

SUNETS HANDBOK I INFORMATIONSSÄKERHET OCH IT-SÄKERHET

Nu fungerar SunetC som det är tänkt och alla är glada. Anslutningarna till lärosätena går som en dans. NORDUnets anslutningar till omvärlden flyter på. Inga bekymmer. Hakuna matata. Fast alla är inte så glada. Nätet är inte längre problemet för de anslutna.

SUSEC (Swedish University information SECURITY group) finns dels för att det måste till en förbättring av säkerheten i system, applikationer och nät och dels för spridning av kunskap om informationssäkerhet. Sveriges myndigheter har klara problem med IT-säkerheten. Nu blev det tråkigt, eller hur?


Antingen du vill inse det eller ej så pågår ett krig i din internetsladd. Det hörs inte och det kommer ingen rök, men kriget pågår lika fullt. Cyberattacker är legio. Svenska företag och myndigheter utsätts för dem varje dag. IT-säkerheten är idag inte en enskild persons problem, den är ett hot mot företag, institutioner, myndigheter, större händelser (som allmänna val) och samhällets kritiska funktioner. Dina uppkopplade enheter, hur oskyldiga de än må betraktas av dig, kan vara en del av "mörka maktens" ambitioner med allt från att dölja pedofilbilder och få din dator att agera server för dessa individer till att vara en del av främmande maktens syften att koordinerat släcka samhällskritiska verksamheter.

INFORMATIONSSÖVERBELASTNINGSTRÖTTTHETSSYNDROM

Vi lever i informationsöverflödets epok. Problemet är att skilja agnarna från vetet – vad är viktigt eller t.o.m. kritiskt att veta. Det är upp till arbetsgivaren att ansvara för att säkerheten upprätthålls på arbetsplatsen, men det fungerar inte alltid. Säkerhetshandboken är åtminstone ett försök att röja upp i träsket.

Arbetet med säkerhetshandboken påbörjades redan år 2001 och har sedan skett i etapper, först genom Sveriges universitets- och högskoleförbund (SUHF) och sedan 2005 genom SUNET. SUSEC svarar för bokens uppdateringar i samråd med en mängd olika lärosäten. Arbetet verkar ha avstannat kring 2011-2012 och boken är ännu inte helt klar.

Det som står i den är dock så visionärt och framstående att det knappast finns något liknande. Boken är beklagligtvis bara ett förslag. Det finns tyvärr inget tvång att använda den vid något lärosäte.

itsakhandbok.irt.kth.se 130% 

Välkommen till Handbok i Informations- och IT-säkerhet

Denna handbok är skriven för ett tänkt medelstort lärosäte.

Tanken är att den ska underlätta för dig som arbetar med informationssäkerhet att utforma lokala regler och råd. När det gäller frågor rörande legala rättstillämpningar hänvisas till respektive lärosätes jurist.

Handboken tar upp den administrativa/logiska säkerheten såsom policies, riktlinjer, regler och råd. Den tar även upp tekniska förutsättningar för en säker infrastruktur såsom nätsäkerhet, elakartad kod, forensics, lagring av trafikdata samt elektroniska ID-tjänster. Här finns också förslag till undervisningsmaterial som bygger på handboken.

Vi har brutit ut det som är alltför tekniskt till ett fördjupningsavsnitt samt kompletterat med nytt material bl a med råd kring bärbara datorer, kryptering, forensics samt nätsäkerhet. Du hittar dit genom att klicka på "läs mer" vid aktuellt avsnitt. Vi har också lagt en del länkar till SS ISO/IEC 27000-serien, Ledningssystem för informationssäkerhet.

