Om Kau skulle ha hackats

Erfarenheter från en krisövning

Krisövningen den 2016-02-23

- En krisövning beställdes av rektor
- Skulle öva krisledningsgruppen, KLG
  - Nyckelpersoner var förvarande om datum och uppbokade
- Informationssäkerhetsinriktning, med fokus på kontinuitet
- Hjälp av MSB med scenario
- Hjälp från räddningstjänsten som spelledare
- Övningen höll på i cirka 4 timmar

Niklas.Nikitin@kau.se

Övningsdeltagare

De som övades (KLG)

- Rektor (valde vem som skulle kallas in)
- Prorektor
- Kommunikationschef
- Enhetschef IT (IT-chefen var *bortrest*)
- Universitetsdirektören
- Chefen för ledningskansliet
- Rektors sekreterare
- (Kriskommunikationsgruppen)

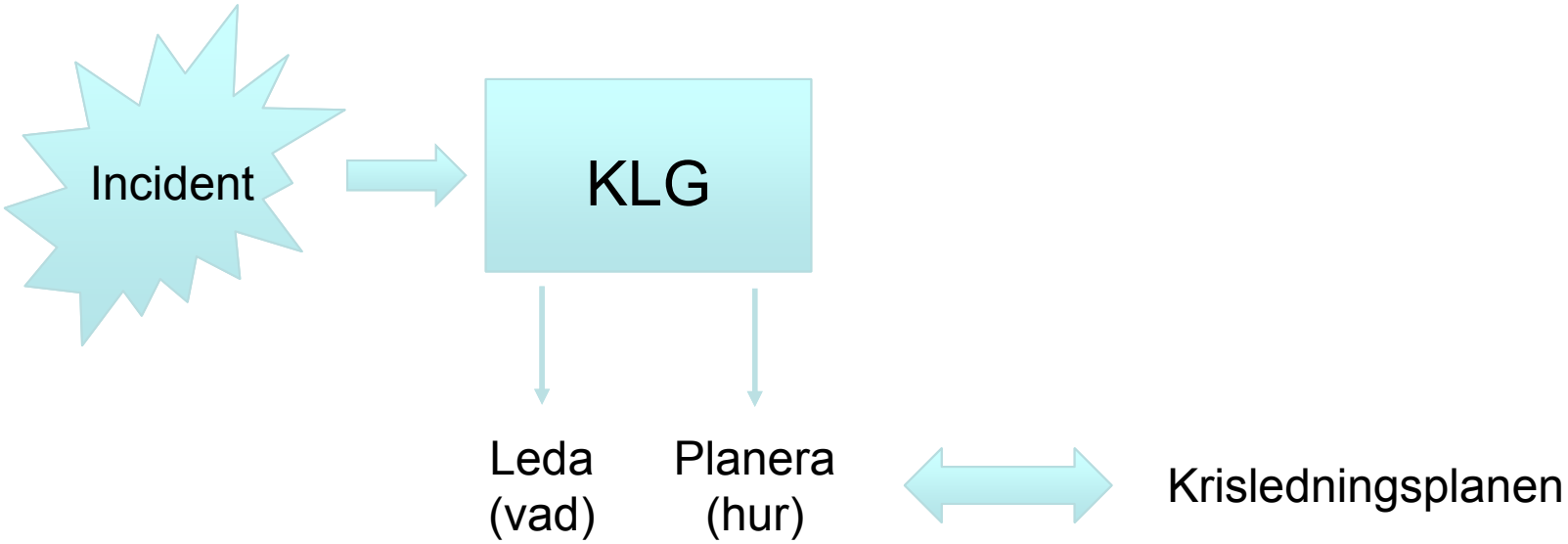
Övningsgruppen

- Säkerhetschefen
- Säkerhetskoordinator, räddningstjänsten
- Informationssäkerhetsansvarig
- IT-säkerhetssamordnare
- Projektingenjör
- Polis
- Press
- Huvudskyddsombudet
- Tre deltagare från IT-avdelningen
- Studentkårens ordförande
- Fem inringare

