IT-säkerhet – för hemmaanvändare och fellow hams

Henrik Persson

hp@sa3bpe.se

Virus, trojaner och maskar

- Datorvirus “infekterar” ett program genom att hänga sig fast vid det, ungefär som naturens virus angriper ett djurs eller en människas kropp.
- Till skillnad från virus, som infekterar vanliga program, kan trojanen existera helt för sig själv.
- Till skillnad från virus är maskar fristående program som inte behöver infektera en viss fil för att infektera en dator. Sprids via nätverken och dess olika protokoll.

Vad kan virus, trojaner och maskar göra för skada?

- Avlyssna ALLT du gör på datorn..
- Leta i filsystem efter dokument.
- Skicka ut spam, dvs skräppost.
- Fjärrstyra datorn.

- Krångligt och osäkert att använda virus, trojaner och maskar för hackning, det kan dock vara ett bra komplement till en fullbordad attack.

Mjukvara & OS

- Ha bara det du behöver och använder installerat på datorn.
- Se till att hålla mjukvara och OS uppdaterat.
- Windows 7 och tidigare ver av detta OS ska du ALDRIG använda ONLINE.

Skydd, dvs sk Antivirus

- Det finns inget 100% skydd!
- Ny kod som inte är analyserad täcker oftast inte in av AV-skyddet.
- Var försiktig när du laddar hem filer! Man kan dölja mjukvara i t ex PDF:er och andra filformat. Genomsök ALLTID filer innan du öppnar de med ditt AV.

Nätfiske, sk ”phishing”

- En angripare lurar av dig information.
- Lämna ALDRIG ut användarnamn eller lösenord. ALDRIG!!!!
- Behöver du skicka uppgifter? Dela då upp informationen, dvs skicka användarnamn i ett email och lösenord som exvis en bild i ett MMS.

Var källkritisk! Ett email som ser ut att komma från din kompis kan vem som helst skapa.

Motring! Be att få ringa upp.

Trådlösa nätverk

- Använd kryptering. Minst WPA2.
- Anslut inte till öppna nätverk.
- Surfa inte på sk loungenätverk
- Använd ALLTID VPN-uppkoppling om du måste ansluta till andra nätverk än ditt hemma- eller företagsnätverk.

Webbadresser och surfning

- Logga ALDRIG in på en okänd site med http
- Kontrollera så att https används!
- Använd en cookieblocker. Cookies är en liten textfil som sparas på din dator och kan användas i allt från statistik till att följa ditt användande av olika nätverk.
- Tillåt bara de cookies som används för anonymiserad statistik. Eller åtminstone de cookies som gör tjänsten/sidan användbar.

Lösenord

- Använd ALDRIG kortare lösenord än 11 tecken. Alla lösenord som kan tänkas finnas med 8 tecken eller mindre är redan knäckta och finns i databaser som florerar på Internet.
- LÖSENORDSHANTERARE- använd detta! En bra och gratis sådan är KeePass, se https://keepass.info/

E-post

- Mejla ALDRIG användarnamn och lösenord tillsammans.
- KRYPTERA!!! PGP-kryptering är mycket bra (Pretty Good Privacy).
- Kom ihåg att kryptera både själva e-mailet OCH ev bifogade filer!
- Din adress syns fortfarande trots kryptering, det är en del av epostsystemet och går ej att komma runt.

Mobilen…

- SKA skyddas och hanteras precis som datorn…
- Android det vanligaste OS för trojaner, virus och maskar.
- IOS då? Börjar komma mer och mer sofistikerad skadlig kod för detta.

Radera filer, hålla rent på datorn

- Radera filer som innehåller känslig information om du kan.
- Datat raderas inte bara för att du raderar filen, du talar då bara om att utrymmet på disken kan skrivas över om så behövs.
- MacOS har funktionen ”Secure Empty Trash”, använd den!
- Windows kräver extra mjukvara för detta, exvis Dr Wiper
- Formatera och byt helst disk om du ska sälja eller byta dator.

- Hantera mobilen lika, aktivera ”remote wipe” så du kan radera remote om mobilen blir stulen eller tappas bort.

Ställ krav, ställ frågor!

- Var är min data i molntjänster?
- Hur lagras mina lösenord?
- Testa de olika systemen i skarpt läge innan du börjar skicka känslig information. Hur återställer jag ett lösenord? Kommer det i klartext i vändande mejl?

Brandvägg och nätverk

- Använd ALLTID brandvägg. Stryp access så mycket du kan och öppna upp portar och protokoll efterhand och behov.
- Använd automatiska funktioner för de olika attacktyperna som kan förekomma på nätverket. Jobba med blacklists och klassificera attacker i ”stage lists”.
- SSH, FTP, Telnet och WWW.

Smarta saker, IoT…

- Segmentera ditt nätverk så att dina smarta saker inte kommer åt NAS, Servrar och datorer med känslig data.
- Smarta saker innehåller en liten dator och kan ställa till stor oreda.
- Tänk dig 200 000 kylskåp som står och spammar…
- Eller att kaffekokaren bara sprutar varmvatten…

Läs mer på MSB’s hemsida om detta!
https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/sakerhet-i-cyberfysiska-system/internet-of-things--iot/

GDPR

- Nyttja GDPR! Begär att din data och uppgifter raderas om du inte har ett giltigt affärsavtal.

Vanliga attackytor idag

- RDP – Remote Desktop Protocol, dvs fjärrskrivbord
- Nätfiske, phising
- Osäkra VPN-servrar och klienter

Läs!

- It-säkerhet för privatpersoner – en introduktion av Daniel Goldberg och Linus Larsson, ISBN 978-91-87437-05-2

Häng med i svängarna på följande siter

- https://www.bleepingcomputer.com/
- https://kryptera.se/
- https://www.facebook.com/groups/sakerhetsbubblan/

Tack för mig!