,0: Niciuna
- 0,1-3,9: Scăzută
- 4,0-6,9: Medie
- 7,0-8,9: Ridicată
- 9,0-10,0: Critică

CVSS ia în considerare factori precum:

- Vectorul de atac (rețea, adiacent, local, fizic)
- Complexitatea atacului
- Privilegiile necesare
- Interacțiunea utilizatorului necesară
- Impactul asupra confidențialității, integrității, disponibilității

Organizațiile folosesc scorurile CVSS pentru a prioritiza eforturile de remediere, deși scorurile ar trebui considerate alături de factorii contextuali specifici fiecărui mediu.

Partea 4: Cadrul MITRE ATT&CK

Cadrul MITRE ATT&CK este o bază de cunoștințe accesibilă global, conținând tactici și tehnici ale adversarilor, bazată pe observații din lumea reală. ATT&CK provine de la Adversarial Tactics, Techniques, and Common Knowledge.

Structura cadrului

ATT&CK organizează comportamentul adversarilor în:

Tactici: "De ce"-ul unui atac, obiectivul adversarului

- Recunoaștere (Reconnaissance)
- Dezvoltarea resurselor (Resource Development)
- Acces inițial (Initial Access)
- Execuție (Execution)
- Persistență (Persistence)
- Escaladarea privilegiilor (Privilege Escalation)

- Evitarea apărării (Defense Evasion)
- Accesul la credențiale (Credential Access)
- Descoperire (Discovery)
- Mișcare laterală (Lateral Movement)
- Colectare (Collection)
- Comandă și control (Command and Control)
- Exfiltrare (Exfiltration)
- Impact (Impact)

Tehnici: "Cum"-ul unui atac, metodele specifice utilizate

Sub-tehnici: Implementări mai specifice ale tehnicilor

Proceduri: Descrieri detaliate ale modului în care grupuri specifice implementează tehnicile

Utilizarea ATT&CK

Organizațiile folosesc ATT&CK pentru:

- **Informații despre amenințări**: Înțelegerea modului în care operează grupuri specifice
- **Detecție**: Dezvoltarea capabilităților de detecție pentru tehnici cunoscute
- **Evaluare**: Evaluarea acoperirii securității în raport cu cadrul
- **Red teaming**: Planificarea simulărilor realiste de atac
- **Instruire**: Educarea echipelor de securitate cu privire la metodele adversarilor

Matricele ATT&CK

MITRE oferă mai multe matrice:

- **Enterprise**: Windows, macOS, Linux, cloud, rețea, containere
- **Mobile**: iOS și Android
- **ICS**: Sisteme de control industrial

Actualizări recente

Începând cu sfârșitul anului 2025, MITRE a lansat versiunea 18 a ATT&CK, care a introdus:

- Obiecte de tip Strategii de Detecție și Analiză
- Ghidaj structurat de detecție axat pe comportament
- Tehnici extinse de atac bazate pe cloud
- Noi tactici legate de atacuri conduse de IA
- Tehnici de compromitere a lanțului de aprovizionare

Evaluările ATT&CK din 2025 s-au concentrat pe atacurile grupului Scattered Spider (grup de infractori cibernetici) și Mustang Panda (actor sponsorizat de statul chinez), cu un accent sporit pe atacurile asupra infrastructurii cloud și capabilitățile de protecție.

Partea 5: Amenințări emergente în 2025-2026

Să examinăm cele mai semnificative amenințări emergente pe care profesioniștii în securitate trebuie să le abordeze.

Atacuri asistate de IA

Inteligența artificială transformă peisajul amenințărilor:

- **Phishing generat de IA**: Modelele lingvistice mari creează conținut de phishing foarte convingător
- **Descoperirea automatizată a vulnerabilităților**: Sistemele de IA găsesc și exploatează vulnerabilități mai rapid
- **Deepfake-uri**: Audio și video realist pentru atacuri de impersonare
- **Software malițios adaptiv**: Software malițios care își modifică comportamentul în funcție de mediu
- **Inginerie socială asistată de IA**: Manipulare personalizată la scară largă

Amenințări ale calculului cuantic

Deși calculatoarele cuantice practice capabile să spargă criptarea actuală nu există încă, organizațiile trebuie să se pregătească:

- **Interceptează acum, decriptează mai târziu**: Atacatorii fură date criptate acum pentru a le decripta când calculatoarele cuantice vor deveni disponibile
- **Migrarea criptografică**: Planificarea tranziției către algoritmi post-cuantici
- **Incertitudinea cronologică**: Estimările variază de la 5 la peste 15 ani

Atacuri pe lanțul de aprovizionare

Atacurile pe lanțul de aprovizionare continuă să crească:

- Instrumente de dezvoltare software compromise
- Cod malițios în dependențele open-source
- Atacuri asupra furnizorilor de servicii gestionate
- Implante hardware

- Mecanisme de actualizare compromise

Organizațiile trebuie să verifice integritatea întregului lor lanț de aprovizionare software.

