

3

Vad gör IT-säkerhetschefen

Vi pratade tidigare om definitionen på säkerhet: att vara utom all fara.

Att drömma om en säkerhetsnivå där du är *utom all fara* är inte bara orealistiskt och naivt; *IT-säkerhetsarbetare som försöker hålla sig utom all fara är fega och inkompetenta och blir en belastning för sitt företag! Det är både oförsvarbart och illojalt mot din arbetsgivare och mot dig själv!* Det kan låta väl hårt, men jag är övertygad om att det är sant. Alltför många säkerhetsarbetare jobbar mest med att skydda sin egen rygg och mindre med att få ett bra säkerhetsarbete utfört.

Din roll som IT-säkerhetsarbetare är att hjälpa ditt företag att ta rätt säkerhetsbeslut. Du ska hjälpa din organisation att förstå vilka risker de tar och att använda din säkerhetsbudget på bästa sätt.

Det finns på många ställen en orealistisk förväntan på säkerhetsarbetare. Det verkar finnas de ledare som tror att det räcker med att anställa en säkerhetschef, för att alla hot ska försvinna. Åtminstone får man någon att skylla dem på!

Det är många gånger svårt att göra ett bra arbete i den här branschen, men man måste inse vilka utmaningarna är så man kan tackla dem i rätt prioritering.

Så vad är då din största utmaning? Vad ska du fokusera största delen av din tid på? Säkerhet är ett mycket brett område och det är nästan omöjligt att vara duktig över hela bredden!

Är det nödvändigt att lära sig allt om teknisk säkerhet och kunna utvärdera alla produkter utan och innan? Är den administrativa säkerheten viktigast så att du måste fokusera på att kunna alla regelverk och processer utan och innan? Kanske ska du ta alla certifieringar som finns och få ett visitkort med "CISSP, CISM, CISA, COMTIA" efter ditt namn? Du kanske bör bli en mästare på matematik och statistisk analys så du kan slå alla på fingrarna med dina rapporter?

Allt det där är bra att kunna, men det finns en sak som får dig att verkligen sticka ut som ett proffs i den här branschen: "Lär känna din verksamhet och vilka hot som finns mot den! Berätta sedan det för din ledning på ett sätt som de förstår!"

Om du saknar det här så spelar resten av dina kunskaper ingen roll! Säkerhet är inte en övning i att skaffa längst nyckellängder eller den fetaste dörren till drifthallen! Det handlar inte ens om att hindra dina medarbetare från att göra sitt jobb med överdrivet långa lösenord (det är bara en bonus ☺)! Du måste lära dig vad du ska skydda och hur mycket det är värt, och sedan måste du kunna övertyga ledningen om varför du ska få pengar till det jobbet! Du ska inte falla för frestelsen att ta i för mycket bara för att du kan stå utan skuld om något händer. Istället bör du använda alldeles lagom med pengar för varje enskilt hot, så att du alltid kan försvara varför det var nödvändigt. Om du kan arbeta på det här sättet så kommer du att få ett väldigt roligt arbete och njuta av det förtroende du får.

Lägg därför mycket mer tid än du tror på att lära dig förstå din verksamhet och prata med kollegor. Du kommer att bli en klippa på att hålla presentationer som kan få en skräckfilmsproducent att vifta med checkhäftet! Skräm upp och lugna ner (men på ett seriöst sätt ☺)!

Ansvar

En sak som är viktig att komma ihåg är att en säkerhetschef inte är säkerhetsansvarig! Många sätter likhetstecken mellan de orden och det kan bli väldigt olyckligt (särskilt för den säkerhetsansvariga). Det är aldrig en persons roll att vara ansvarig för säkerheten! Alla dina kollegor är ansvariga för att utföra sitt arbete på ett säkert sätt, och det är ditt jobb att få dem att förstå det! Utvecklarna skriver säker kod, kas-sörskan kontrollerar ID-kort enligt alla regler, it-avdelningen klappar på burkar, vaktmästaren låser och larmar och ekonomipersonalen har ordning och reda på pengarna. Tillsammans kan ni skapa en miljö där ni har koll på riskerna och klarar av även smärre katastrofer när de inträffar (och det gör de, eller hur?).

IT-säkerhetschefens arbetsuppgifter

Här tittar vi helt kort på några av de arbetsuppgifter som en säkerhetschef bör ägna sig åt.

