HÖGSKOLAN I SKÖVDE

INFORMATIONSSÄKERHET
EN ANGELÄGENHET FÖR HELA SAMHÄLLET

Rose-Mharie Åhlfeldt
Bitr professor, Högskolan Skövde

VEM ÄR JAG?

- Bitr professor i informationsteknologi
- Informationssäkerhetsprogrammet 2020 – LIS i kommuner Västra Götaland
- Dataskydd och informationssäkerhet i organisationer
- DOME – Patientens journal via nätet

SAMHÄLLSBEHOV

- För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi (N2017/03643/D)
  - Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter
- ”Informationssäkerhet är en förutsättning för att nya digitala företeelser i samhället ska kunna fungera” (MSB, 2018).

HÖGSKOLAN I SKÖVDE

Markant ökning av digitala incidenter under mars månad

Digitala incidenter som hotar informationssäkerhet- och trygghet har ökat avsevärt i svenska och nordiska nätverk, det visar KPMG:s omvärldsbevakning och hotbildsanalys tydligt.
– Enligt vår bedömning beror ökningen till stor del på att många gått över till distansarbete, säger Per-Olov Humla, chef för KPMG Cyber Security.

KPMG:s cyberteam har studerat informationssäkerhetsincidenter hos organisationer och under de tre första veckorna i mars ser man en markant ökning av attacker.

– Angripare etablerar sig inuti nätverk och distribuerar skadlig programvara eller använder IT-resurserna för att attackera någon annan. Vi ser sådant som redan inträffat, trots organisationens säkerhetskontroller och som användare i stor utsträckning är omedvetna om.

https://home.kpmg/se/sv/home/nyheter-rapporter/2020/04/cyberattacker-okar-i-sparen-av-covid-19.html

Expert: Pandemin ligger bakom ökning av cyberattacker

2020-08-03 06:00 Av: John Edgren 0 kommentarer

Aktivera Talande Webb

Antalet cyberattacker ökar markant. Oliver Popov, professor vid Stockholms universitet, anser att ökningen beror på att pandemin har skapat en samhällsstörning.

https://www.nyteknik.se/premium/expert-pandemin-ligger-bakom-okning-av-cyberattacker-6998954

Hemmajobb ökar cyberattackerna: ”Vi har varit för naiva”

2020-06-22 09:05 Av: Henning Eklund/TT 5 kommentarer

Hemmajobb leder till ökade risker för cyberhot. Foto: TT

Aktivera Talande Webb

Hemmajobb under pandemin ökar riskerna för cyberattacker mot svenska företag. Sedan förra året har det skett en stor ökning – och Sverige håller på att halka efter omvärlden. ”Vi har varit för naiva”, säger cybersäkerhetsexperten Jakob Bundgaard.

Förra året uppgav hälften av alla medelstora och stora svenska företag att de varit utsatta för cyberattacker. I år är siffran 63 procent, enligt en undersökning som revisions- och affärsrådgivningsföretaget PWC Sverige genomfört bland 100 företag.

Jakob Bundgaard, ansvarig för cybersäkerhet på PWC Sverige, tror att ökningen både har att göra med en faktisk ökning och en ökad öppenhet.

https://www.nyteknik.se/sakerhet/hemmajobb-okar-cyberattackerna-vi-har-varit-for-naiva-6997539

HÖGSKOLAN I SKÖVDE

SÄKERHET 2019-11-15 06:02

Betalar hellre utpressare än investerar i it-säkerhet – ”en pedagogisk utmaning”

It-attacker oroar svenska företag mer än en lågkonjunktur. Samtidigt verkar det finnas en gräns där man hellre betalar lösen för ransomware än fortsätter minska risken genom investeringar i it-miljön.

SÄKERHET 2020-11-04 07:01

MSB varnar för växande hot mot vården – ransomware ökar kraftigt

PRO LÄS FRITT TILL 09:01

Den senaste tidens våg av varningar och verkliga attacker mot sjukvården runt om i världen får nu MSB att varna för att något liknande kan hända i Sverige.