Amenințări native cloud

Pe măsură ce sarcinile de lucru migrează către cloud:

- Configurarea greșită rămâne cauza principală a breșelor de securitate în cloud
- Atacuri specifice pentru containere și Kubernetes
- Vulnerabilități ale funcțiilor serverless
- Atacuri cross-tenant
- Furtul credențialelor cloud

Atacuri bazate pe identitate

Atacatorii vizează din ce în ce mai mult identitatea:

- Phishing și furt de credențiale
- Tehnici de ocolire a MFA
- Deturnarea sesiunilor
- Escaladarea privilegiilor
- Atacuri asupra federării identității

Atacuri fără software malițios

O tendință semnificativă evidențiată de Raportul Global de Amenințări CrowdStrike din 2025: 81 la sută din intruziuni au fost fără software malițios:

- Tehnici de tip Living off the Land folosind instrumente legitime
- Atacuri fără fișiere care rezidă doar în memorie
- Abuzul aplicațiilor de încredere
- Atacuri bazate pe PowerShell și scripturi
- Mai greu de detectat cu antivirusul tradițional

Partea 6: Informații despre amenințări

Informațiile despre amenințări (Threat Intelligence) reprezintă cunoștințe bazate pe dovezi despre amenințări care ajută organizațiile să ia decizii informate de securitate.

Tipuri de informații despre amenințări

Informații strategice: Informații de nivel înalt despre tendințe și riscuri pentru conducerea executivă

Informații tactice: Informații despre instrumentele, tehnicile și procedurile atacatorilor pentru echipele de securitate

Informații operaționale: Detalii despre atacuri specifice, campanii sau actori

Informații tehnice: Indicatori de compromitere (IOC) pentru sistemele de detecție

Indicatori de compromitere (IOC)

IOC sunt artefacte care indică o posibilă activitate malițioasă:

- Adrese IP
- Nume de domeniu
- Hash-uri de fișiere
- URL-uri
- Adrese de e-mail
- Chei de registru
- Nume de mutex

Instrumentele de securitate folosesc IOC-uri pentru a detecta amenințări cunoscute.

Partajarea informațiilor despre amenințări

Organizațiile partajează informații despre amenințări prin:

- Centre de partajare și analiză a informațiilor (ISAC)
- Programe guvernamentale (CISA, FBI)
- Fluxuri comerciale de informații despre amenințări
- Informații din surse deschise (OSINT)
- Grupuri și parteneriate din industrie

Partajarea îmbunătățește apărarea colectivă, dar necesită gestionarea atentă a informațiilor sensibile.

Partea 7: Exercițiu practic

Să analizăm un scenariu din lumea reală pentru a ilustra aceste concepte.

Scenariu: Atacul SolarWinds

În decembrie 2020, a fost descoperit atacul pe lanțul de aprovizionare SolarWinds. Să-l analizăm folosind cadrul nostru:

Actor de amenințare: APT29 (Cozy Bear), asociat cu serviciul de informații rusesc

Motivație: Spionaj, acces la rețelele guvernamentale ale SUA

Vector de atac: Lanțul de aprovizionare (actualizare software compromisă)

Acces inițial (ATT&CK): Compromiterea lanțului de aprovizionare (T1195.002)

Tehnici utilizate:

- Actualizare software troianizată
- Comandă și control furtiv
- Recunoaștere extinsă
- Recoltarea credențialelor
- Mișcare laterală
- Exfiltrarea datelor

Impact:

- 18.000 de organizații au primit actualizarea compromisă
- Agenții guvernamentale majore ale SUA au fost compromise
- Multiple companii private afectate
- Luni de acces nedetectat

Lecții:

- Securitatea lanțului de aprovizionare este critică
- Statele au capabilități extinse
- Detectarea actorilor sofisticați este extrem de dificilă
- Încrederea în furnizori trebuie verificată

Concluzie

Astăzi am explorat peisajul amenințărilor în profunzime:

1. **Actorii de amenințare**: Actorii statali, infractorii cibernetici, hacktiviștii, amenințările interne și alții au motivații și capabilități diferite
2. **Vectorii de atac**: Atacuri de rețea, aplicații, fizice, de inginerie socială, pe lanțul de aprovizionare și în cloud

