
UMEÅ UNIVERSITET

IT-säkerhet
Tek Nat Prefektmöte

IT-chef

2015-03-12

Ämnen

- IT-säkerhet
- Behörighetsmodell
- Riskanalys
- Aktiviteter under 2015

Jag behöver en dialog med er om IT-säkerhet

IT-säkerhet vid UmU

- Skydda våra resurser
- Upptäcka intrång
- Agera mot oönskade händelser

- Riskhantering mycket viktigt
- Ärendehantering för alla IT-säkerhetsincidenter

IT-säkerhet

- 2.575 IRT-incidenter under 2014. Ökning med 100% sedan 2013
- Stort mörkertal då många incidenter inte blir inrapporterade
- Varje sekund görs 10 hackningsförsök mot Root-konton på server
- IT-säkerhet utgår från systemarkitektur
- Regelbundna säkerhetsgranskningar och analyser
- Stenhård kontroll på access och behörighet
- Nya hot hela tiden, vi är reaktiva och försöker fixa …..
- Vi måste bli proaktiva

IT-säkerhet, forts

- Stort intrång april 2014. Påskincidenten, 300 system angripna
- Sommaren 2014. 60 skrivare attackerade
- TV-apparater hackade
- Klimatstyrningsutrustning angripna
- Videokonferensutrustning angripen
- Vad ligger och väntar …….?

IT-säkerhet, forts

- Den svarta onsdagen den 7 januari
- Sex av våra medarbetare svarade på phisingmail den dagen
- De blev blockerade av vår Ironport
- Jmf. utbildning vs. tekniska skydd
- Nollvision för phising och intrång
- Berörda prefekter kontaktas alltid

Behörighetsmodell

LOA – Level Of Assurance	Accestyp	Anm
LOA 0	Gäst.	Ingen kontroll
LOA 1	Identifierade användare.	AD, CAS, annat
LOA 2	IT-utvecklare. Checka in/ut kod.	ITS, Yubikey
LOA 3	Serveransvariga. Root-konto.	ITS. Yubikey

Riskanalys

Sannolikhet				
4	Nätscanningar	Nätattack	Internet of Things	Roothack/AD-hack
3			CAS	
2			Läckage av skyddade ID/org	DNS-hack
1			Passagesystem	Nätutrustning
	1	2	3	4
				Konsekvens

Basaktiviteter IRT

- Incidentmottagning och Incidenthantering
- Scanningar/kontroller över hela UmU
- Granskningar
  - Beställda av institutioner
  - Internt beordrade
- Utbildning och Information
- Omvärldsinformation
- Rådgivning

Projektaktiviteter 2015

- Utveckla IT-säkerhetsorganisationen
- Inför 2-faktorautenticering
- Utveckla logganalyser
- Se över brandväggar
- Inför Trustsec för utrustning?
- Inför DNSSEC på umu.se
- Inför IPv6 på umu.se
- Ge extra Information och utbildning

IT-säkerhet

- Utbildningsinsatser
- Förstärkning av IT-säkerhetsinformationen till verksamheten. Test av förslag.
- En starkare IT-säkerhetsorganisation med tätare koppling mellan institutionerna och IRT-funktionen. Hur kan den se ut?
- Interna granskningar. Mandat för genomförande.
- Införande av 2-faktorautenticering vid institutioner som har egen IT-drift.
- Förväntningar på rådgivningskapacitet i IT-säkerhetsfrågor.

Utbildning, för vem? VT 2015

- IT sys adm och IT kontaktpersoner
  - Olika innehåll och omfattning
- IT-säkerhet, vad är det
- Proaktivitet
- Utredningar och analyser
- Rapportering
- Etablera IT-säkerhetsorganisation

Kursinnehåll för lokala IT-tekniker

- Krypteringstekniker
- Public-Key kryptering, Yubikey
- Meddelandeautenticering
- Autenticering och Hash-funktioner
- Kryptering
- Digitala signaturer och autenticering
- Protokoll
- Autenticeringsapplikationer
- E-post-säkerhet
- IP-säkerhet, nätverkssäkerhet
- Webb-säkerhet
- Intrång och virus
- Brandväggar

IT-säkerhetsorganisationen

- Ansvaret – linjen
- Sunet nationell CERT (Computer Emergency Response Team).
- IRT (Incident Response Team) den lokala IT-säkerhetsnoden. Vårt ansvar enligt avtal med Sunet.
- Behov av kontaktpersoner vid institutioner och enheter
- Behov av återkoppling om incidenter och åtgärder

Interna granskningar

- Scanningar av vårt nätverk efter brister
- Genomlysning av centrala applikationer
- Nätverksanalyser
- Lokala applikationers access till centrala system
- Modell för access till centrala uppgifter

Införande av 2-faktorautenticering vid institutioner som har egen IT-drift

- Centralt införande av Yubico
- Möjlighet eller obligatoriskt för inst att ansluta sig till Yubico
- Placering av viktig IT-utrustning i ITS datorhall

Rådgivning i IT-säkerhet

- Info till prefekter
- Info till nyanställd personal
- Resurser vid IRT om IT-säkerhet
- Vad tillhandahålls centralt och vad kan köpas?

Utvärdera
Utbilda
Hantera