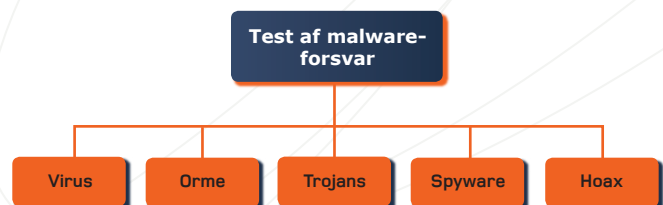


Malware koster hvert år danske virksomheder et større milliardbeløb, idet datas tilgængelighed, fortrolighed og integritet brydes. For at imødegå disse trusler er et effektivt forsvar mod malware nødvendigt. Ezenta tilbyder dybdegående sikkerhedstests af de applikationer der skal detektere og forhindre malware'en så som tests af virksomhedens antivirus-system.



Ezentas sikkerhedsspecialister gennemgår virksomhedens forsvar mod malware så som test af det implementerede antivirus-system. Systemets effektivitet vurderes, idet der bl.a. køres en række filer mod det. Disse filer inkluderer:

- Kendt malware
- Omdøbt malware
- Ompakket malware
- Recompiled malware
- Krypteret malware
- Malware gemt via steganografi
- Malware med signaturændring
- Ny (proprietær) malware
- Link til malware

Derudover besidder Ezentas sikkerhedsspecialister stor kompetence mht. eksisterende antivirus-systemer. Således kendes til en række svagheder og styrker i specifikke antivirus-applikationer.

Testen inkluderer alle former for malware. Dette omfatter virus, orme, trojanere, spyware og adware.

Virus & Orme

Virus er ondsindede programmer der spreder sig når brugeren kører dem. Virus påvirker ofte datas tilgængelighed og integritet og undtagelsesvis datas fortrolighed. Størstedelen af danske virksomheders tab som følge af malware skyldes virus-/ormeangreb, og de væsentligste udgiftsposter er oftest til genetablering af data samt tabt omsætning/produktivitet som følge af at data er gjort utilgængelige. Orme har samme funktionalitet som virus, idet de dog spreder sig automatisk (uden brugeren behøver køre dem) ved at udnytte sårbarheder i applikationer eller i et givent operativsystem.

Trojanere

Trojanere er programmer der udover evt. at gøre det som de lover, også har en skjult funktionalitet mht. at bryde datas tilgængelighed, fortrolighed og/eller integritet. Den trojanske hest vil ofte være afsendt af en hacker der ønsker at opnå kontrol over virksomhedens systemer. Flere af de mest udbredte trojanske heste tilbyder sniffing, keylogging, aflytning af webcams/mikrofoner m.v. Ezenta ser ligeledes en begyndende tendens til at de trojanske heste selv opretter forbindelse til f.eks. en server på Internettet som hackeren har kontrol over. Dermed vil den inficerede klient kunne styres fra Internettet, selv hvis firewallen ikke tillader indgående trafik mod den pågældende klient og f.eks. kun tillader udgående HTTP-trafik.

Spyware og adware

Spyware og adware bliver ligeledes mere og mere udbredt. Denne type malware installeres typisk sammen med et program, som brugeren har valgt at installere. Information om malware'ens eksistens findes til tider "skrevet med småt" i programmets licensbetingelser, men det er langt fra altid tilfældet. Malware'en spionerer på brugerens adfærd og får f.eks. målrettede og uønskede reklamer til at poppe op og/eller sende information om brugerens adfærd ud til en ukendt server på Internettet. Spyware der keylogger eller sniffer information ses ligeledes, måske hijacker spyware'en browseren, og enkelte spyware programmer lader sig styre af deres ejer direkte fra Internettet. Da malware'en ofte vil ligge på interne maskiner kan de informationer som der sendes ud være særdeles følsomme.