Cyberforsvar – kan du løse gåden?

Introduktion

> Hver dag bliver der smadret mod Danmarks digitale forsvarsværk, men der uddannes ikke nok 'good guy'-hackere til at forsvare os. Det skal du prøve! Skolens system er blevet ramt af et angreb. Alt er låst ned, og tiden løber. I skal arbejde som et team af etiske hackere, finde ud af hvem der står bag, og knække koden, før nedtællingen når nul. Nogle spor ligger på skærmen – andre ligger på selve skolen…

Sikkerhed

VIGTIGT – læs dette sikkerhedsafsnit, inden du går i gang!

Opmærksomhed

Alt du foretager dig i denne aktivitet er med fokus på etisk hacking, for at forstå hvordan du kan beskytte dig selv og andre.

- Alle navne, IP-adresser, servere og mails i aktiviteten er fiktive eller ligger i et lukket øvemiljø.
- Det er ulovligt at skaffe sig adgang til andres computere, konti eller servere uden tilladelse (straffelovens § 263). Du må kun arbejde i det miljø, læreren har åbnet for.
- Indtast aldrig dine egne rigtige brugernavne eller adgangskoder i øvelsen.

Forholdsregler

- Det her er en IT-øvelse. Der er ingen rigtig nødsituation, og skolens døre og alarmer er upåvirkede.
- Hvis I finder en USB-nøgle, må I aldrig sætte den i en computer. Aflever den til læreren.
- Hold jer til de systemer og den adresse, læreren har givet jer. Prøv ikke at scanne eller afprøve andre sider eller netværk.
- Ingen må tage skolens ting væk eller åbne lokaler, der ikke er en del af øvelsen. Alle fysiske spor ligger frit synlige på de aftalte steder.
- Ret ikke i andres filer eller indstillinger på øveserveren.
- Skriv aldrig rigtige personoplysninger ned i opgaverne.

Førstehjælp

- Hvis du er kommet til at indtaste rigtige oplysninger et sted, så sig det straks til læreren. Skift adgangskoden med det samme, og fortæl en voksen.
- Bliver det for stressende, så sig stop. Tidspresset er en del af spillet, men ingen skal have det dårligt over det. Der er altid hints og en nødudgang.
- Hvis noget går i stykker på øveserveren, siger du det til læreren. Det kan nulstilles, og der er ingens skyld.

Oprydning

- Luk alle faner og log ud af øvesystemerne.
- Læg alle fysiske spor, post-its, USB-nøgler og udskrifter tilbage hos læreren, så de kan bruges igen.
- Slet ikke noget på servere, og gem ikke koder eller oplysninger til senere.

□□ Materialer

I skal bruge følgende:

- En computer eller tablet pr. gruppe (3-4 elever)
- Link til escape roomet: Lindeholm Skole IT
- Link til øveserveren: skolelabs.dk/cyberhack

- Opgaveark: print mailens header, IP-opslagstabel, serverrapport, chifferark og en kodestribe til hver gruppe
- Hint-kort (3 pr. gruppe)
- Papir og blyant
- En QR-kode med ren tekst, sat op på opslagstavlen på gangen
- Et tastatur på et bord med skiltet “Admin-PC” og en seddel under det
- En kasse med en kombinationslås på tre cifre (eller et kuvert)
- Bonus: en tom USB-nøgle eller et tomt USB-hylster
- Ur eller storskærm med nedtælling

Vejledning

Følg vejledningen trin for trin:

Intro: Systemnedbrud (Akt 1)

- Klassen får en mail fra “skolen”, og læreren åbner den.
- Mailen leder til en loginside, og så starter IT-lockdown med nedtælling.
- Gruppernes mål er at finde en slutkode, der låser systemet op.
- Hver mission giver et kodefragment. Skriv dem alle på kodestriben.

Mission 1: Hvem sendte mailen? (analog)

- Læs det printede mail-header-ark.
- Sæt ring om alle røde flag, fx et afsenderdomæne, der ikke er skolens, en Reply-To-adresse et andet sted hen, tidspres eller et link, der ikke passer.
- Antallet af røde flag giver jeres første kodefragment: HEADER.

Mission 2: IP-adressen (analog)

- Find IP-adressen i linjen “Received” i header-arket.
- Slå den op i IP-tabellen, og find udbyder og type.
- Diskuter: Hvad kan man se, og hvad kan man ikke se?
- Tallet i tabellen giver fragmentet IP.

Mission 3: Serverens placering (analog)

- Brug serverrapporten og kortet over datacentre.
- Find ud af, hvilket datacenter og land serveren står i, og skriv hvorfor det betyder noget.
- Det sidste ciffer i datacenterets kode giver fragmentet MAP.

Kassen (Akt 1 – slut)

- Brug fragmenterne HEADER, IP og KORT til at åbne kassen.
- I kassen ligger fragmentet KASSE, et chifferark og missionskortet til Akt 2.

Systemet genstarter (Akt 2)

- En ny nedtælling starter, og I går på jagt efter oplysninger til serveren.

Spor på skolen (papir og rum)

- Spor A: Scan QR-koden på gangen.
- Spor B: Find Admin-PC'en i lokalet. Hvad afslører menneskelige vaner, fx en seddel under et tastatur?
- Bonus: Hvis I finder en tabt USB-nøgle, hvad gør I så?

Mission 4: Adgang til serveren (digital)

- Brug oplysningerne fra sporene til at logge ind på øveserveren i CyberHack.
- Find nødkode-filen, og læs den.
- Tænk over: Hvad gjorde kodeordet nemt at gætte?
- Filen giver fragmentet FIL.