HÖGSKOLAN I SKÖVDE

SAMHÄLLSBEHOV

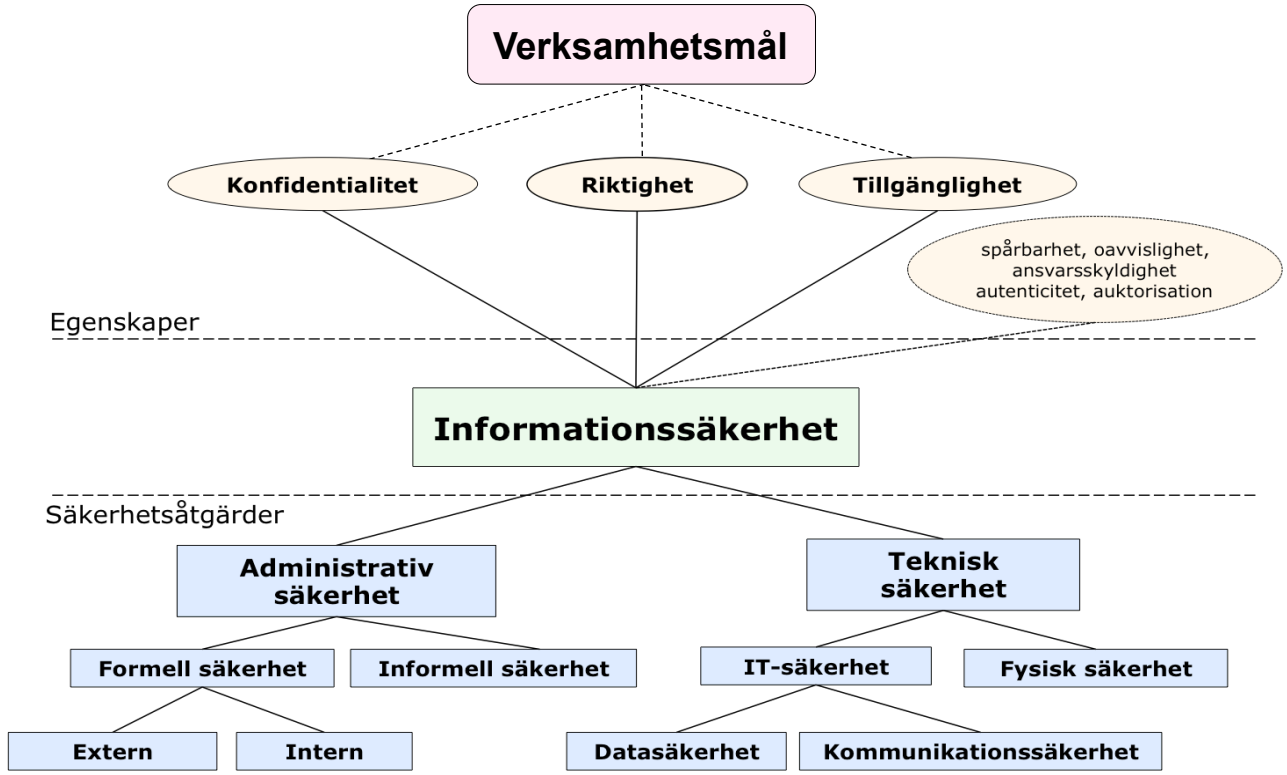
- Utredningar som visar på stora brister och behov av informationssäkerhet i den statliga förvaltningen och med koppling till samhällets alla tjänster.
  - Informationssäkerhetsutredningen (SOU 2015:23)
  - Riksrevisionens rapport (RIR 2016:8)
- Befintliga och nya lagar/förordningar som ställer krav på säker informationshantering och hantering av privacy
  - MSBs föreskrift för statliga myndigheter (MSBFS 2016:1)
  - Dataskyddsförordningen (GDPR)
  - NIS-direktivet – säkerhet i nätverk och informationssystem i samhällsviktiga tjänster

LÄGESBESKRIVNING?

HÖGSKOLAN I SKÖVDE

INFORMATIONSSÄKERHETSMODELLEN

HÖGSKOLAN I SKÖVDE



RÅD TILL ORGANISATIONEN

(MSB, 2020)

Vilka regler gäller för distansarbete och användningen av it-system utanför organisationen? Är reglerna aktuella och relevanta eller behöver de snabbt förbättras? Kommunicera och påminn alla medarbetare om reglerna. Se till att de är lätta att hitta och publicera dem gärna på intranätet.

Vilken kapacitet har organisationen avseende hur många som kan arbeta på distans? Om ni har begränsningar i antal möjliga distansuppkopplingar behöver viktig verksamhet prioriteras och annat arbete göras lokalt på datorn, utan uppkoppling. Det kräver struktur och samordning. Se över möjligheterna att några medarbetare kan koppla upp sig på olika tider för att exempelvis hämta dokument från server till dator. På så sätt kan fler arbeta lokalt till dess att ni fått fler uppkopplingar eller mer utrymme.

Finns säkra inloggningar för distansarbete? Säkerställ att it-funktionen har de resurser som krävs för att upprätthålla säkra inloggningar för distansarbete, installera säkerhetsuppdateringar snabbt och hantera incidenter med mera. Läs mer på https://cert.se/2020/03/sakerhet-och-infrastruktur-vid-arbete-hemifran om vilka åtgärder som kan behöva göras.

Incidenter behöver hanteras skyndsamt. Säkerställ att incidenter fångas upp och följs upp så snart som möjligt så att ni snabbt kan åtgärda sårbarheter som har uppstått på grund av ändrade förutsättningar.

RÅD TILL ORGANISATIONEN
(MSB, 2020)

Finns säkra arbetssätt för behörighets-tilldelning vid distansarbete? Säkerställ att den interna supporten arbetar enligt reglerna för behörighetstilldelning för uppkoppling vid distansarbete. Var medveten om att det kan förekomma falska samtal om lösenordsåter-ställning och även falska inloggningslänkar. Eventuell avvikelse från reglerna kan ske först efter medvetna riskbeslut.

