ITReload

https://itreload.dk/artikel/sikkerhed/ai-driver-fremtidens-sikkerhed
AI driver fremtidens sikkerhed
03/10/18

Rik Turner (tv), Jan Guldentops, Roark Pollock og Simon Crumplin snakker som it-sikkerhed og AI. Foto: Lars Bennetzen

AI driver fremtidens sikkerhed

Trusler fra internettet bliver stadig mere alvorlige og problematiske. Samtidig er eksisterende teknologier ikke længere nok i kampen, kunstig intelligens er nødvendig for sikre både virksomheder og private

Af Lars Bennetzen

Det bliver stadig mere usikkert at have en forbindelse til det store internet, og samtidig er det nødvendigt for virksomhederne at være forbundet til omverdenen. Kunstig intelligens (AI, red) bliver derfor brugt i stigende grad for at hjælpe virksomheder til at beskytte sig selv.

”I dag står vi i en situation hvor traditionel antivirus-software maksimalt fanger mellem 30 og 40% af alle malware, og tallet er sikkert endnu mindre. Samtidig er de cyberkriminelle blevet langt mere avancerede. Vi snakker ikke længere kun om script kiddies, men om kriminelle bander, hacktivister og statssponsorerede grupper, og det gør truslerne langt

mere komplicerede," siger Rik Turner, Principal Analyst, Infrastructure Solutions hos Ovum til IT-Reload.

Samtidig er der kommet et meget attraktivt marked for værktøjer til at udvikle cyberangreb på Dark Web. Her er tilgængeligheden af værktøjer næsten uendelig og Rik Turner fortæller at det er let at få fat i dem.

"Du kan let finde ressourcer og endda køre lukkede og kontrollerede test inden du slipper din malware løs, og det gør det næsten umuligt at forudse et angreb," forklarer Rik Turner.

Nye teknologier nødvendige

Så hvor det for ganske få år siden var et stort hit at benytte sig af sandboxing i kampen mod cyberangreb, så har det også ændret sig.

"Sandboxing blev brug til at smide alt der bare var en anelse mistænkeligt ind i en sandbox, og så tjekke om det var ondsindet. Det var populært og teknologien blev hurtig spredt til alle antivirustjenester. Men hackerne skrev så bare kode der tjekkede om deres software var i en sandbox, og sikrede at koden ikke blev afviklet så længe den var i en sandbox," forklarer Rik Turner.

Da AI efterhånden var blevet ret avanceret, blev denne teknologi derfor taget i brug i kampen mod cybertrusler.

"Men hvorfor stoppe her, hvorfor kun bruge AI til at opdage trusler med? Hvorfor kan vi ikke bruge det til at forudsige trusler med. Jeg er sikker på, at brugt rigtigt så vil AI være med til at vi kan bruge det til at forudse, hvilke angreb du og din virksomhed risikerer at blive ramt af," siger Rik Turner.

Roark Pollock, Senior Vice President of Marketing hos Ziften Technologies, er ikke i tvivl om, hvorfor AI og Machine Learning er enig, og til IT-Reload siger han at det vigtigste spørgsmål er, hvorfor vi overhovedet snakker om AI i forbindelse med cybersikkerhed nu, for cybersikkerhed er ikke just nyt, og svarer selv på spørgsmålet.

"Dels er teknologien kommet så langt at den rent faktisk er brugbar, dels har vi adgang til data nok og dels er de enheder/endpoints vi kører AI på så stærke at det ikke sender dem i knæ at benytte AI til cybersikkerhed," pointerer Roark Pollock.

Signaturmodeller, som de fleste antivirusprogrammer i vid udstrækning benytter sig af, har været her i årevis, og de virker godt over for kendte trusler. Men de største trusler kommer fra ukendt malware.

”Når vi kender malware kan vi lave en signatur og dermed blokere den. Men den model tager omkring to uger, hvis vi er effektive, så et eventuelt hul kan være der i to uger eller længere. Så med signaturmetoden er du ikke beskyttet mod ukendt malware før den er fundet, en signatur er udviklet og den er sendt ud til din klient,” siger Roark Pollock og fortsætter:

”Samtidig er de fleste af vores sikkerhedsmodeller bygget op omkring filer. Vi leder efter filer vi kan finde, men hvad når jeg har en word-fil med indbygget makro der er ondsindet? Vi har jo tillid til filen, og de fleste metoder ignorerer disse filer. Derfor er AI og ML nødvendig.”

Mennesket kan ikke undværes

Det er dog nødvendigt at huske på, at ikke alle trusler er en risiko for alle virksomheder, nogle virksomheder er mere sårbare overfor bestemte trusselstyper end andre.

”Hvis jeg f.eks. rammes af en malware der stjæler kreditkortinformationer, men jeg ikke håndterer disse informationer, så har jeg ikke et akut problem. Det skal naturligvis stadig adresseres, men det er ikke på presserende,” siger Simon Crumplin, Founder & CEO hos Secrutiny til IT-Reload.

Derfor er det også nødvendigt med en menneskelig bagstopper, AI kan være godt men det er ikke en magisk pille der løser alle problemer.

”Hvsi det f.eks. er et menneske der står bag et målrette angreb, et man-in-the-middle-angreb, så vil AI og ML ramme ved siden af i op til 25% a alle tilfælder, så vi må ikke glemme den menneskelige bagstopper,” siger Simon Crumplin.

”Du skal huske på at vurdere, hvad det er du vil opnå med sikkerhed, og så bruge dine penge og ressourcer der. Det gælder i høj grad også med AI og ML,” slutter Roark Pollock.