INDUSTRIELLA UTVECKLINGSCENTRA
IUC SYD

Välkommen till webbinarium 9/12, kl 15-16: Cyberangreppen ökar – vad behöver vi ha koll på?

KPMG:s omvärldsbevakning och hotbildsanalys visar att digitala incidenter som hotar informationssäkerhet och trygghet har ökar avsevärt under den globala pandemin

KPMG:s cyberspecialister Patrick Bladh och Stefan Schreiter informerar och ger råd under dagens webbinar.

Ställ gärna frågor löpande i chatten. Uppskattar om ni stänger av kamera och ljud när webbinariet börjar kl 1500

KPMG

REGION SKÅNE

EUROPEISKA UNIONEN
Europeiska regionala utvecklingsfonden

KPMG

Det digitala säkerhetsläget 2020

9 December 2020

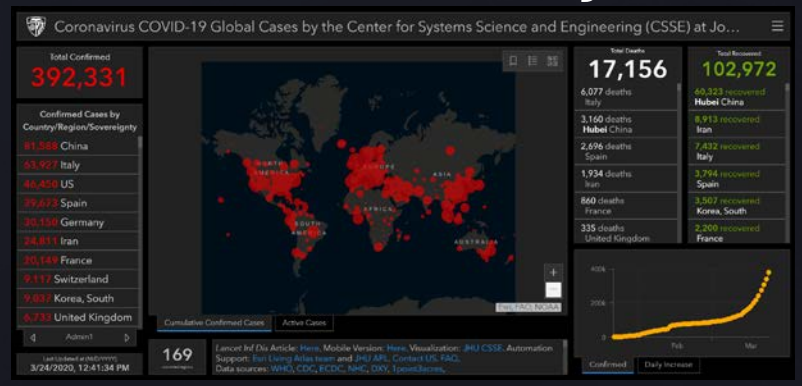
Ett tufft år för sjukvården även avseende Cyber

Den sedan tidigare mycket utbredda ransomwareepidemin riskerar att orsaka stora konsekvenser om kritisk infrastruktur drabbas. Exempel på detta är primär- och sekundärvård, elförsörjning.

Brnos universitetssjukhus drabbades av en ransomware attack och tvingades stänga ner hela sitt nätverk.

Det första dödsfallet till följd av ett cyberangrepp rapporterades i Tyskland på universitetssjukhuset i Düsseldorf

Utpressning mot enskilda patienter till psykoterapiföretaget Vastaamo i Finland.



Coronavirus, COVID19, folkhälsa och hälsoråd används som förevändning vid phishing och skadlig kod. Både kriminella och statsaktörer använder coronaviruset som en bakgrundshistoria för intrångsförsök, med infekterade filer med råd, karantänsinstruktioner m.m. bifogas.

En kopia av en populär spridningskarta (John Hopkins) har använts som en del av ett kit för att sprida malware.

Källor: https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/
https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus
https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html
https://www.svd.se/patienter-utpressas-efter-hackning-i-finland
https://isc.sans.edu/forums/diary/COVID19+Themed+Multistage+Malware/25922/

https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/

Cyberrelaterade händelser 2020

Sårbarheter i legacy-system

Stulna credentials genom spearphishing

Återanvända credentials stulna och läckta

Supply chain attacks

- Typosquatting
- Attacker mot OSS/github
- SaltStack
- FireEye

CVSS 10: Zero-Logon – utmaningen med OneDay- sårbarheter. Även Citrix buggen från i julas spökade långt in på året.

Drovorub - GRU's verktygslåda för Linuxssystem.

Entreprenörskap bland de cyberkriminella – diffrentiering och specialisering och mikrotjänstutbud har visat sig vara framgånsrikt för cyberkriminella. Trickbot har visat att Access-as-a-Service är ett fungerande koncept. DarkBasin har gjort motsvarande på konsultbasis.

Ransomware-epidemin påverkar cyberförsäkringar. Det kommer ställas högre krav på säkerheten hos de försäkrades organisationer.

US Treasury gick ut och varnade för att betala ut ransom till entiteter under sanktioner.

