By
Trine Gutubakken

april 20, 2018

Hacking - 5 nye teknikker og hvordan de forekommer

Ransomware Sikkerhet Phishing

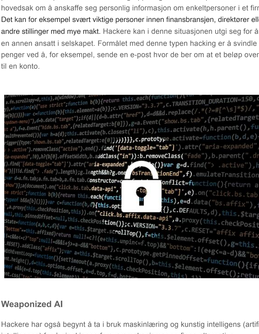
For en tid tilbake publiserte vi blogginnlegget: Hva er et virus? Enkelt forklart er et virus en skadelig programkode som blir kopiert inn i kjørbare filer og servere. Bare på den korte tiden fra da blogginnlegget ble publisert, har både ny teknologi og utvikling i markedet bidratt til nye former for cyberangrep. Disse er ofte vanskeligere å oppdage og håndtere. Det er derfor viktig at du og din bedrift vet hva dere må tenke på når det kommer til å sikre blant annet sensitiv informasjon og bedriftskritiske data.

De nyeste og største truslene

Metodene benyttet i forbindelse med hacking og skadelig programvare (malware) har blitt mer sofistikert. Nedenfor kan du lese mer om det som anses å være nåtidens største trusler innenfor cybercrime.

Cryptojacking

Ved cryptojacking tar en tredjepart kontroll over ressursene på din PC eller server for å utvinne kryptovaluta («mining»). Ofte bruker hackere andres datamaskiner til å utvinne kryptovaluta for dem. Cryptojacking kan forekomme ved at en nettside eller annonse er infisert med en JavaScript-kode som automatisk lastes opp i nettleseren. Koden vil løpe i bakgrunnen, mens datamaskinen kan brukes som normalt. Det eneste tegnet til at du kan være utsatt for cryptojacking er at hastigheten på PCen reduseres eller at PCen henger. Hovedgrunnen til at denne formen har blitt populær blant hackere er at de enklere kan få tilgang til mer valuta, med lavere risiko.



Data Hijacking

Denne formen for hacking foregår når en tredjepart stjeler sensitive data som de deretter bruker imot deg. Dette kan for eksempel være et krav om penger. Et eksempel er når persondata stjeles og man kreves for løsepenger mot at vedkommende ikke forteller myndighetene at de har klart å stjele persondata fra selskapet.

Whaling

Whaling er en spesifikk form for phishing («spear phishing»), rettet mot høyt profilerte enkeltpersoner eller mindre grupperinger i et selskap. Det handler i hovedsak om å anskaffe seg personlig informasjon om enkeltpersoner i et firma. Det kan for eksempel svært viktige personer innen finansbransjen, direktører eller andre stillinger med mye makt. Hackere kan i denne situasjonen utgi seg for å være en annen ansatt i selskapet. Formålet med denne typen hacking er å svindle til seg penger ved å, for eksempel, sende en e-post hvor de ber om at et beløp overføres til en konto.

Weaponized AI

Hackere har også begynt å ta i bruk maskinlæring og kunstig intelligens (artificial intelligence) for å gjenkjenne forsvarsmekanismer og finne alternative angrepsmetoder. De bruker kunstig intelligens til å bestemme seg for hva de skal angripe, hvem de skal angripe og når de skal angripe.

Fake Updates

Fake updates er i hovedsak malware som spres ved at gjerningspersonene legger inn en kode i legitime nettsider, som gjør at de besøkende får opp et nytt vindu. Eksempler på fake updates kan være falske oppdateringer til legitime sider som Chrome, Flash Player og Windows. En bruker vil få spørsmål om å oppdatere til for eksempel nyere versjon. Ved å oppdatere vil et virus installeres på maskinen.

Hvordan kan du beskytte deg?

- Aktivér Windows-sikkerhetsfunksjoner
- Hold alle programvarer oppdatert
- Vær forsiktig med å åpne uventede vedlegg eller linker i e-post
- Hold deg til godkjente sider når du surfer på Internett
- Ikke bruk piratkopiert materiell
- Opprettholdt gode sikkerhetskopier av dataene dine og test dem regelmessig

Det er viktig at PCen har det siste av oppdateringer. Når du laster ned en fil fra Internett, må du være sikker på at filen kommer fra en pålitelig kilde. En løsning kan være å scanne filen i et virusprogram. Man kan for eksempel bruke VirusTotal, et gratis verktøy som scanner suspekte filer og finner eventuelle virus eller malware. Et tips er å alltid bruke opprinnelig nettside for programmet når man skal oppdatere et program.
Virus spres ofte via e-post, og kan i mange tilfeller virke veldig pålitelig. Dersom man mottar en uventet fil må påliteligheten vurderes nøye, og du kan stille deg følgende kontrollspørsmål:

- Ser vedlegget eller linken ut som noe avsenderen kunne sendt deg?
- Samsvarer språket i e-posten med avsenderen?
- Ser URLen som dukker opp når du holder pilen over linken legitim ut?

Du kan lese mer om et av sikkerhetstiltakene her.

Konklusjon

Teknologien er i stadig endring og vi er mer tilkoblet enn noen gang. Med den raske utviklingen ser man også at IT-sikkerhet stadig blir utfordret av nye typer cyberangrep. Slike angrep er blitt mer sofistikerte og rammer stadig flere, og det er derfor viktigere enn noen gang at ansatte kjenner til hvordan de kan bidra til å minske truslene.

Legg igjen en kommentar

Navn*

Kommentar*

beskyttet av reCAPTCHA
Personvern Vilkår

Kommentér

Previous Post
SERVERFRI – neste generasjons IT-løsning

Next Post
OneNote skilles ut fra Office-pakken. Hva betyr det?