Erfarenheter från IRT-verksamhet

Einar Hillbom

UMDAC

Umeå Universitet

IT-organisation

- **IT-enheten** ingår i universitetsförvaltningen och har det strategiska ansvaret för universitetets IT-användning.
- **UMDAC** tillhandahåller service, tjänster och datorkraft för Umeå universitet. Institutionerna har dock frihet att välja annan leverantör. Samarbetar med IT-enheten i säkerhetsfrågor.

IRT-gruppen

Består av 4 personer:

1 st Gruppledare 100% IRT

2 st 50% IRT, 50% UNIX-drift

1 st 50% IRT, 50% NT-drift

IRT-gruppens huvuduppgifter

Hanterar och utreder:

- **Missbruk av nätverks- och datorresurser**
- **Intrång**
- **Intrångsförsök**
- **Oetiskt uppförande**

IRT-gruppens övriga verksamheter

- **Policy-CA inom SwUPKI**
- **CA för Umeå universitet**
- **Arrangerar föreläsningar inom datasäkerhetsområdet för universitetets systemadministratörer**

Befogenheter

- **Rätt att utan enhetschefs tillstånd när som helst tillkalla nät- och driftpersonal.**
- **Rätt att utan enhetschefs tillstånd utnyttja obekväm arbetstid.**
- **Rätt att under utredning stänga av datorsystem och nätverksanslutningar.**
- **Rätt att när som helst på dygnet kontakta IT-enhetens chef.**

Exempel på incidenter

- **Hackade institutionsdatorer**
- **Studenter som distribuerar upphovsrättskyddad musik, film och programvara**
- **Scanningar och intrångsförsök mot universitetets datorer**
- **Kränkande och hotfulla e-mail som skickats via våra mailservrar**

Fler exempel på incidenter

- För hårt utnyttjande av nätverksresurser
- Studenter som upplåter universitetets nätverks- och datorresurser till utomstående
- Scanningar, intrång och intrångsförsök utförda av studenter mot utomstående
- Denial-of-service-attacker mot datorer och nätverksutrustning

Ännu fler exempel på incidenter

- **Spam riktad till universitetsanställda och studenter**
- **Datavirus i e-post**

Datavirus

- Hög medvetenhet bland universitetets personal
- Antivirusprogram med automatisk uppdatering
- Virusscanning i mailservrarna utreds

Förfrågningar utifrån

Ex.vis förfrågningar om vem som innehar ett visst IP-nummer i samband med scanningar, intrångsförsök, e-post etc.

Personuppgifter lämnas EJ ut till annan än rättsvårdande myndighet

Polisförfrågningar

Vi frågar alltid efter polismannens namn.

Vi ringer sedan polisstationen och ber att få bli kopplad till vederbörande.

Det kan vara någon obehörig som försöker få ut uppgifter.

Hantering av incident

1. Avgör om anmälan är korrekt (ex.vis kontroll av loggar)
2. Vidtag lämpliga åtgärder (ex.vis stäng av uttag)
3. Informera (ex.vis IT-enheten, systemadministratör, supportpersonal)
4. Dokumentera (ärendehanteringssystem)

Åtgärder

- Stäng av nätverksanslutning
- Blockera IP-adress i router
- Stäng av e-post-konto
- Stäng av användarkonto
- Tag backup på hackade datorer inom universitetet
- Koppla ev. tillbaka hackad dator på nätet med maximal loggning för att säkerställa ytterligare bevis

Hantering av studenter

- Avstängning av nätverksanslutning i samråd med IT-chefen
- Möte mellan studenten, IT-chefen och delar av IRT-gruppen
- Studenten avkrävs skriftlig, egenhändigt undertecknad redogörelse som diarieförs
- IT-chefen beslutar om ev. anmälan till disciplinnämnd och/eller polis

Polisanmälan

Beslut om polisanmälan tas av IT-chefen som även hanterar anmälningsförfarandet.

I brådskande fall kan ansvarig vid institutionen göra polisanmälan.

Prioriterat

- Datorintrång
- Anmälan från Microsoft, IFPI, MPA etc. om spridning av upphovsrättskyddat material
- Polisanmälningar
- Pågående denial-of-service-attacker

Publika campusnätet

- Labsalar, hörsalar och andra offentliga utrymmen
- Internetåtkomst endast via proxy
- Inloggning med e-postadress och lösenord
- Användning kan spåras i proxy-loggarna

Personal- och studentbostadsnät

- Datorer som kan knytas till en viss anställd eller student
- Inga begränsningar, direktkoppling till Internet.
- Riktning och volym på trafiken kan kontrolleras i routerloggarna

Övervakningsmetoder

- **Automatisk kontroll av routerloggar (NetFlow) för att upptäcka scanningar mot universitetets datorer, onormalt hög utgående trafik (misstanke om servrar med copyrightskyddad film, musik etc.)**
- **Routerloggarna kan fria eller fälla när det gäller påstådda scanningar, intrång eller intrångsförsök.**
- **Proxyloggar kan ex.vis avslöja vem som skickat hotbrev via webmailtjänster, ex.vis Hotmail**

Samarbete med SUNET-CERT

http://www.cert.sunet.se

- **SUNET-CERT i Uppsala assisterar svenska universitet för att förbättra deras IT-säkerhet**
- **SUNET-CERT arrangerar kurser med bl.a. föreläsare från universitet och polisen**
- **Universiteten rapporterar in incidenter till SUNET-CERT som gör sammanställningar**
- **SUNET-CERT går ut med varningar och råd till medlemmarna när något är på gång**

Katten på råttan …

- Om NORDUnet upptäcker attacker mot eller från SUNET kan anslutningen till SUNET stängas av
- SUNET kan stänga av berörda universitet
- Universiteten kan stänga av berörda institutioner
- Institutionerna kan stänga av enskilda datorer

Statistik

2001-01-01 – 2001-09-23

Typ	I år	Senaste månaden
Denial-of-service	3	-
Hackade datorer	17	3
Mail relaying	13	2
Misuse	66	6
Spamming	30	7
Virus	193	82
Scanningar	364	35
Förfrågningar	163	33
Övrigt	68	31