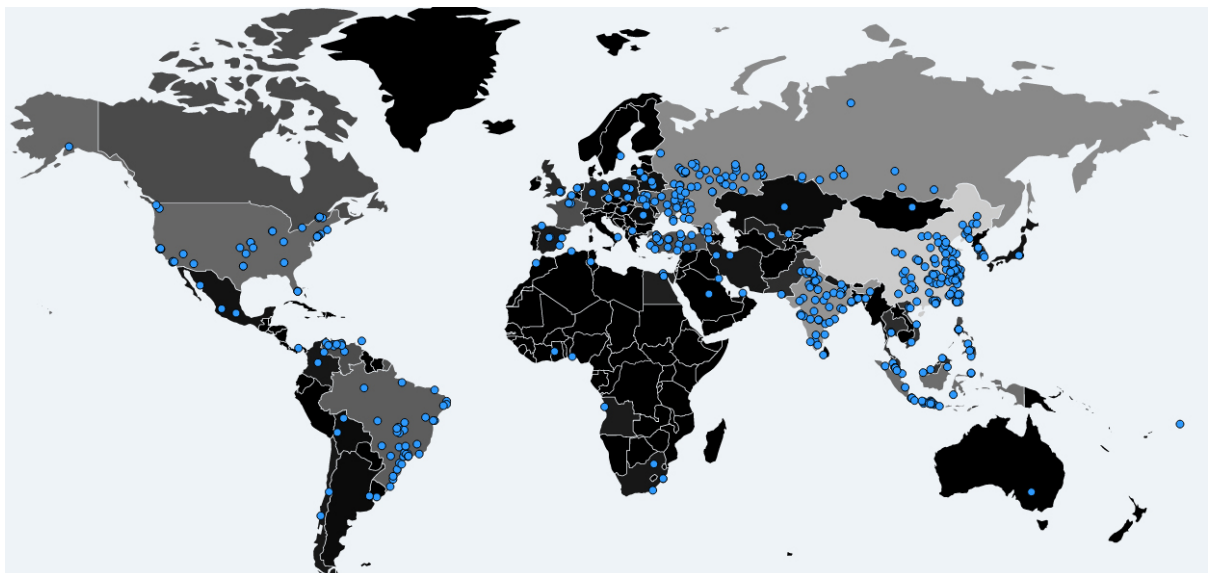
Den innehåller också en lista på referenslitteratur inom informationssäkerhetsområdet, en sammanställning av aktuella lagar, en ordlista samt ett stort antal användbara länkar. Aktuella standarder har följts så långt möjligt.

Handboken har producerats genom samarbete mellan flera universitet och högskolor och Swedish University information SECURITY group (SUSEC) med ekonomiskt stöd från SUHF (Sveriges Universitets- och Högskoleförbund) och SUNET. Materialet kommer även fortsättningsvis att uppdateras/kompletteras genom fortsatt samarbete där projektledning och styrgrupp kvarstår och med fortsatt ekonomiskt stöd från SUNET.

Läs mer under "Om handboken". Där finns bl a en kortfattad sammanfattning av innehållet i de olika avsnitten.

Handbok i Informations- och IT-säkerhet | [Utskriftsvänlig sida](#) | [Kontakt](#)

Den är inte vacker. Den är inte konstnärligt utformad. Den är inte ens färdig (2017). **Den är bara astronomiskt bra!** Det står något tänkvärdt i varje kapitel. Det går utmärkt för en icke-myndighetspublik att bara byta ut orden "lärosäte" eller "myndighet" mot "företag" och "rektor" mot "företagsledning" så fungerar denna handbok för hela det svenska näringslivet. Om nu bara någon vore intresserad...



Karta: malwaretech.com

Om man ska döma av spridningskartan för trojanen Wannacrypt i mitten av 2017 är det väldigt få som är intresserade.

Handboken bör läsas av alla, för att säkerhetsproblemen påverkar den enskilde, såväl som institutionen och samhället. Den som vägrar läsa och förstå, utsätter sig, institutionen och samhället för fara. Det kan låta högtravande, men med tanke på vad som nyligen hänt med myndigheter, sjukhus, dagstidningar, ja hela länders kraftförsörjning, är det kanske inte så högtravande ändå?

För dig som inte klarar av långa texter, har jag här sammanfattat det viktigaste i handboken.

