Kryptovirus

Skulle din verksamhet överleva en större dataförlust?

Vad gör du för att förhindra en attack och är ni förberedda på hur ni agerar om det skulle hända? Vi har sammanställt några enkla tips kring åtgärder och hur man ska tänka.

Var försiktig!
Det absolut viktigaste är att utbilda användarna i hur de ska tänka och att de är försiktiga när de öppnar e-post till exempel. Om det finns osäkerheter kring innehållet i ett mail – öppna mailet i en mobiltelefon och då helst en iPhone.

Skydd på alla nivåer
Det vanligaste sättet att bli drabbad av kryptovirus i sitt nätverk är via e-post, alternativt att någon klickat på en olämplig länk i sin webbläsare eller installerat ett program som laddats ner från Internet. Användare, leverantörer och konsulter använder många olika typer av enheter vilket gör det svårt att förhindra virus i nätverket. Det är därför viktigt att skydda inte bara datorer, utan även servrar och brandväggar. På detta sätt kan man isolera viruset till endast en dator och undvika spridning till andra datorer eller servrar, med betydligt allvarligare konsekvenser.

IT-Tjänster

Vi är specialister inom IT och tillgodoser era behov och gör er vardag enklare. PrimeQ levererar IT-drift-, support, moln- och konsulttjänster. Vi vet hur viktigt det är att IT-lösningarna fungerar för att verksamheten ska flyta på och vi lägger stor vikt vid personlig service och tar fram system som är noggrant anpassade utefter era behov.

Vill du veta mer om våra IT-tjänster eller PrimeQ?

Vänligen kontakta:
sales@primeq.se

Checklista

Bra att veta om generell IT-säkerhet

Visste du att det just nu finns över 16000 infekterade datorer bara i Sverige? Se realtidsdata över infekterade datorer på https://cert.se

---

Skydd på alla nivåer

Dator: Vi rekommenderar starkt att en installation av Webroot eller liknande malware skydd på samtliga datorer. Se också till att era datorer har de senaste säkerhetspatcharna.

Server: Underhåll era servrar med de senaste säkerhetspatcharna och installera Webroot eller liknande skydd på servrarna. Framförallt på fil- och TS/RDS-servrar.

Brandvägg: Se till att ni har en brandvägg som har stöd för malware/botnet skydd. Detta är en funktion som ofta finns i mer avancerade brandväggar, men väl värt investeringen då det oftast stoppar ett kryptovirus från att aktiveras, även om det kommit in i er miljö.

E-post: Kontrollera att ni har ett bra centralt spamskydd för er e-post.

Allmänt säkerhetstänk

Access: Om dina användare har access till servrar direkt via RDP/TS, se till att använda VPN/Gateway eller begränsa till access från exempelvis vissa datorer eller platser. Detta är det absolut vanligaste sättet att infektera, näst efter e-post.

Lösenord: Tvinga dina användare att byta lösenord ibland. Ännu viktigare är dock att kräva ett komplext lösenord.

Checklista

Bra att veta om generell IT-säkerhet

Om olyckan ändå är framme

Information: Informera era användare att om de misstänker virus – stäng av datorn och dra ut nätverkssladden OMEDELBART! Kontakta därefter IT.
Säkerhetskopiering: Se till att du har fungerande backuper och inte bara filbackuper utan riktiga ”Image backuper”.
Återläsning: Säkerhetskopiering i all ära men det är återläsning som är det viktiga. Hur lång tid tar det att läsa tillbaka, är all data återläsningsbar, har ni testat att läsa tillbaka er miljö?
Dekryptering: För vissa kryptovirus finns dekryteringsprogram framtagna. Se mer på www.nomoreransome.org.

Var ska vi börja?

- Börja med att utföra en säkerhetsscanning av ert nätverk för att ta reda på status och eventuella brister.
- Installera Webroot SecureAnywhere på samtliga datorer och på servrar.
- Se över era brandväggar och uppgradera till en brandvägg med malwareskydd.
- Utbilda användarna i hur de ska agera.
- Gör en återläsningsövning på era affärskritiska system för att kontrollera om det går att göra en återläsning samt hur lång tid det kan tänkas ta.

Vill du veta mer om hur vi kan hjälpa er med IT-säkerhet?
Vänligen kontakta: sales@primeq.se
eller läs mer på webbplats https://www.primeq.se