Kommunikation

Vi har sagt det ett par gånger men det är värt att upprepa! En viktig del av ditt arbete är att prata med dina arbetskamrater. Om det inte faller sig naturligt för dig att göra det, eller om du har svårt att hitta tiden, så behöver du boka tid i kalendern för kommunikation:

- Prata med dina arbetskamrater i olika delar av organisationen. Bli den på ditt företag som bäst förstår de olika delarna av verksamheten.
- Håll en nära kontakt med företagsledningen. Hitta en speciell kontaktperson (sponsor) i ledningen för säkerhetsarbetet och håll honom/henne underrättad kontinuerligt om ditt arbete. Se till att du förstår ledningens och ägarnas prioriteringar. Det ger dig en mycket bättre möjlighet att utforma säkerhetsarbetet så det tas väl emot i organisationen.
- Prata med styrelsen. Det är inte fel om du känner styrelsen på företaget och om de känner igen dig. Om/när något illa händer så faller det på dig att rapportera läget. Prata med ledningen om ditt engagemang i styrelsen. Beroende på vad ni har för verksamhet kan behovet se olika ut, men det bör inte vara omöjligt för dig att göra 1-2 gästpass per år utan att det känns krystat.
- Lär känna branschkollegor. På många plan är det tabu att prata med sina konkurrenter på marknaden. Inom vårt område kan du med lite tur få en förståelse för att vi har mer att vinna på att hjälpa varandra än att låta var och en stå ensam. Det finns naturligtvis undantag där säkerhetsutbyte är ytterst olämpligt; till exempel om du arbetar med att utveckla säkerhetsprodukter så tycker jag inte att du ska låta andra ta del av dina kunskaper. I många andra situationer kan man hitta former för säkerhetssamverkan där man undviker känsliga områden.

Kontinuitetsplan

Kontinuitetsplanering (Business Continuity Planning – BCP) handlar om att förbereda sig för en katastrof innan den inträffar. Målet är att

minimera skadan och säkerställa att företaget kan fortsätta att bedriva verksamhet.

Kontinuitetsplanen tar upp de lite större och (förhoppningsvis) mer sällsynta olyckor som kan drabba ett företag. En liten lista med osorterade exempel på såna katastrofer följer här. Har jag missat några? Skriv till dina egna på slutet:

- Era lokaler brinner ner till grunden.
- Er webserver slutar fungera och ingen vet varför.
- Ett mjukvarufel gör att stora delar av er viktigaste databas plötsligt innehåller felaktigt data.
- Strejk eller blockad.
- Översvämning dränker datahallen och lagret.
- Jordskred blockerar infarten till er produktionsanläggning så att ni varken kan få råvaror levererade eller skeppa iväg färdiga produkter.
- Vandaler.
- Stöld.
- Sabotage.
- Rån, Mord, Mordbrand.
- Flygplanet med hela ledningen på väg till konferens exploderar.
- En arg kund hackar ert datasystem eller smittar ner VD, marknadschefens och ekonomichefens datorer med en trojan som stjälar all information de har tillgång till (eller värre, långsamt förändrar all information).
- Långvariga elavbrott.
- Långvariga kommunikationsavbrott.
- Den enda personen som förstår ekonomisystemet blir överkörd av en buss och dör.
- Den lyx-dessertost som ni tillverkar visar sig döda kunderna.
- Er nya produkt kastas i soptunnan av Sverker på bästa tvsändningstid.

Tidigare pratade vi lite om hur man gör en sårbarhetsanalys. Kontinuitetsplanen och sårbarhetsanalys ligger nära varandra och kan hanteras med samma process.

TIPS 1:

När en katastrof inträffar så blir man mycket stressad! Det första som ryker under stark stress är förmågan att tänka klart. Ha därför enkla och tydliga checklistor som du kan följa och pricka av dina framsteg på

TIPS 2:

Om lokalerna har brunnit ner så kan du inte logga in på servern och läsa checklistan längre! Skriv ut hela kontinuitetsplanen, lägg den i en stadig och RÖD pärm. Skriv ”KRIS” med stora bokstäver på framsidan och se till att alla nyckelpersoner har ett uppdaterat exemplar hemma hos sig. Fråga ibland om de vet var den är!

TIPS 3:

Om datorer och kommunikationssystem är utslagna så är det svårt att få tag på folk! Fyll på längst bak i planen med kontaktlistor till viktiga personer där du anger så många kommunikationssätt som möjligt. Förslag på personer att ta med i en sådan lista:

- alla chefer
- viktiga tekniker
- viktiga kunder
- styrelsen
- viktiga underleverantörer
- hyresvärderna
- vaktbolaget (skriv även upp larmkoder och kundnummer)
- försäkringsbolag
- privatsjukvård (om ni har sådana avtal)
- jourhavande präst
- systembolaget (nej just det, det var på min privata lista 😊)

TIPS 4:

Skriv ut en mall för en händelselogg där du kort noterar vad du gör och när du gjorde det. När allt har blåst förbi ska du kunna redogöra för vad som har hänt och jag lovar att du inte kommer att minnas särskilt klart vad som har hänt om det har stormat friskt!

Sårbarhetsanalys

Det här ämnet har vi redan ägnat mycket text åt så det behövs ingen mer kommentar här. Kom bara ihåg att göra det!