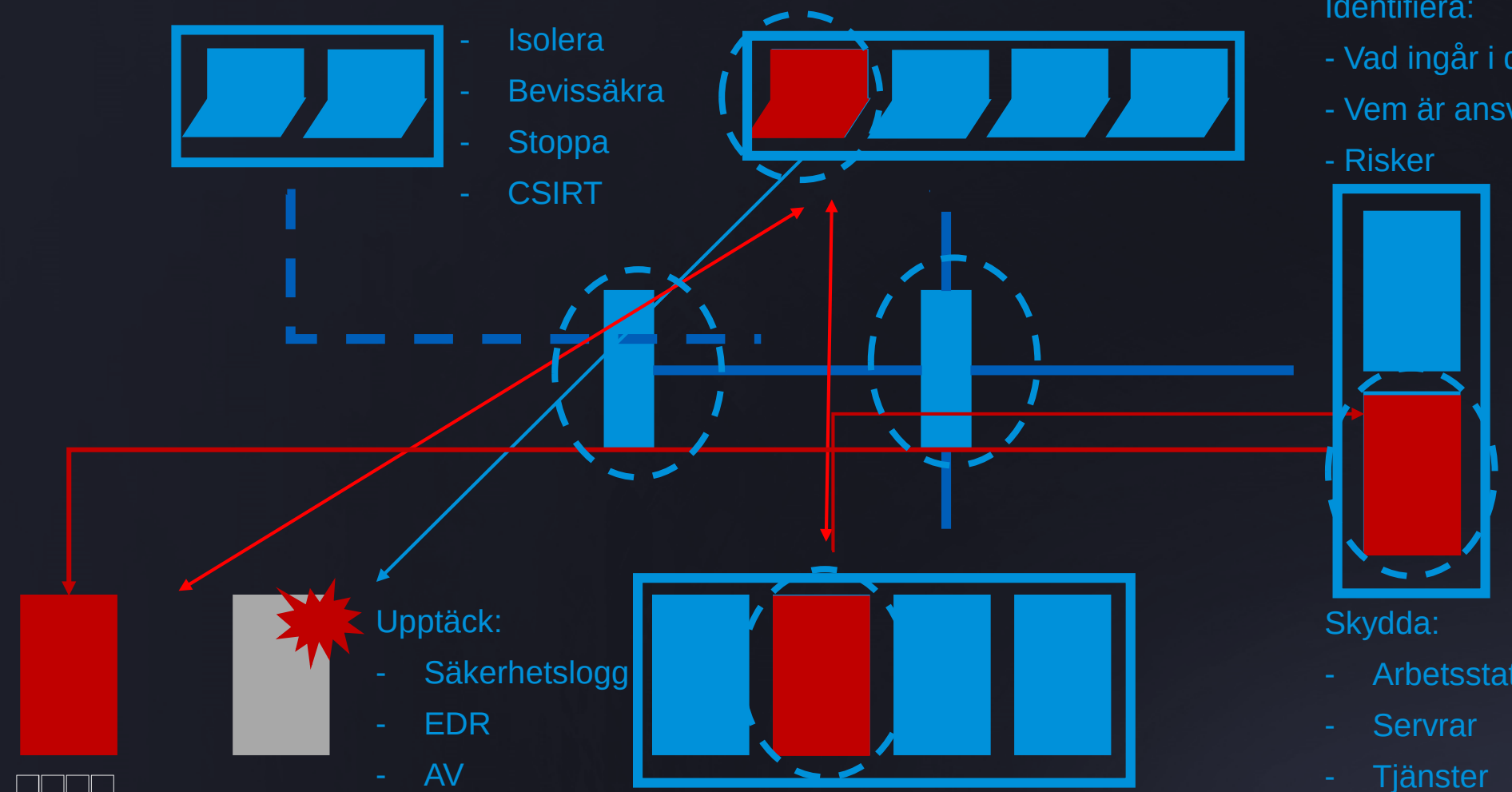
KPMG

Vad ingår i Cybersäkerhet?

Återställ:
- Arbetsstationer och Servrar
- Anmälan och rapportskyldighet
- Patcha och Utbilda

Hantera:
- Isolera
- Bevissäkra
- Stoppa
- CSIRT

Identifiera:
- Vad ingår i din miljö?
- Vem är ansvarig?
- Risker



Upptäck:
- Säkerhetslogg
- EDR
- AV
- DLP
- SOC

Skydda:
- Arbetsstationer
- Servrar
- Tjänster
- Utbildning och Awareness

KPMG

Lärdomar att dra från det gångna året

- Zero-trust modellen med djupförsvar har blivit allt mer viktig ju flexiblare vår digitala arbetsmiljö behöver vara.
- Säkerhetsövervakning och framförallt förmåga att agera på larmsignaler har varit A och O för att hantera cyberangrepp.
- DLP och övervakning av var organisationens information flödar ger en ytterligare dimension för att agera.
- Användarhantering och IAM ger en grundplatta för att hantera tillgången till organisationens interna information.
- Det kommer bli svårare att försäkra bort framförallt utpressningssummor.