ALLMÄNNA REGLER OCH ANSVAR



Man kan börja med det allra viktigaste, som det slarvas allra mest med på alla arbetsplatser, statliga såväl som privata. Något av det farligaste som många datoranvändare har lärt sig är att "klicka bort" obegripliga eller otrevliga dialogrutor. Vad var det som hände? Vet inte? Men vad stod det? Jag klickade bort det!

Låt oss börja med avsnitt 6.2 Säker arbetsplats. Sidan börjar med det viktigaste av alla råd, som om alla följde det, skulle ha förhindrat de allra flesta attacker av trojaner och malware:

Lämna aldrig ut ditt lösenord eller dina kontouppgifter till andra. Banker frågar aldrig. Systemavdelningar frågar aldrig. Det är alltid en bluff när någon frågar.

Se till att dina data är säkerhetskopierade. Hårddisken på din bärbara dator är ingen säkerhetskopia.

Klicka inte på allt skräp som dyker upp. Klicka inte på länkar och bilder som du inte vet var de kommer ifrån. Klicka inte OK utan att läsa vad du OK:ar till. Du kan råka installera virus eller annat otyg på din dator.

Spara inte kontonummer på din dator.

Varför följer inte alla dessa enkla regler? Förmodligen för att man inte har hört talas om dem. Förmodligen för att utbildning i och intresse av IT-säkerhet i princip är obefintlig hos de flesta myndigheter och privatföretag.

Ditt konto är ditt ansvar!

men

Arbetsgivaren är ansvarig för IT-säkerheten och ska se till att den upprätthålls.

OM ANSKAFFNING OCH UTGALLRING AV UTRUSTNING

I kapitel 3 som handlar om att utforma riktlinjer sägs det smarta saker om anskaffning av utrustning, som:

Produkten ska gå att köra på ett operativsystem som förväntas ha fortsatt support beträffande säkerhetsuppggraderingar under hela produktens livscykel.

Det kan tolkas som "Du skall icke köra gammal Windows". Och vad hittar vi under 3.5 Gallring och rensning?

Datorer som avskrivits och skall skrotas eller ges bort skall alltid rensas om de kan innehålla någon känslig information.

Detsamma gäller givetvis mobiltelefoner.

RISKHANTERING



Början av avsnitt 3.10 som handlar om riskhantering och riskanalys är så bra att jag återger den hel och hållen:

Varje myndighet skall identifiera vilka risker för skador eller förluster som finns i myndighetens verksamhet. Myndigheten skall värdera riskerna och beräkna vilka kostnader som staten har eller kan få med hänsyn till dessa risker. Resultatet skall sammanställas i en riskanalys. Varje myndighet skall vidta lämpliga åtgärder för att begränsa risker och förebygga skador eller förluster.

Det är det där sista som är nyckeln och bör stämma till eftertanke: "...skall vidta lämpliga åtgärder för att begränsa risker och förebygga skador". Det är formulerat som ett skall-krav och innebär bland annat att ledningen ska läsa igenom hela boken och genomföra det som står där. Innan något ens hänt. Om alla bara vidtog lämpliga åtgärder för att begränsa riskerna, skulle Sverige vara ett högsäkerhetsland som ingen hacker ens skulle fundera på att angripa. Men så är det inte. Istället är svenska datorinstallationer som ett såll och massor av attacker slinker igenom varenda dag. Det finns snart inte en myndighet, sjukhus eller skola som inte råkat ut för en trojan.

SÄKERHETSKOPIERING



Och så det eviga tjetet om säkerhetskopiering, som ständigt tycks falla på hälleberget, eller fara in i och därefter ut ur döva öron. Läs avsnitt 6.2:

Det säger sig självt att man ska ta regelbundna säkerhetskopior. Det kan vara speciellt viktigt att komma ihåg detta för bärbara datorer direkt innan man far iväg på en resa. Men, på resan kanske du inte är betjänt av den centrala säkerhetskopian ifall du får problem med din bärbara. Det kan vara till fördel att ha med exempelvis din presentation och eventuella andra viktiga filer på ett USB-minne som reserv. Har du känsliga data – se till att ha krypterad kopia, både på server och under överföring.