Har ni antagit kontinuitetsplaner? Säkerställ att dessa följs. Om det saknas planer kan du stötta genom att få igång ett samtal om vilka delar i verksamheten som är kritiska för organisationen. Mer information om kontinui-tetshantering för informationstillgångar finns i Metod https://www.informationssakerhet.se/metodstodet/utforma/#kontinuitetshantering-för-informationstillgångar-anchor ationssä-kerhetsarbete via www.informationssakerhet.se/metodstodet/utforma/#kontinuitetshante-ring-för-informationstillgångar-anchor. Information om kontinuitetshantering för andra tillgångar finns på www.msb.se/kontinuitets-hantering.

Kommunicera till ledningen regelbundet, kort och koncist. Redogör för vad ni gör, varför och förklara risker och dess konsekvenser. Var aktiv och bidra med beslutsunderlag så att ledningen kan fatta riskmedvetna beslut.

Skjut upp inplanerade icke nödvändiga systemändringar.

RÅD TILL DISTANSARBETAREN
(MSB, 2020)

Vilka regler gäller för distansarbete i din organisation? Ta reda på vad som gäller och följ dem så att du inte blir en säkerhetsrisk. Håll dig informerad eftersom reglerna i kristider kan förändras snabbt.

Vilka regler gäller för uppkoppling mot arbetsplatsen/organisationen? När du kopplar upp dig mot organisationens it-miljö, följ reglerna. Ditt hemmanätverk kan av olika anledningar vara osäkert och inte ge informationen tillräckligt skydd. Kräver din organisation att du använder en VPN-tjänst eller tvåfaktorsinloggning? Finns krav på att enbart koppla upp dig via mobiltelefonen och använda mobildata? Du behöver veta vad som gäller.

Om det uppstår begränsningar i antalet uppkopplade medarbetare behöver ni komma överens om hur ni kan lägga upp arbetet och prioritera det viktigaste i verksamheten. Håll dig informerad om vad som gäller och hur ni kan hjälpas åt att minska belastningen. Exempelvis kan du bli ombedd att arbeta lokalt och enbart koppla upp dig korta stunder eller vissa tider.

Om du inte har åtkomst till organisationens informationssystem, på grund av att nätverket har gått ned behöver du få råd om hur du kan spara informationen på ett säkert sätt. Spara aldrig känslig information i privata molnlösningar.

RÅD TILL DISTANSARBETAREN
(MSB, 2020)

Din arbetsutrustning – dator, surfplatta eller mobiltelefon är personlig och ska inte användas för privat bruk eller av andra. Informationen där ska skyddas. Det innebär att du alltid ska logga ut och låsa datorn när du lämnar den, även hemma. Ingen annan ska ha tillgång till utrustningen eller kunna ta del av informationen. Säkerställ att du har starka lösenord.

USB-minnen ska inte användas mellan privat utrustning och din arbetsdator eftersom virus kan spridas mellan enheter.

Tänk på att skydda också viktig information som finns på papper och i anteckningar. Förvara din information säkert och tänk på att låsa utrymmen där känslig information finns.

Vid digitala arbetsmöten, bedöm risken att andra kan höra eller se informationen som förmedlas.

Minska risken för att bli utsatt för bedrägeri genom att låta bli att klicka på länkar eller bilagor från okända avsändare. Ladda heller inte ned program som kommer via e-post, sms eller olika webbsidor, särskilt när avsändaren är okänd.

KOMPETENSBEHOVET

HÖGSKOLAN I SKÖVDE

Foto:

Global kompetensbrist inom cybersäkerhet

Enligt en rapport från det brittiska rekryteringsbolaget Marlin Hawk kommer bristen på it-säkerhetschefer att förvärras de kommande fem åren. Den globala industrirapporten utforskar rollen, demografin och de utmaningar som it-säkerhetschefer står inför.

https://unt.se/artikel/wl65g88r

Bristen på relevant kompetens inom cyber-säkerhet är ett samhällsproblem

I den nya rapporten *Cybersäkerhet i Sverige – Hot, metoder, brister och beroenden* som släpptes i dagarna beskrivs bristen på relevant kompetens inom cybersäkerhet som ett samhällsproblem. FRA, Försvarsmakten, MSB och Säkerhetspolisen tillsammans med Polismyndigheten har gemensamt tagit fram rapporten och den visar på allvarliga risker i Sveriges säkerhet.

Vi har sedan länge varit medvetna om den kompetensbrist som finns inom cybersäkerhet. Bara i Sverige kommer det saknas 70 000 personer inom IT-sektorn redan är 2022 enligt IT & Telekomföretagens rapport *IT-kompetensbristen – en rapport om den svenska digitala sektorns behov av spetskompetens.* Detta är dock inte endast ett nationellt problem utan en global utmaning som de flesta länder måste hantera. Enligt (ISC)² studie *Cybersecurity Workforce Study* från 2019 bedömer man att det saknas över 4 miljoner personer med kompetens inom Cybersäkerhet globalt.

https://www.mynewsdesk.com/se/it-total/blog_posts/bristen-paa-relevant-kompetens-inom-cybersaekerhet-aer-ett-samhaellsproblem-93077

HÖGSKOLAN
I SKÖVDE

TACK !!!