

## Nya hot kräver nya strategier

*På senaste tiden har det dykt upp fler och fler nyheter om dataintrång och hackerattacker i media. Vi läser om allt ifrån intrång hos banker, där listor med nummer till bank- och kreditkort stjäls, till spionaffären i valrörelsen 2006.*

*Att svenska företag och myndigheter försöker skydda sina tillgångar genom försäkringar, lås, inbrottslarm och brandlarm är ingen hemlighet. Men hur står det till med informationssäkerheten?*

*Vi har talat informationssäkerhet med Andreas Wiman, vd för det internationella företaget Swedish Security & Training Centre AB som erbjuder helhetslösningar inom säkerhet på den internationella arenan.*

### **Hur stor är skillnaderna mellan hotbilden mot företagens informationssäkerhet nu jämfört med för fem år sedan?**

Som natt och dag. Hackers som förut varit relativt harmlösa har de senaste två åren blivit en ny typ av yrkesbrottslingar. I denna oroväckande trend ser vi bland annat att de:

- Verkar som legosoldater genom att bjuda ut sina tjänster till högstbjudande
- Idkar beskyddarverksamhet genom att först slå ut dataverksamheten på myndigheter och företag för att sedan sälja garantin att det inte ska hända igen
- Stjäl värdefull information – genom att begå dataintrång - som sedan säljs vidare på internet

I takt med att IT-brottsligheten ökar blir brottslingarna också allt mer sofistikerade. Ofta använder de privatpersoners och företags datorer som verktyg för att dölja vem som egentligen ligger bakom en attack. Dessa verktyg kallas "botnets" och är uppbyggda av tusentals kapade datorer som kan användas i överbelastningsattacker, som kombinerat med utpressning, används för att tjäna pengar på företag och organisationer.

Angreppen har också gått från att vara ganska ogenomtänkta till att bli skraddarsydda, riktade direkt mot enskilda företag. Idag kan man få en specialskriven trojan från Ryssland för runt 3000 dollar vilket även inkluderar uppdateringar och fri support!

### **Vilka ligger bakom hotet?**

Hotet kommer idag främst från kriminella grupperingar, industrier och utländska nationella underrättelseorganisationer.

Men vi ska inte glömma bort att två tredjedelar av alla IT-brott som begås sker med hjälp från insidan. Teknik i all ära, men vad händer med brandväggar, intrångsdetektionssystem och antivirusprogram när en medarbetare en dag blir varslad om uppsägning och bestämmer sig för att han eller hon inte längre har någonting att förlora på att stjäla affärskritisk information från företaget för att sedan sälja den vidare till konkurrenter?

## **Rent konkret, varför är den ökade IT-brottligheten ett problem för företag och organisationer?**

Jag väljer att svara med en fråga. Vad händer om ett konkurrerande företag kommer över ditt företags kunddatabas, delar av er finansiella information eller information om utvecklingsprojekt och konkurrensfördelar? Den totala ekonomiska skadan av dylika incidenter är svåra att uppskatta.

Många företag tror felaktigt att IT-brottlighet bara skadar dem rent ekonomiskt. Det är därför en del banker och kreditkortsbolag tycker att det är billigare att ersätta kunder som blivit bestulna direkt, istället för att investera i en säkrare infrastruktur och gå till botten med problemet.

Vad många företag inte tänker på är vad det förlorade anseendet kostar, som en sådan typ av incident för med sig. Om du inte kan lita på den bank du anförtror dina pengar till så kanske det är dags att byta bank?

Grunden till problemen är egentligen att många företag anser att informationssäkerhet är en stor kostnad som är svår att motivera. Den klassiska ”det-händer-inte-mig-principen” är vida utbredd. Att styra upp tillfredställande informationssäkerhet i en organisation är ett tidskrävande och kontinuerligt arbete som givetvis innebär en kostnad. Men jämfört med vad den totala prislappen för en IT-säkerhetsincident brukar bli är den försvinnanden liten.

## **Hur kan mitt företag bäst bemöta den rådande hotbilden?**

Det finns egentligen två vägar att gå. Antingen anställer ni personal som aktivt arbetar med informationssäkerhet eller så outsourcar ni hela eller delar av arbetet till experter. Det finns framförallt två stora fördelar med att outsourca informationssäkerheten:

- Lägre kostnader. Kostnaden är mycket större för att anställa samma kompetens som ni får tillgång till genom att anlita ett seriöst informationssäkerhetsföretag.
- Tillgång till expertis och erfarenhet. Genom att anlita experter utifrån kan du ställa höga krav på att de alltid har toppkompetens inom sitt område. Dessutom kan du dra nytta av erfarenheten som dedikerade experter har av säkerhetsarbete med andra kunder.

## **Hur väljer jag rätt partner inom informationssäkerhet?**

Genom att noggrant utvärdera dina möjligheter. Tyvärr så har delar av branschen smittats av aktörer som tänker mer på snabba pengar än på att rekrytera och leverera noggrant kontrollerade konsulter. Därför är det ytterst viktigt att du väljer en seriös partner som kan garantera konsulternas höga säkerhetsmedvetande.

På SSTC har vi rigorösa kvalitetssäkringar av anställda såväl som underleverantörer. Vår största styrka är vår personal och det slår vi vakt om. Samtliga av våra konsulter är professionella experter inom sitt arbetsområde och har lång erfarenhet av informationssäkerhetsarbete både i Sverige och internationellt. Våra medarbetares erfarenheter kommer bland annat från militär underrättelse- och säkerhetstjänst, juridiskt arbete, polisen, utrikesdepartementet och den privata säkerhetssektorn.

## **Hur arbetar SSTC med informationssäkerhet?**

Snabba lösningar är ingenting för oss. Vi vet av erfarenhet att det inte går att slänga upp en brandvägg och installera ett antivirusprogram och sedan tro att man är säker. För att vara verksamt bör informationssäkerhetsarbete ses som en långsiktig, kontinuerlig process som genomsyrar en organisations hela verksamhet – från managementnivå till medarbetare och slutprodukt.

Vi hjälper våra kunder att etablera effektiva säkerhetsorganisationer med väl integrerade ledningssystem för informationssäkerhet. På så sätt får vi till stånd en väl genomtänkt och därmed säkrare miljö där risken för att drabbas av dataintrång och attacker minimeras. Och när det händer något hjälper ett gediget proaktivt säkerhetsarbete till att minimera effekterna av allt från trojan-, virus- och överbelastningsattacker till insiderbrott och social engineering-operationer.

## **Bildtexter**

### **Bild nr 1 (bild på Anders Wiman)**

För att vara verksamt bör informationssäkerhetsarbete ses som en långsiktig, kontinuerlig process som genomsyrar en organisations hela verksamhet, säger Andreas Wiman, vd för det internationella företaget Swedish Security & Training Centre AB.

### **Bild nr 2 (tangentbord)**

Hotet mot företags informationssäkerhet kommer idag främst från kriminella grupperingar, industrier och utländska nationella underrättelseorganisationer.