BROTT OCH STRAFF



Handboken lämnar inte ansvaret opåtalat. Faktum är att någon måste ha ansvar för att reglerna följs och när denne struntar i sitt ansvar måste det bli en påföljd. Det ska alla veta om. Vid hur många myndigheter, sjukhus, företag, hamnkontor, polisstationer, domstolar och banker tillämpas dessa regler? Och med "tillämpas" menar jag inte att reglerna finns någonstans på intranätet där de enkelt kan ignoreras, utan att straff faktiskt mäts ut.

Påföljder vid överträdelse av användarregler Vid överträdelse av dessa användarregler kan användaren riskera att blir helt eller delvis avstängd från lärosätets IT-resurser. Användaren kan dock bli anvisad dator (som inte är ansluten till annat än eluttag) så att användaren kan fullgöra sina studier eller arbetsuppgifter under tid för eventuell utredning. Misskött eller missbrukat IT-resurs kan med omedelbar verkan stängas av.

Disciplinära påföljder för medarbetare Medarbetare kan vid överträdelse av användarreglerna riskera att anmälas till rektor och personalansvarsnämnd. De disciplinära påföljderna är disciplinansvar eller avstängning.

Med tanke på alla som drabbats av trojaner och utpressningsprogram på det senaste kan man sluta sig till att ingen, eller åtminstone väldigt få hört talas om det ovan, eller riskerar att drabbas av påföljderna. Man kan förledas att tro att om reglerna tillämpades strikt, skulle många sjukhus, kontor osv bli helt utan personal.

Det måste svida att bara strunta i allt och klicka på fantastiska erbjudande om pengar från fjärran land, snygga tjejer, eller "utstående paket" från Post Nord.

Ta bara den helt rimliga regeln "Misskött eller missbrukat IT-resurs kan med omedelbar verkan stängas av" som exempelvis kan tolkas som att "kan du inte sköta din telefon utan infekterar den med allehanda trojaner, så blir du av med den." Detsamma gäller folk som hämtar hem trojaner och skadar företagets verksamhet och ekonomi. Där gäller regeln "Påföljderna är disciplinansvar eller avstängning". Den som inte bryr sig om reglerna måste ta sitt straff, oavsett befattning. Handboken frikänner ingen i högre ställning från ansvar. Det står bara "medarbetare".

ETT SNACK MED EN FÖRFATTARE

Patrik Lidehäll på KTH har varit med om att skriva nästan varje kapitel i handboken. Han får berätta om tillkomsten och det fortsatta arbetet.



– Utbildnings- och myndighetsvärlden består av en hel mängd aktörer, allt från de väldigt stora till de väldigt små. KTH är exempelvis väldigt stort, medan Statens Musiksamlingar hamnar bland de väldigt små. Alla dessa har haft samma problem och har försökt lösa dem hemma på kammaren så gott man kunnat, men det har brutit i samarbetet dem emellan. Ekonomin sätter också stopp för mera avancerade riskanalyser vid de riktigt små lärosätena.

SUSEC skickade ut en enkät till att högskolorna och kom fram till att det behövdes en säkerhetshandbok. Därför samlade man ihop ett antal tekniker och språkmänniskor och arbetet påbörjades, men efter ett antal år hade arbetsgruppen utarmats på grund av att medlemmarna fått nya arbeten, gått i pension osv. I slutänden blev bara jag och Anne-Marie Achrenius på Chalmers kvar.

Samtidigt har universitetsvärlden förlorat duktiga krafter till exempelvis konsultvärlden. Konsulter såg helst att de fick betalt för sin möda och skulle aldrig lägga ut en skrift som säkerhetshandboken gratis på Internet. Det är därför SUNETs Handbok i Informations- och IT-säkerhet är så värdefull!

Har den varit framgångsrik?