3. **Ciclul de viață al vulnerabilităților**: Descoperirea, divulgarea, remedierea și sistemele CVE/CVSS
4. **MITRE ATT&CK**: Cadrul pentru înțelegerea comportamentului adversarilor
5. **Amenințări emergente**: Atacuri asistate de IA, amenințări cuantice, lanțul de aprovizionare, atacuri native cloud și atacuri fără software malițios
6. **Informații despre amenințări**: Utilizarea cunoștințelor bazate pe dovezi pentru apărare

În lecția următoare, vom examina în detaliu software-ul malițios, inclusiv tipurile de malware, metodele de infectare și tehnologiile defensive.

Întrebări de discuție

1. Cum ar trebui organizațiile să prioritizeze apărarea împotriva diferiților actori de amenințare?
2. Care sunt implicațiile etice ale acumulării vulnerabilităților zero-day de către guverne?
3. Cum pot organizațiile să verifice securitatea lanțului lor de aprovizionare software?

Vă mulțumesc pentru atenție. Ne vedem la următoarea sesiune.

Întrebări de recapitulare

1. Identificați și comparați cele șase categorii principale de actori de amenințare. Ce le distinge motivațiile și capabilitățile?
2. Ce este o vulnerabilitate de tip zero-day și de ce este deosebit de periculoasă?
3. Explicați sistemul CVE și cum ajută evaluarea CVSS organizațiile să prioritizeze remedierea vulnerabilităților.
4. Descrieți cadrul MITRE ATT&CK. Cum este organizat și cum îl pot utiliza apărătorii?
5. Care sunt vectorii de atac principali prin care organizațiile sunt compromise?
6. Cum diferă atacurile pe lanțul de aprovizionare de atacurile directe și de ce sunt dificil de apărat?
7. Ce tipuri de informații despre amenințări există și cum ar trebui utilizat fiecare într-o organizație?
8. Explicați conceptul de divulgare responsabilă și rolul acestuia în ciclul de viață al vulnerabilităților.

Termeni cheie

- **Atac asistat de IA**: Un atac cibernetic care utilizează inteligența artificială pentru a automatiza descoperirea vulnerabilităților sau pentru a îmbunătăți capabilitățile de atac
- **APT (Amenințare Persistentă Avansată)**: Un atac cibernetic prelungit și țintit, desfășurat de un adversar sofisticat
- **Vector de atac**: Calea sau metoda utilizată de un atacator pentru a obține acces la o țintă
- **CVE**: Common Vulnerabilities and Exposures, un sistem de identificare a vulnerabilităților cunoscute
- **CVSS**: Common Vulnerability Scoring System, un cadru de evaluare a severității vulnerabilităților
- **Infractor cibernetic**: Un individ sau grup care comite infracțiuni folosind calculatoare sau rețele pentru câștig financiar
- **Hacktivism**: Hacking motivat de cauze politice sau sociale
- **Interceptează acum, decriptează mai târziu**: O strategie în care atacatorii colectează date criptate acum cu intenția de a le decripta când calculatoarele cuantice vor deveni disponibile
- **Indicator de compromitere (IOC)**: Dovadă că a avut loc o breșă de securitate
- **Amenințare internă**: Un risc de securitate care provine din interiorul organizației
- **MITRE ATT&CK**: O bază de cunoștințe despre tacticile, tehnicile și procedurile adversarilor
- **Actor statal**: Un actor de amenințare sponsorizat de guvern care desfășoară operațiuni cibernetice
- **Divulgare responsabilă**: Practica de a raporta în mod privat vulnerabilitățile de securitate producătorilor înainte de a le face publice
- **Lista componentelor software (SBOM)**: Un inventar complet al tuturor componentelor și dependențelor dintr-un produs software
- **Atac pe lanțul de aprovizionare**: Un atac care vizează elementele mai puțin securizate dintr-un lanț de aprovizionare
- **Actor de amenințare**: O entitate responsabilă de un eveniment sau incident care afectează securitatea altei entități
- **Informații despre amenințări**: Cunoștințe bazate pe dovezi despre amenințări existente sau emergente
- **Zero-day**: O vulnerabilitate necunoscută producătorului, fără patch disponibil

Referințe și lecturi suplimentare

- MITRE ATT&CK Framework (attack.mitre.org)
- NIST National Vulnerability Database (nvd.nist.gov)
- Verizon Data Breach Investigations Report
- ENISA Threat Landscape Report
- Mandiant M-Trends Report
- CISA Known Exploited Vulnerabilities Catalog