

# Vi burde uddanne hackere: cand.hack

Danmark er ved at tabe krigen mod ondsindede hackere, mener en af landets mest erfarne 'hvide hatte' – folk, der hacker it-systemer for at finde fejl. Hvis USA's militær hyrer spilnørder til at flyve droner, hvorfor så ikke spejde efter fremtidens cyberpoliti allerede i folkeskolen?



ADAM HANNESTAD

Når Henrik Limkilde træder ind i et lokale, virker han ikke som en person, man skal være bange for. Den trinde og rundkindede 48-årige mand har venlige øjne og let til latter, og den sorte hawaiiiskjorte blødgør det *corporate image*, der ellers udsendes af det faste håndtryk, de blankpolerede sko og det schweiziske Breitling på hans håndled.

Men tag ikke fejl: Henrik Limkilde er en farlig mand. Han er højt kvalificeret hacker, et af de mennesker, der er i stand til at få computernetværk til at rulle rundt og gå på kommando. Og hans arbejde er at bryde ind i it-systemer på alle tænkelige måder – også dem, der lyder som en spionfilm.

Som når han henkastet taler om dengang, han inficerede et system ved at smide et usb-stik, hvorpå han havde fået skrevet »PET«, Politiets Efterretningstjeneste, på et firmas parkeringsplads.

»Der gik kun få minutter, så var der en, der havde samlet det op og sat det i en computer. Så var vi inde«, siger han med et grin.

Heldigvis er firmaerne i gode hænder. For Henrik Limkilde har titel af *certified ethical hacker*: Han har et internationalt diplom på, at han gerne må hacke sig ind i netværk for at finde fejl, og at han er forpligtet til aldrig at misbruge det, han finder ud af, men tværtimod advare om fejl eller brister.

Til daglig er han leder af et seksmandshold i it-selskabet Axxess, som ejes af det norske konsulentfirma Atea. Holdet er det, man i faget kalder hvide hatte: It-verdens sheriffer, der bekæmper cyberkriminalitet, et emne, der den seneste uge har været i fokus på grund af det globale afpresningsangreb med virussen WannaCry.

Det såkaldte ransomwareangreb blev netop stoppet, da hvide hatte hurtigt

fandt en måde at bekæmpe den på. Men angrebet var en advarsel om, at vi skal forberede os på meget værre sager, mener han.

»Man skal huske, at ransomware er det aller, alle, allersidste, du bliver ramt af. Inden da har hackeren prøvet at finde ud af, om han kan finde oplysninger i systemet: Er der kreditkortdata, man kan sælge? Er der hemmelige informationer om firmaet, for eksempel om en børsnotering, man kan give til konkurrenten? Det får han meget mere ud af. Men hvis man ikke kan få fat i noget, så smider man ransomware efter dem. Så har man da fået lidt ud af arbejdet«.

## Den uheldige receptionist

I Axxess foregår holdets arbejde ved, at firmaer beder om at få testet deres systemer. Især ved det, der kaldes penetrationsanalyse, altså det klassiske forsøg på at trænge igennem de elektroniske forsvarsforbindelser på distancen.

Men det er ikke nok at have en god firewall eller en årvågen it-afdeling. Hvis man helt vil undgå angreb, handler det også om at have en god it-kultur og lære alle medarbejdere, hvad de skal gøre.

»Et af vores skræmmeksempler er en kunde, hvor receptionisten blev ramt af ransomware. Hun fik at vide, at hun bare skulle slukke skærmene og gå hjem, for hun kunne jo ikke arbejde den dag. Det gjorde hun så, men da hun kun slukkede skærmene og ikke selve pc'en, fik virussen så lov til at stå og kryptere hele virksomhedens system hen over natten«.

Det er også en god idé at tænke over, om hackerne bare kan gå stille og roligt ind ad fordøren. Har man sat en bøjle i døren, fordi det er varmt, og alle pc'erne er låst op? Den slags sker, si-

ger Henrik Limkilde.

Et andet problem er mange ansattes tendens til ikke at spørge, hvem man er.

»Jeg har været udlånt til et firma, hvor vi aftalte, at jeg skulle sidde i chefens stol så længe som muligt. Så der sad jeg iklædt en Microsoft-bluse og brugte pladsen. Der gik en hel uge, fordi ingen turde spørge. Den første, der spurgte,



**DEFCON.** Kranieemblemet fik Henrik Limkilde i 2016 på hackerkongressen Defcon i Las Vegas. Hvide hatte, som han selv, er uglesete her, men tolereres. Kraniet er en minicomputer med en ultrasvær indbygget kode, og der er høj blæreværdi i at hacke den.

Foto: Jacob Ehrbahn



var en, der ville vide, om jeg ville med i fredagsbaren«.

## Tøjet betyder alt

»Jeg har været til en konference, hvor jeg mødte op i hættetrøje, solbriller og en sort T-shirt med ordet 'hacker'. Fire-fem personer spurgte mig, hvem jeg var. Men da jeg gik ud og skiftede til skjorte og jakke og kom ind igen, var der ingen, der spurgte mig om noget – ud over om de skulle hjælpe mig med at sætte mit udstyr op«.