Handlingsplanen

Kom du ihåg att det viktiga med sårbarhetsanalysen var handlingsplanen? Glöm inte bort att ta fram en sådan (och genomför den!) (och följ upp hur det gick!)

Utbildning

Utbilda din personal i säkerhet. Mycket i ett företags fokus ligger på snabb leverans av sexiga produkter! Säkerhet kommer inte alltid upp högst på dagordningen. Du som jobbar med säkerhet behöver förklara för dina kollegor varför de också måste tänka på säkerhet. Du behöver också ge dem verktyg för att kunna bli bättre på säkerhetsfrågorna.

Utvecklingsprojekt

Du kan ha säkrat upp er verksamhet enligt konstens alla regler och till en nivå som ni alla är överens om. Nu är arbetet inte klart här eftersom verksamheten, produkter och personal förändras över tiden. Du behöver vara med (tidigt) i utvecklingsprojekt och bidra med ett säkerhetsfokus. Det går inte att klistra på säkerhet som ett plåster på slutet så du behöver in tidigt för att ha en chans.

Personlig utveckling

Vidareutveckla dig själv på säkerhetsområdet för att fortsätta vara duktig och tycka om det du gör! Gå på några relevanta mässor, träffa kollegor, ta en certifiering, läs en bok (en bok till när du är klar med den här ☺), gå en kurs. Det finns många sätt och (nästan) alla är bra. Glöm inte bort det i all stress bara.

Vem vet, du kanske lär dig något som gör din vardag enklare? Vi tipsar om utbildningar och annan bra information för fortbildning i kapitel 13.

Vanliga fel

Vad är de vanligaste felen när man arbetar med säkerhet? Det finns många fel att välja på. Angriparna (skurkar, missnöjda anställda eller otur) har det bra mycket lättare än vi som ska förhindra olyckor. Det är mycket svårare att bygga en stark och tät vägg än att hitta en liten svaghet och utnyttja den. Jag tänker inte försöka lista alla olika typer av fel man ska undvika, så jag fokuserar på tre stora.

Dessutom tänkte jag stjäla det här helt och hållet från en artikel jag hittade på www.idg.se! Jag tyckte den var genial! Tyvärr hittade jag inte artikeln så jag kan ge författaren den cred han förtjänar. Dessutom minns jag inte helt vad han skrev så förutom att förbli onämnd så blir vår stackars författare felciterad! (förlåt förlåt!) Ja, så kan det vara ibland, men nu kör vi!

PS, ett framgångsrikt säkerhetsarbete består till 99 procent av stöld. Om du börjar uppfinna egna saker så gör du det onödigt jobbigt för dig (eller så är du bra mycket duktigare än alla andra, och då får jag gratulera dig!). DS

Tre vanliga fel

1. Ingen känner till säkerhetsreglerna

Du kan ha jobbat i år på att ta fram en perfekt samling regler och skydd som skulle garantera att ni aldrig råkar ut för något ont! Du glömde bara att berätta om det för någon så ingen följer dina rutiner eller använder dina skydd som det är tänkt. Ett annat misstag är att du

berättade om detta en gång i början på ett bolagsmöte för ett år sedan och tror att folk kommer ihåg vad du sa. Sådant här behöver nötas in och paketeras väl för att kunna få en effekt. Upprepning och uppföljning.

2. Ingen följer säkerhetsreglerna

Du kanske var duktig och berättade för folk om ditt vackra säkerhetsarbete men ingen gör som du säger! Så fräckt. Efter allt arbete du lagt ner! För inte är det väl ditt fel att ingen gör som du sa...

Glömde du kanske att förklara varför? Eller skrämde du dem inte med vad som kan hända om de brister? Saknar du stöd från ledning och chefer? Var budskapet inte anpassat till åhörarna eller fick de inte information om HUR de skulle följa reglerna? Det kan finnas många skäl till att ingen följer reglerna.

3. Det är omöjligt att följa säkerhetsreglerna

Säg att du fick de två första rätt så kanske du snubblar här. Du berättar för folk om vad de behöver göra och lyckas förklara varför så att de verkligen försöker. Dina kära kollegor ger däremot snart upp för att det inte går att följa dina instruktioner i praktiken! Det kanske gör deras arbete outhärdligt, eller så fungerar verktygen helt enkelt inte ihop.

När man läser en sådan här lista är det lätt att sucka och tänka, det här händer aldrig mig, eller, man får allt vara bra dum om man gör bort sig så här. Tänk igen, för det är vanligare än du tror.

Skräckexempel:

Säkerhetschefen som är känd bara för att hindra och stoppa projekt, men när något går fel, snabbt blir syndabock och aldrig gör det han ska.

Säkerhetsavdelningen som ett sista steg i projekten vilka man tillfrågar: Är det här säkert! Man svarar alltid nej (för det är aldrig säkert), och det leder till att man antingen stoppar projekt eller blir överkörd utan att några förbättringar införs.