Mission 5: Den krypterede besked (analog)

- Brug chifferarket til at afkode en besked med et Cæsar-chiffer. Nøglen har I allerede fundet.
- Beskeden fortæller, i hvilken rækkefølge fragmenterne skal stå.

Outro: Slutkoden

- Saml alle fragmenter i den rigtige rækkefølge.
- Tast slutkoden ind, før tiden løber ud.

Opsamling

Prøv at svare på følgende spørgsmål:

- Hvilke tegn afslørede, at mailen var phishing?
- Hvad kunne I og kunne I ikke finde ud af ud fra en IP-adresse?
- Hvad gjorde kodeordet på serveren svagt, og hvordan laver man et stærkt?
- Hvilke spor i skolen afslørede menneskelige fejl, og hvorfor er det farligt?
- Hvad skal man gøre, hvis man finder en USB-nøgle, man ikke kender?
- Hvad er forskellen på en etisk hacker og en kriminel?
- Hvad ville I gøre, hvis I fik en lignende mail i virkeligheden?

Faglig forklaring+

Domæner og subdomæner: Det rigtige domæne står lige før endelsen. I lindeholmskole.skolelabs.dk er domænet skolelabs.dk, ikke skolens navn. Angribere bruger tit et subdomæne, der ligner en kendt adresse.

Serverplacering og jurisdiktion: En server står i et bestemt land, og landets love gælder for den. Derfor kan politiet ikke bare gå ind i en udenlandsk server. I EU og EØS gælder GDPR. En server i et land siger ikke noget om, hvor angriberen selv sidder.

Hosting: Man kan leje servere hos en udbyder, så en angriber kan sende mails fra en server i et helt andet land.

Phishing er forsøg på at narre dig til at give oplysninger eller klikke på et link ved at udgive sig for at være en betroet afsender. Typiske tegn er forkerte domæner, hastesprog og uventede vedhæftninger.

IP-adresse er en enhed på internettet, ligesom en adresse. Den afslører typisk udbyder og omtrentlig placering, ikke den præcise adresse. En VPN eller proxy kan skjule den.

Domæner og subdomæner: Det rigtige domæne står lige før endelsen. I edbit.login-sikkerhed.skolelabs.dk er domænet skolelabs.dk.

Adgangskoder: Lange, unikke koder og tofaktorlogin beskytter bedre end korte og genbrugte. En password manager gør det nemt.

Social engineering er at udnytte mennesker frem for teknik, fx ved at finde kodeord på post-its eller en tabt USB-nøgle.

Kryptering gør data ulæselige uden en nøgle. Cæsar-chiffer er en simpel og gammel form, men princippet er det samme i moderne kryptering.

Etisk hacking betyder at teste sikkerhed med tilladelse for at forbedre den.

Lærervejledning+

Tid: 2 x 45 minutter inklusiv tid til opstart og opsamling.

Tid	Aktivitet	Form
Akt 1: 0-10 min	Snak om sikkerhed, hacking og phishing	Klassen
10-15 min	Mailen åbnes, lockdown starter (nedtælling 25 min)	Skærm
15-40 min	Mission 1, 2 og 3	Papir
40-45 min	Kassen åbnes	Rum
Akt 2: 0-3 min	Systemet genstarter (nedtælling 30 min)	Skærm
3-15 min	Spor A og B samt mission 5	Rum og papir
15-28 min	Mission 4: CyberHack	Skærm
28-30 min	Slutkoden tastes ind	Skærm
30-45 min	Opsamling	Klassen

Forberedelse:

- Aftal forløbet med skoleleder og IT-ansvarlig, så skolens systemer ikke reagerer på phishing-siden.
- Brug kun fiktive data: et fiktivt skolenavn og IP-adresser fra de reserverede testområder (fx 203.0.113.x).
- Phishing-siden skal have en dummy-login, hvor du selv taster opdigtede oplysninger. Ingen oplysninger må gemmes.
- Placer de fysiske spor før timen, og tjek at QR-koden kan læses på både telefoner og tablets.
- Indlæs scenariet i CyberHack, og gennemfør mission 4 selv én gang.
- Print opgavearkene og hint-kortene.

Organisering: Grupper på 3-4 (halv til hel klasse). Fordel roller: en læser, en skriver, en løber til de fysiske spor og en kodevogter. Højst to elever fra hver gruppe er ude på gangen ad gangen.

Balance mellem digitalt og analogt: Kun mission 4 og de to indtastninger kræver skærm. Mission 1, 2, 3 og 5, de fysiske spor og kassen foregår på papir eller i rummet. Hold øje med, at grupperne skifter mellem bord og rum.

Hints: Hver gruppe har 3 hint-kort. Brug af et hint koster 2 minutter på uret.

Bonus: Grupper, der afleverer en tabt USB-nøgle uden at sætte den i en computer, får 3 minutter ekstra.

Nødudgang: Hvis tiden løber ud, "genstarter systemet i sikker tilstand", og du giver slutkoden til alle. Opsamlingen er vigtigere end at have "vundet".

Differentiering: Hurtige grupper kan få bonusmissioner, fx en dybere analyse af mail-headeren. Grupper, der har brug for hjælp, får ekstra hints.

Til andre skoler: Scenariet til CyberHack kan eksporteres som JSON-fil og importeres på en anden skole, så skolerne kan tilpasse det til deres egne navne og rum.

Fagmål (teknologiforståelse): Digital myndiggørelse, kritisk vurdering af digitale kilder, forståelse for netværk og kryptering samt etisk refleksion.

Kildehenvisning+

- Center for Cybersikkerhed: cfcs.dk
- Sikker Digital (Digitaliseringsstyrelsen): sikkerdigital.dk
- Datatilsynet: datatilsynet.dk
- Straffeloven § 263 (uberettiget adgang til data): retsinformation.dk