● Brandvägg, koder, lösensummor och hackers. IT-säkerhet kan kännas abstrakt, men samtidigt är det något som berör allt fler. För IT-branschen är säkerhet ett växande affärsområde.

Att fysiskt förstöra hårddiskar till datorer kan verka drastiskt, men det är ett av få sätt där man kan garantera att informationen som funnits på disken inte går att återskapa. Christian Hellemar, affärsområdeschef för IT på Front, demonstrerar hur en hårddisk ser ut efter att den körts i deras kross.

Säkerhet som affärsidé: ”Man får vara extra misstänksam”

BORÅS. Christian Hellemar öppnar upp ett dokument på datorn, där det står ”Hope for the best, plan for the worst”.

Det är mycket av det som säkerhetsarbetet inom IT går ut på. Att hoppas på det bästa, men förbereda sig för det värsta.

Men något hundraprocentigt skydd finns inte. Att vara vaksam är Christian Hellemars bästa tips.

– Som privatperson får man vara extra misstänksam och kritisk framöver, tyvärr. Exempelvis betonar bankerna hela tiden att ingen hos dem någonsin kommer att begära att du ska nollställa ditt lösenord.

Christian Hellemar är affärsområdeschef för IT på Front, tidigare var han vd för Switch-IT som vid årsskiftet slogs ihop med systerbolaget Mediacad. Bolaget är en del av den Boråsbaserade Hydia-koncernen, som har verksamheter inom allt från skog och fastigheter till ventilation och vatten. Där sköter Front IT-driften, men de har också externa kunder.

För Front är säkerhet en viktig del av affärsmodellen. Medvetenheten och efterfrågan har ökat ute bland kunderna, enligt Christian Hellemar.

– Det är lättare att sitta och prata med kunder om det nu. Man blir annars lätt fartblind när allt fungerar, och först när något händer inser man hur sårbar man är. Men vi får ändå tjata om vissa grejer, säger Christian Hellemar.

Ett problem som fått allt mer uppmärksamhet är så kallad ransomeware, där hackare tar innehållet på ett företags servrar som gisslan.

– Det är virus precis som på 80- och 90-talet, men den krypterar allt den kommer åt på serverar, datorer, med mera. Sedan får man en länk och en lösensumma som ska betalas, ofta i bitcoins.

Lösningen i det här fallet stavas backup.

– Vi har varit med om att kunder drabbats av ransomeware två gånger, och båda gångerna har det fungerat att återställa innehållet med backups. Rådet är att inte betala lösensumman, för man vet ändå inte om man får tillbaka innehållet.

Det gäller också att ha ett uppdaterat skydd och att hålla medarbetarna informerade. Christian Hellemar berättar att 94 procent av all så kallad ransomeware förra året tog sig in i systemen genom e-post, men att det också kan ta sig in genom exempelvis hemsidor man besöker.

– Den stora massan av hackarna är inte så duktiga, utan de går någon kurs och sitter sedan med färdiga verktyg och jobbar.

En annan säkerhetsrisk är så kallade vd-mejl, där någon utger sig för att vara vd för ett bolag. I ett fall som Christian Hellemar känner till fick ekonomichefen ett mejl från vd:n om en transaktion som skulle göras till ett konto i USA.

– Den gången gick det att stoppa. Det man kan lära sig är vikten av att se över sina rutiner för hur betalningar ska göras, säger Christian Hellemar.

– Ett annat vanligt problem är fishing-mejl eller telefonsamtal, där någon hör av sig och uppger att de är från Microsoft och säger att de behöver fjärrstyra datorn för att lösa ett problem som uppstått.

FAKTA

Tips – att tänka på kring IT-säkerhet

- Ha så kallad ”två-faktor login” på framförallt viktiga system, som e-post, affärssystem, filer med mera. Det innebär att det inte räcker med endast ett lösenord utan krävs en extra verifiering, exempelvis genom en app i mobilen. Många molntjänster har denna funktion gratis, bara att aktivera. I andra fall går det att komplettera befintliga system.
- Se till att mjukvaran på din smartphone och din dator är uppdaterade, ofta är det säkerhetsbrister som åtgärdas.
- Se till att ha skydd mot skadlig kod och brandvägg på samtliga enheter. Ha system som har koll på att säkerhetsmekanismer är aktiva och fungerar.
- Ha inte samma lösenord på flera olika tjänster. Blir en sajt hackad kan lösenordet användas för att ta sig in på andra ställen.
- För att skydda innehållet på datorn om den skulle bli stulen eller hackad kan man kryptera hårddisken.

TEXT
AGNES WESTBERG
agnes.westberg
@bt.se
033-700 07 42

FOTO
JAN PETTERSSON
jan.pettersson
@bt.se
033-700 07 33