Jens Myrup Pedersen (th.) er professor i cybersikkerhed ved Aarhus Universitet og landstræner for det danske cyberlandshold. Han forsker i blandt andet netværkssikkerhed og udvikler cyber-øvelser, der træner unge talenter i at tænke kreativt og finde sårbarheder i digitale systemer. Foto: Mads Nielsen.

Et digitalt escape room: Sådan lærer unge at hacke

På det danske cyberlandshold træner unge talenter i at bryde ind i systemer, finde skjulte sårbarheder og tænke som hackere. Det kan ligne et ondsindet spil, men i virkeligheden handler det om at beskytte et af verdens mest digitaliserede samfund.

Jesper Bruun · journalist, AU Engineering, Aarhus Universitet

JENS MYRUP PEDERSEN

Jens Myrup Pedersen er professor i cybersikkerhed ved Aarhus Universitet og landstræner for det danske cyberlandshold. Han er uddannet cand.scient. i matematik og datalogi fra Aalborg Universitet og har en ph.d. i computernetværk.

Hans forskning fokuserer blandt andet på netværkssikkerhed og på, hvordan man kan opdage og håndtere sårbarheder i komplekse digitale systemer. Derudover arbejder han med at udvikle realistiske cyberøvelser og konkurrencer, som træner evnen til at tænke kreativt og finde fejl i systemer. Som landstræner er han med til at udvikle unge talenter og styrke Danmarks kompetencer inden for cybersikkerhed.

jensmyrup@ece.au.dk

En profil på et socialt medie. Et billede af en burger. Et navn: Mr. Beef.
Umiddelbart ligner det bare endnu en bruger på endnu en platform, der poster alt lige fra jokes til memes og madopskrifter til mere eller mindre privat indhold.
Men noget stemmer ikke helt.
Måske har brugeren brugt det samme password flere steder? Måske afslører opslaget lidt for meget? Måske ligger svaret gemt i små detaljer, som kun den opmærksomme opdager?
Opgaven lyder enkel: Find ud af, hvem Mr. Beef er i virkeligheden. Men vejen dertil er alt andet end simpel.
Velkommen til træning i cybersikkerhed.

At tænke som en hacker

Rundt omkring ved computere sidder unge mennesker og leder efter spor. De klikker, analyserer, tænker sig om, tester og kombinerer informationer. Ikke for at bryde loven, men for at forstå, hvordan systemer kan brydes.

For Jens Myrup Pedersen, professor ved Aarhus Universitet og landsholdstræner for cyberlandsholdet, er det netop den måde at arbejde på, der gør cybersikkerhed fascinerende. Hvor man prøver forskellige veje og tænker kreativt for at finde løsninger.

»Hvad nu hvis man gør ting på en anden eller tredje eller fjerde måde? Eller i en rækkefølge, som ingen har prøvet før? Hacking er ikke bare en teknisk disciplin, men først og fremmest en kreativ disciplin. Det handler om, at man prøver noget af, som der ikke er nogen, der har tænkt på før,« siger han.

Cyberlandsholdet består af 10 unge i alderen 15 til 25 år, som udvælges gennem konkurrencer og træningsforløb. De repræsenterer Danmark ved internationale mesterskaber og træner gennem realistiske cyberopgaver.

De opgaver, landsholdet arbejder med, er dog væsentligt mere avancerede end de eksempler, man umiddelbart kan gennemskue. Her kræver det ofte, at man kombinerer flere teknikker, arbejder på tværs af systemer og holder overblik over komplekse sammenhænge.

»Grunden til, at vi har landsholdet, er også at give synlighed til cybersikkerhed og vise, at det er et spændende område for unge mennesker,« siger Jens Myrup Pedersen.

Sådan bliver en cyberopgave til

En god opgave starter ikke med kode. Den starter med en idé.

»Den gode opgave begynder tit ved et whiteboard, hvor der er en original idé og en god historie bag,« forklarer Jens Myrup Pedersen. Historien er afgørende. For hvis opgaven føles som et univers, bliver den også mere engagerende at løse.

»Vi laver opgaver, som man har lyst til at gå på opdagelse i. Det skal ikke bare være teknisk, men en oplevelse,« siger han.

Det kan være et socialt medie, en webshop eller et digitalt system. Men de er ikke bygget korrekt:

»Vi bygger faktisk sårbarhederne ind i den hjemmeside eller de systemer, man bruger til konkurrencen. Deltagerne skal så finde sårbarhederne og udnytte dem,« siger Jens Myrup Pedersen.