KPMG

Säkerhetsåtgärder vid fjärrarbete

- Använd multifaktorautentisering
- Se till att all trafik går genom organisationens VPN så att den blir synlig för era interna sensorer
- Tillhandahåll säkra alternativ till era anställdas behov.
- Få grepp om er identitetshantering och tillämpa principen om lägst privilegium
- Testa er säkerhet, testa er detektionsförmåga och testa er responsförmåga – övning ger färdighet
- Komplettera patchprocessen med en rutin för kompensatoriska åtgärder.

Din plats på marknaden - ett ofta bortglömt skyddsvärde

När organisationer tittar på sitt behov av cybersäkerhet blir fokus ofta:

- Företagshemligheter och IP
- Kreditkortsuppgifter, betalflöden, bankuppgifter
- Personuppgifter
- Affärskritiska system

Vad som dock visat sig om och om senaste åren är att en viktig aspekt är: organisationens plats på marknaden och i en leverantörskedja.

Exampel:

- Zoom – 10 års marknadsresa på en månad
- M.E.Doc – Skatterapportering för Ukraina
- OpenSSL – Någon som kommer ihåg Heartbleed?

Vad finns downstream från din organisation?

KPMG

Informations - och IT-säkerhetsorganisationens utmaningar

- Endast lokala resurser övervakas
- Bristande överblick i moln, outsourced IT eller i leveranskedjor
- Angrepp och dess efterspel upptäcks ofta inte
- Upptäckt och försvar bygger på inkommande hot
- Incident detektionstid mellan 50-100 dagar
- Förebygga kommande incidenter via ett systematiskt säkerhetsarbete
- Utmaningar kring kommande digitaliseringsprojek

KPMG Threat Intelligence-tjänst och ett systematiskt säkerhetsarbete

- 24/7 extern övervakning utan sensorer
- Tillgänglig globalt för publika ip adresser
- Flera korrelerade hotflöden
- Automatiska larm
- Sektorspecifika rapporter
- Audit och nulägesanalyser kring säkerhetnivån
- Riskbaserat arbetssätt

*** KPMG TI ersätter inte IDP, EDR eller antivirus, det är ett tillägg till befintliga säkerhetskontroller**

KPMG

Summering

1. Svårt att veta om du är exponerad
Precis som de hälsomässiga riskerna med Covid -19 är det svårt att veta om du påverkats av de digitala riskerna. Både intern och extern övervakning behövs

2. Din organisations cybersäkerhetsbeteende bör vara heltäckande
Genom att praktisera cybersäkerhet i vardagen och bygga en säkerhetskultur kommer skyddet att öka i takt med medvetenheten om riskerna. Förstärk förmågan att hantera kommande förändringar genom ett systematisk och riskbasera säkerhetsarbete.

3. Tänk på att din organisations behov av Cybersäkerhet kan vara större än du tror
Din plats på marknaden och i leverantörskedjan kan vara just det som en angripare vill åt.

KPMG

© 2020 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Frågor

© 2020 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Kontaktuppgifter

Per-Olov Humla
E-post: per-olov.humla@kpmg.se
Tel: +46 708 80 88 70

Stefan Schreiter
E-post: stefan.schreitet@kpmg.se
Tel:+46 70 939 68 05

Patrick Bladh
E-post: patrick.bladh@kpmg.se
Tel:+46 70 939 65 83

© 2020 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

INDUSTRIELLA UTVECKLINGSCENTRA
IUC SYD

Tack för visat intresse!

Vill ni veta mer om IUC Syd eller om projektet SPIRA är ni varmt välkomna att kontakta mig på camilla.dahlin@iucsyd.se

Årets sista webbinar i denna serien

Den 16/12 kl 15-16 – Dra ner eller investera, konkreta tips och belysning av IP-strategi, patent och varumärke.
Webbinar tillsammans med AWA

KPMG

REGION SKÅNE

EUROPEISKA UNIONEN
Europeiska regionala utvecklingsfonden