Niklas.Nikitin@kau.se

Vad som övades

- Metod: Problembaserat lärande, PBL



Niklas.Nikitin@kau.se

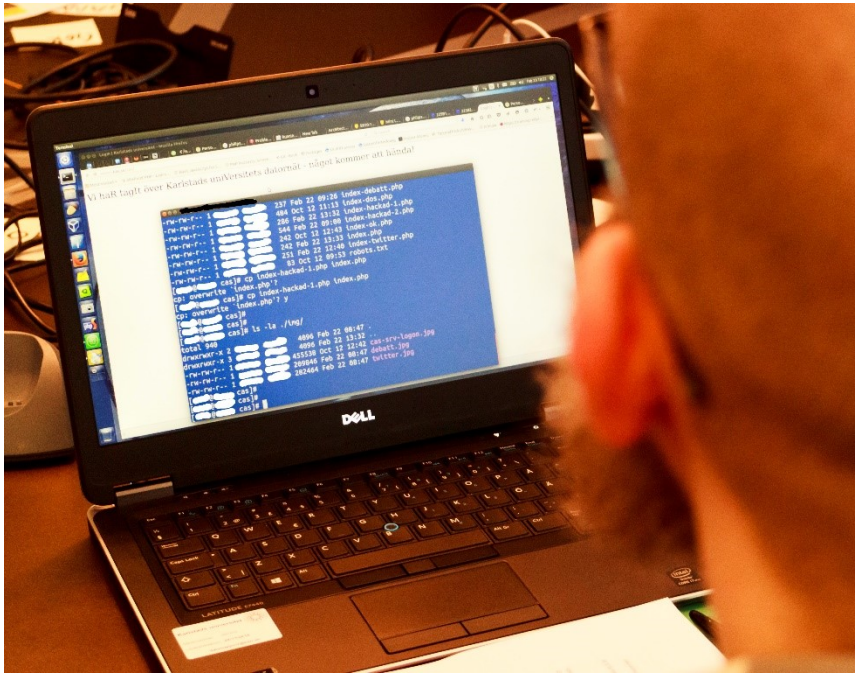
Scenario

1. En lektor publicerar ett debattinlägg
2. RiV hackar CAS
3. RiV ddosar Kau:s webbplats och CAS
4. RiV kommer med fysiska hot
5. Utrymning av hus
6. Överlämning

Niklas.Nikitin@kau.se

Inspel

- Webben
  - RiV
  - IT-avdelningen
- Telefon
  - Press
  - Medarbetare
  - Studentkår
  - IT-avdelningen
  - RiV
- Besök
  - Press
  - Studentkår
  - IT-avdelningen
  - Medarbetare



Niklas.Nikitin@kau.se

Kommunikationsvägar ut från de som övades

- Telefon
  - Växel
  - IT-avdelningen
- Sociala media, web
  - Worddokument
- *Live feed*
  - *Ljud och bild till övningsgruppen*

Niklas.Nikitin@kau.se

Deltagarna skall föra en loggbok

Tidpunkt	Vxl	IT	KLG	KKG
10.15	Säkchef går in till rektor och prorektor och ger förutsättningarna för övningen.			
10.21	Rektor sammankallar krisledningsgruppen som kommer			
10.24	Projektorn kopplas upp			
10.25			Krisgrupp inkallad – Webben är hackad Rektor kallar in de två lagen för att informera om vad som är på gång Studentcentrum är på väg på konferens ej här	
10.26	Ringer efter Enhetschef IT			
10.26	Prorektor ringer studentcentrum, de är på tjänsteresa			
10.27	Rektor vill kalla in båda krisgrupperna			
10.28	Chefen för ledningskansliet kommer			
10.31	Säkchefen går in och förtydligar vilka telefoner som är tillåtna att använda			
10.32	IT-avd ringer till rektor och informerar att det är problem	Vi har vi sett att CAS tjänsten ligger nere, IT-avd ringer enhetschef IT	De två lagen är samlade – (ej ngn fr studentcentrum) – Rektor informerar om läget IT ringer, är medvetna om att sidan är hackad	
10.35	Kommunikatör kommer. Pressen ringer och rektor ber att få återkomma eller om han kan återkomma om 5 minuter			
10.36			Inkommande telefonsamtal till rektor – ringer tillbaka om 5 min – P4 Värmland som ringde – Enhetschef IT informerar P4 Värmland om vad som händer Kommunikationschef kallar in teamet kommunikation som lägger ut på sociala medier	
10.38	Kårordförande kommer in och meddelar att studenterna har problem med inloggning		Studentkåren kommer och frågar om vad som händer – många studenter som ring och undrar	

Niklas.Nikitin@kau.se

Erfarenheter från att arrangera denna övning

- Viktigt med en erfaren spelledare.
- Bygg ett tidsflöde med post-it lappar i olika färger för respektive tänkta aktiviteter (telefonsamtal, besök, uppdatering av webb etc) som kan flyttas, läggas till respektive tas bort. Använda aktiviteter markeras.
  - Var dynamisk med aktiviteterna, använd dem när de behövs.
- De som övas kommer inte att följa tänkta flöden. ☺
  - Improvisera och ändra scenario, men koordinera med spelledaren!
- Noggrann genomgång så att alla vet sin roll.
- Ha någon ansvarig som koordinerar de som skall ring in.
- Ge ett detaljerat speldirektiv till de som skall övas.
  - Inte använda egen mobil, ej lämna lokalen etc.
- Styra all kommunikation in respektive ut.
  - Isolera de övade.
- Ordna mat och dryck till de som ansvara för övningen.
- Gasa inte på för mycket, ge de som övas tid.
- Hantera all personer som inte är med i övningen men ändå skall behöva att nås.
  - En/några person som agerar som alla dem.
  - Registrera och bekräfta.