I de svære opgaver skal flere ting gå op på én gang.

»Hvis det skal være svært, skal der gerne være flere brikker, der skal falde på plads på samme tid, hvor man skal udnytte flere redskaber og sårbarheder på samme tid,« forklarer han.

Det er også her, forskellen for alvor viser sig: Hvor begynderniveauet kan handle om at finde enkelte spor, arbejder landsholdet med opgaver, hvor mange lag af systemer spiller sammen, og hvor løsningen kræver både erfaring, kreativitet og vedholdenhed. Det er kun de allerdygtigste, der når til det niveau.

Hvem er Mr. Beef?
Tilbage til opgaven med at finde ud af, hvem Mr. Beef er:

Her har nogle af folkene bag De Danske Cybermesterskaber bygget et helt netværk af brugere, opslag og relationer. Det ligner en rigtig platform, men er i virkeligheden en nøje konstrueret opgave.

Mr. Beef er én af brugerne. Han poster billeder. Kommenterer. Liker opslag. Ved første øjekast er det ligegyldigt. Men for en hacker er det spor. Et opslag kan afsløre en vane. Et like kan afsløre en interesse. Et billede kan afsløre noget i baggrunden.

»Det kan være, at en bruger poster et billede, hvor man kan ane en post-it med brugernavn og password,« siger professoren.

Et andet spor kan være mere subtilt.

»Man kan måske gennemskue sammensatte spor og i sidste ende gennemskue password til en af brugerne, fordi vedkommende liker en post, hvor der står, at man kan lave passwords efter navnet på ens kæledyr og fødselsår eller sådan noget lignende,« forklarer han.

Så begynder arbejdet. Man finder kæledyrets navn. Man finder fødselsåret. Man tester kombinationer. Langsomt samler billedet sig.

»Ved at lægge de informationer sammen kan man så bruge det til at finde frem til ting, der gør, at man kan komme ind i systemet. Lige som et escape-room med små spor, der samlet giver en opgave, der gør, at man føler, at man kommer tættere og tættere på.« Opgaverne er ikke tilfældige. De afspejler virkeligheden.

»Vi træner ikke folk i at være ondsindede hackere, men noget af det, vi træner folk i, er at lære sårbarhederne at kende, så man ikke laver dem i de systemer, man selv laver, og at finde sårbarhederne hurtigt, så man kan lukke dem, før ondsindede hackere finder dem,« siger Jens Myrup Pedersen.

Den type fejl findes overalt: Genbrugte passwords. For mange oplysninger på sociale medier. Systemer, der ikke er tænkt sikkert fra starten. Det er ikke avancerede hacks. Det er blot menneskelige utilsigtede fejl.

Eksemplet med Mr. Beef er en forsimplet version af den type opgaver, deltagerne møder. I virkeligheden er opgaverne på cyberlandsholdets niveau langt mere komplekse og kræver, at man kombinerer flere forskellige sårbarheder, arbejder på tværs af systemer og ofte løser flere trin i den rigtige rækkefølge for overhovedet at komme videre.

Når 400 unge hacker hinanden
Cybersikkerhed har ry for at være svært og snævert. Det forsøger cyberlandsholdet at ændre.

»Vi vil gerne gøre det endnu mere tilgængeligt for alle, også dem, der kun har en halv time af en arbejdsdag på en måned, de kan dedikere til cybersikkerhed,« siger Jens Myrup Pedersen og fortsætter:

»Vi vil gerne tale til alle og ikke kun de allermest nørdede drenge, så vi kan få mere diversitet ind.« Derfor handler opgaverne også om for eksempel sociale medier, data og privatliv.

»Hvis man åbner det op og inddrager data og måden, man bruger sociale medier på, og beskyttelse af privatliv, så er der pludselig en meget større gruppe, som synes, det er spændende. Cybersikkerhed er super vigtigt for hele samfundet,« forklarer han.

Ved de europæiske mesterskaber skifter tempoet.

»Når vi holder de europæiske mesterskaber, er der både opgaver og attack-defence dage, hvor 400 unge mennesker sidder og hacker hinanden på kryds og tværs. Det er mega fedt,« siger professoren.

Her arbejder holdene både med at angribe og forsvare. De skal beskytte deres egne systemer og samtidig forsøge at bryde ind hos de andre. Cybersikkerhed i praksis.