– Nog är IT-handboken känd. Den har tagits upp och stötts och blötts vid varenda Sunetdag de senaste tio åren. Jag har blivit kontaktad av många, framför allt kommuner och landsting, som sitter i samma båt som lärosätena. Återkoppling har också kommit från Sambruk, den kommunala samverkansgruppen för verksamhetsutveckling av e-tjänster, såväl som ett antal kommersiella företag. Så nog har den varit framgångsrik. IT-folket på KTH och SUNET har dessutom försökt hjälpa de mindre lärosätena, efter förmåga. Inför varje Sunetdag har man besökt den skola som arrangerat tillställningen och hjälpt dem rusta upp sitt trådlösa nät och i samband med detta har man hållit en säkerhetsteknisk genomgång.

Men boken måste väl göras färdig och anpassas till utvecklingen?

– Givetvis ska den fortsätta utvecklas. Arbetet pågår med att göra den färdig och det finns mera text som inte ännu är publicerad. IT-utvecklingen står inte still heller. Verkligheten har dessutom infört ett antal nyheter på IT-fronten på det senaste, som EU:s nya dataskyddsförordning GDPR (General Data Protection Regulation), som måste beskrivas. Det finns andra EU-direktiv som också måste hanteras.

En idé är att skärskåda ISO/IEC 27000, en samling säkerhetsstandarder och rekommendera viktiga bitar och sätta dem i rätt sammanhang för utbildningsvärlden.

Den kommande utgåvan ska också innehålla praktisk vägledning, sk How-to-texter, till exempel om hur man konfigurerar brandväggen i Windows och liknande. Dessa tips kommer att sättas samman av IT-experter, incidenthanterare och de som jobbar på SUNET CERT, folk som är praktiskt ansvariga för flera tusen datorer, och kunna motverka de "alternativa kunskaperna" som flödar på sociala medier.

SUNETS SÄKERHETSTJÄNSTER

Svenska lärosäten har tillgång till ytterligare säkerhetstjänster från SUNET, såsom en världsomfattande säker inloggningsprocedur (eduroam, skolvärldens single-sign-on), kostnadsfria certifikat (TCS) och rådgivning från en central incidentbyrå (CERT), med mera. Det här är sådant som kommersiella företag får köpa, som få faktiskt gör, vilket får undertecknad att tro att utbildningsvärlden ligger långt före de svenska företagen i gemen.

AVSLUTNING

SUNETs Handbok i Informations- och IT-säkerhet innehåller en oerhörd massa intelligent information och bör läsas av var och en som bryr sig det minsta om sin mobiltelefon, dator, nätverk eller datorhall.

1. Implementerar man säkerhetshandboken
2. Läser den här artikeln
3. Applicerar logik

så klarar man sig från Wannacry, Petya, trojaner, ransomware, ID-kapningar och andra phishing-försök. Inga problem!

LÄS MER

Handboken finns som en länk från SUSECs webbsida: <https://susec.se/>

Eller för sig själv: <http://itsakhandbok.irt.kth.se/>

ISO/IEC 27000-serien: https://sv.wikipedia.org/wiki/ISO/IEC_27000

Om social ingenjörskonst och hur den används för att lura av oss information och pengar, examensarbetet "Social ingenjörskonst, en studie i modern IT-brottslighet" av Elin Hjorth vid Högskolan i Halmstad: <http://www.diva-portal.se/smash/get/diva2:541172/FULLTEXT01.pdf>

Om trojaner och e-post på KTH: <https://www.sunet.se/blogg/den-okanda-hasten-fran-troja/>

Attackvektorn, det är du: <http://www.sweclockers.com/artikel/21218-attackvektorn-det-ar-du>

Alla attackers attack drabbade Estland år 2007, men de klarade av det, tack vare gott säkerhetssamarbete och fiendens misstag: <https://techworld.idg.se/2.2524/1.440124/estland-under-attack>

Skriven av



JÖRGEN STÄDJE

Jag heter Jörgen Städje och har skrivit om teknik
och vetenskap sedan 1984. Friskt kopplat, hälften
brunnet!