Niklas.Nikitin@kau.se

Val av tidpunkt för övningen

- Gärna strax innan antagning till höst- respektive vårtermin.
  Vår övning var först tänkt under hösten 2015 (antagningsveckan för vårterminen), men pga hot via Jodel (http://www.svt.se/nyheter/lokalt/varmland/hot-mot-universitetet-i-karlstad) blev övningen inställd.
- Cirka en vecka efter vår övning var det stora ddos-attacker mot mediahusen (https://www.cert.se/2016/03/overbelastningsattacker-mot-media) – detta blev en snackis hos ledningen på Kau.

Niklas.Nikitin@kau.se

Synpunkter från de övade (KLG)

- Bra övning och bra upplägg
- Realistisk övning
- Viktigt och angeläget att öva kontinuerligt
- KLG kändes mer övade (säkrare i sitt agerande), men KLG2 behöver övas
- Övningsförutsättningarna begränsade handlingsutrymmet rent övningstekniskt
- Önskar övning/utbildning i stabsmetodik

Niklas.Nikitin@kau.se

Erfarenheter och efterspel från övningen

- Övning ger färdighet, mycket kortare startsträcka jämfört med tidigare övningar.
- En förståelse av IT-incidenter och kontinuitetsplanering hos universitetsledningen.
- IT har fått i uppdrag att ta fram rutiner för kontinuitetsplanering.
- Hur skall funktioner med fysisk placering (fasta arbetsplatser) hanteras vid en utrymning och ändå kunna fungera?

Niklas.Nikitin@kau.se

Uppmärksamhet i pressen

- http://www.tjugofyra7.se/globalassets/tjugofyra7-pdfer/tjugofyra7_nr_29_2015.pdf
- http://sverigesradio.se/sida/artikel.aspx?programid=93&artikel=6391601

Universitet

Nu ska myndigheter rapportera IT-incidenter

Nu vill regeringen att statliga myndigheter ska ha bättre koll på vilka hot de möter från Internet. Från den förste april ska myndigheter rapportera in IT-incidenter till bland annat Myndigheten för samhällsskydd och beredskap - MSB.

Richard Oehme, verksamhetschef för cybersäkerhet och skydd av samhällsviktig verksamhet på MSB, hoppas nu att organisationer verkligen börjar tänka över hur de hanterar IT-hot.

– Alla bör ta det här på allvar och ta upp det i ledningsgrupper, säger Richard Oehme. Det här är ingen IT-fråga, det är en strategisk fråga för respektive ledning att hantera.

Trots att man kommit en lång bit på väg så anser Richard Oehme att det finns mycket kvar att göra.

– Det är en utmaning när IT-utvecklingen går så snabbt framåt att det tar en hel del tid att vidta de här säkerhetsåtgärderna.

En vanlig miss som organisationer gör, enligt Richard Oehme, är att inte ha koll på var inhyrda serverhallar i praktiken står - ibland kan de vara inhyrda i både andra och tredje hand och kanske finnas utomlands. Och där förvaras då känslig information.

Attacker kan till exempel handla om hemsidor som kapas och fylls med oönskad information, om sidor som bombarderas med information så att de slutar fungera eller virusprogram som låser viktig information och kräver lösen för att öppnas.

En organisation som valt att öva att hantera en IT-attack är Karlstads universitet, där Jan Gambring är säkerhetschef.

– Att få en IT-incident är idag mer sannolikt än att få en rent fysisk incident på sig, säger Jan Gambring.

Vilka krav ställer det på er?

– Att vi hela tiden måste ha en beredskap för att det kan hända någonting och att vi hela tiden har verktyg så att vi kan jobba emot eventuella incidenter.

IT-struktur slogs ut och det var skälet till att krisledningsgruppen kallades in. Gruppen utsattes för olika alternativ och hoppas att det kommer att skapa nya rutiner, säger Niklas Nikitin.