AI: En ny med- og modspiller
Tilbage til Mr. Beef. Forestil dig nu, at du ikke selv behøvede finde sporene. Forestil dig, at du kunne få en kunstig intelligens til at gøre det for dig. Den kunne analysere opslag. Finde mønstre i adfærd. Gætte sandsynlige passwords. Alt sammen på få sekunder. Det er ikke science fiction. Det er virkeligheden i dag. I løbet af få år har kunstig intelligens ændret cybersikkerhed markant.

»AI betyder rigtig meget i den her verden. Det ændrer både angrebet og forsvaret,« siger Jens Myrup Pedersen.

Hvor phishing-mails tidligere ofte var lette at gennemskue med dårligt sprog og generiske formuleringer, kan AI i dag eksempelvis skrive beskeder, der er sprogligt korrekte og tilpasset den enkelte modtager.

Med dens hjælp kan en angriber for eksempel analysere dine sociale medier og lave målrettede angreb og skrive personlige phishing-mails. Og AI kan efterligne stemmer eller personer eller teste tusindvis af password-kombinationer intelligent.

»Det kan for eksempel være i phishing-angreb, hvor AI'en kan være rigtig stærk til at skrive gode phishing-mails, der er målrettet enkelte personer, så det fremstår meget troværdigt,« siger professoren.

Det, der tidligere krævede tid og ekspertise, kan nu udføres hurtigere og med færre ressourcer. Én person kan potentielt ramme tusindvis af mål med skræddersyede angreb. Det gør angreb hurtigere, billigere og mere præcise. Og ved at analysere store mængder kode eller netværkstrafik kan algoritmer

Jens Myrup Pedersen sammen med det danske cyberlandshold i 2025. Landsholdet består af unge talenter fra hele landet, som trænes i at finde og forstå sårbarheder i digitale systemer og repræsenterer Danmark ved de europæiske cybermesterskaber. Foto: Lasse Møller Badstuen

■

FAKTA OM CYBERLANDSHOLDET

Det danske cyberlandshold består af 10 unge i alderen 15 til 25 år, som udvælges gennem konkurrencer og træningsforløb. De trænes i at finde og udnytte sårbarheder i digitale systemer med det formål at lære, hvordan man opdager og forebygger cyberangreb.

Landsholdet repræsenterer Danmark ved de europæiske cybermesterskaber, European Cybersecurity Challenge (ECSC), hvor unge fra hele Europa konkurrerer i cybersikkerhed. Her arbejder deltagerne både med at analysere sårbare systemer og med at angribe og forsvare digitale infrastrukturer i realistiske scenarier.

Formålet er både at udvikle de bedste talenter og at skabe interesse for cybersikkerhed i en tid, hvor behovet for kompetencer er kraftigt stigende. Cyberlandsholdet er finansieret af Industriens Fond.

identificere svage punkter langt hurtigere end et menneske.

»Efter min vurdering har det gjort det klart lettere for angriberne,« siger Jens Myrup Pedersen. Samtidig bliver forsvaret sværere.

»Det hænger sammen med, at cybersikkerhed er en asymmetrisk konkurrence, hvor vi på forsvarssiden skal vinde hver gang. Bare angriberne kommer igennem én gang, har de vundet. Det forsvar, vi laver, skal virke hver gang,« forklarer han.

AI forstærker den ubalance.

Derfor er det vigtigt

Cybersikkerhed er blevet en forudsætning for samfundet, og behovet for mennesker, der forstår det, vokser.

»Der er rigtig meget brug for talenter,« siger Jens Myrup Pedersen. Men det kræver, at flere får lyst til at engagere sig.

»Hvis vi ikke har de der elementer med gamification og rewards og escaperoom, så er der mange, der allerede fra starten siger: "Nej det er for svært, det kan jeg ikke finde ud af", så det kan virkelig noget,« forklarer han.

Når det bliver en oplevelse, ændrer det noget. Når deltagerne forsøger at afsløre Mr. Beef – eller langt mere komplekse opgaver på landsholdsniveau – handler det ikke kun om at løse en opgave.

De lærer at tænke. At stille spørgsmål. At se mønstre. At være nysgerrige. Og vigtigst af alt: At digitale systemer aldrig er perfekte. Det er den erkendelse, der gør dem i stand til at bygge bedre løsninger.

Cyberlandsholdet fungerer samtidig som en form for talentudvikling på et område, hvor behovet for kompetencer vokser, og hvor samfundet i stigende grad er afhængigt af, at flere kan forstå og arbejde med cybersikkerhed. For i sidste ende handler det ikke om at hacke. Det handler om at forstå og beskytte. ■