Henrik Limkilde har længe studeret kulturen i hackermiljøet, og for fem år

siden skrev han på opfordring en manual til Politiskolen om profilering af hackere. Af den fremgår, at man skal passe på med at hænge sig i klicheer om utilpassede og indadvendte unge. Blandt de mest dominerende karaktertræk – ud over gode matematiske evner – er behovet for anerkendelse.

»Hvis du for eksempel er blevet mobbet, hvis din sociale arv ikke er i orden, og hvis du er teknisk anlagt, så er der stor sandsynlighed for, at du har nemmere ved at falde i og blive fristet«, siger han.

»Folk starter typisk som *script kiddies*

# eller cand.cybercrime



med at inficere en hjemmeside og skriver deres gamernavn på den. Så bliver det anerkendt for et eller andet».

Han erkender, at han sagtens selv kunne være endt på den side af loven. Han kommer fra en håndværkerfamilie og kom lidt tilfældigt ind i it-verdenen. Han fik i en ung alder job som supporter hos IBM og Danmarks Lærerhøjskole. Her var det tæt på at gå galt, for sammen med en kollega hackede han skolens it-system for sjov. Næste dag måtte han stå skoleret for rektor, der ville vide, »hvad fanden de havde gang i«.

»Der lærte jeg for første gang, at der er

systemer, der holder øje med, hvad man laver, så man skal holde snitterne væk. En hackers opgave er at skjule sine spor, det er det vigtigste for ham. Det var faktisk mit held, at jeg blev fanget, for ellers kunne jeg i dag have været lyssky og siddet i en mørk kælder. For selvfølgelig bliver man ... Altså, man tænker, nogle tjener 2-3 millioner om måneden på at hacke. Man kan let blive fristet«.

#### Et lille råd: Ansæt de kriminelle

*Kan man overhovedet være en god hvid hat, hvis man ikke selv på et tidspunkt har siddet og lavet noget lidt gråt – eller sort?*

»Nej, i mine øjne kan man ikke. Du bliver nødt til at have noget kendskab til, hvor hackeren sidder, og hvad hans tankegang er. Det er den gamle historie om, at en politimand skal kunne tænke som en kriminel for at fange ham«.

De færreste firmaer vil i dag ansætte folk, der har en dom for it-kriminalitet. Det er en stor fejl, mener Henrik Limkilde.

»I princippet burde man jo tage dem, der har aftjent deres værnepligt – der har afsonet deres dom – og så bruge dem til Yahooat komme videre. Men mange vil ikke tage dem, der har en straffeattest«.

#### HVID HAT.

**Henrik Limkilde arbejder til daglig med at forebygge og forhindre indbrud i it-systemer. Danmark er ved at tage kampen mod hackerne, mener han. Foto: Jacob Ehrbahn**

## ORDLISTE

### Hackertyperne

**Hacker:** En, der skærer ting op. Siden ca. 1975 brugt om computerkodeentusiaster, ofte negativt; egentlig er ordet neutralt

**Cracker:** En angribende eller kriminel hacker. Stammer fra udtrykket 'cracking a safe' – at bryde ind i et pengeskab

**Black hat:** Computerskurk. Udtrykket skyldes en joke om, at skurken i westerns ofte har sort hat på

**White hat:** Computerhelt, der hacker for at forsvare data. Den sorte hats fjende

**Grey hat:** En hacker på kanten af loven

**Certified ethical hacker (CEH):** Person med diplom i computerforsvar. Professionel hvid hat

**Script kiddy:** 'Kodebaby', nedsættende udtryk om hacker, der kun bruger andres programmer uden at skabe noget nyt

*Kan man groft sagt tale om, at der er en magtbalance mellem black hats og white hats?*

»Ja«.

*Hvem vinder?*

»Det gør black hats«.

*Hvorfor?*

»Fordi vi ikke får uddannet nok mennesker i Danmark til at være på den rigtige side. Forsvarets Efterretningstjeneste og politiet får ikke de mennesker, de skal bruge, fordi de ikke er villige til at betale for dem. De dygtige folk vil ikke have 38.000 kroner om måneden i det offentlige for det, de kan, når de ved, at de kan få det dobbelte plus alle frynsegoderne i det private erhvervsliv«.

I det hele taget er det offentlige Danmark slet ikke god nok til at forstå, hvor vigtigt emnet er, mener han.

»Vi har ingen uddannelse i hackere, fordi det er et farligt ord, men i princippet burde vi uddanne hackere: cand. hack eller cand.cybercrime. Det burde være sådan, at vi uddannede folk enten til at hacke for os som stat eller til at forsvare os mod angreb fra andre steder. Det er vi rigtig dårlige til i Danmark, men jeg tror, at det bliver vi nødt til. Vi skal snuppe de unge efter 10. klasse, ligesom man i udlandet tager dem, der er gode til flysimulatorspil, og bruger dem til at flyve droner for militæret. Vi skal have fat i dem, der sidder i skolen og knækker sudoku – deres hjerner skal vi have ind og forsvare Danmark, for ellers har vi allerede tabt«.

Han tager en dyb indånding, før hans ansigt flækker i et af de karakteristiske brede grin:

»Den sikreste måde, du kan redde dig selv fra alt det, der foregår, er ved ikke at være på internettet. Og pøj-pøj med det, siger jeg bare«.

adam.hannestad@pol.dk