GUNNO IVANSSON

Niklas.Nikitin@kau.se

Detaljerat (tänkt) scenario, del 1 (det blev inte så här)

1. Säkerhetschefen går in till Rektor med information om att CAS-sidan är hackad – inga webbtjänster (inslaget, min-sida, Box, egenrapportering etc) med inloggning går inte att komma åt. Ingen avsändare är angiven. Användarna möts av ”Vi har tagit över Karlstads universitets datornät – något kommer att hända!”.
   - säkerhetschefen lämnar över papper med relevant information
2. Rektor kallar krisledningsgruppen (KLG).
3. Enhetschef IT bör ringa IT-avd. Om inte, så ringer IT-avd 5 minuter efter att hela KLG är samlad
   - Enhetschef IT frågar IT-avdelningen, får ett svar – vi kollar och återkommer.
4. Pressen ringer Rektor. Har sett den hackade sidan.
5. Studentkåren undrar hur det ska gå med alla studenterna
6. IT-avdelningen avvaktar cirka 10 minuter med att ge ett initialt ger ett lugnade felaktigt svar – vi är hackade, men kan snabbt återställa problemet.
7. Administratör ringer SA-chef om Ladok. Forskare ringer Enhetschef IT. *Tyske professorn* ringer Rektor.
8. IT-avdelningen återkommer efter 5 minuter med korrekt svar.
9. Hemsidan uppdateras av hackarna med avsändare (Rävjägarna i Värmland [RiV]) och anledning om varför dom har angripit Kau. En biolog har som privatperson talat negativt om rävjakten och skrivit under debattinlägget som lektor Kau. ”Universitetet ska straffas för att dom har anställda som på gravt felaktigt sätt hänger ut rävjägare. Rävjägare som är en viktig del av den Värmländska kulturen. Hur kan ni ha anställda som Björn Niklasson och låta denne föra er talan. Han måste bort!”
10. Debattinlägget visas på hemsidan.
11. IT-avdelningen oinbjudna kommer in och ger en stressad, förvirrad superteknisk presentation, med två olika lösningsförslag
    - Återställa från backup
    - Rensa manuellt
12. Beroende på KLG beslut så agerar IT-avd
13. Pressen besöker Rektor. Ifrågasätter lektorns uttalande, finns det ingen policy om hur man får uttala sig?
14. Studentkåren frågar Univ.dir hur det ska gå med alla studenterna
15. IT-avdelningen meddelar Enhetschef IT att problemet är löst enligt önskemål
16. Osäkerhet med om tentamens anmälan har kommit in? Förälder ringer SA-chef.

Niklas.Nikitin@kau.se

Detaljerat (tänkt) scenario, del 2 (det blev inte så här)

17. Kau:s webbplats och CAS ddos:as, och är inte tillgängliga
    - (interna system slutar därför att fungera.)
18. Telefon till rektor om att RiV har ddos:at Kau och att Björn Niklasson ska bort.
19. Pressen ringer Kom.ch.
20. Studentkåren undrar hur det ska gå med alla studenterna, Univ.dir
21. Forskare ringer Rektor.
22. Om Enhetschef IT inte kontaktar IT-avdelningen så ringer de efter ett tag med två lösningsförslag och en fråga (tentamens anmälan, information om kurser etc):
    - Hålla upp sidan så länge det går med stora störningar på interna system
    - Statisk hemsida med begränsad av information, inga störningar på interna system
    - Vilken server ska prioriteras?
23. Lösningen från krisgruppen implementeras
24. Lärare ringer Univ.dir (som är ytterst ansvarig för systemen).
25. Administratör ringer IT-chef eftersom problemen inte löser sig.
26. IT-avdelningen meddelar att ddos:en dör ut.
27. Paus ca 20 min
28. Pressen ringer Kom.ch – fråga – hur ska ni förhindra detta i framtiden?
29. Huvudskyddsombudet kommer in med patroner och brev som är hittade i biologis lokaler, tillsammans med hot mot biologilektorn.
30. RiV kontaktar rektor och begär ett dementerande av biologilektorns uttalande, annars kommer något att hända i hus 5F.
31. Hus 5F utryms och meddelas KLG.
32. Orolig medarbetare ringer Pers.ch från hus 3 och undrar vad som händer i 5F.
33. Välkomstcenter meddelar att en misstänkt person med vapenfodral har synts i huvudingången.
34. Om ledningen ringer Polis så kommer de och meddelar om falskt larm och status uppdatering.
    - Det var ett musikinstrument personen bar.
35. Säkerhetschefen befaller överlämning till det andra krislaget. Informera krisgruppen att det är dags att lämna över.
36. Övningen avbryts.
37. Säkerhetschefen och resten av övningsledningen håller några slutord.

Niklas.Nikitin@kau.se

Frågor?

Tack för er uppmärksamhet!

Niklas.Nikitin@kau.se