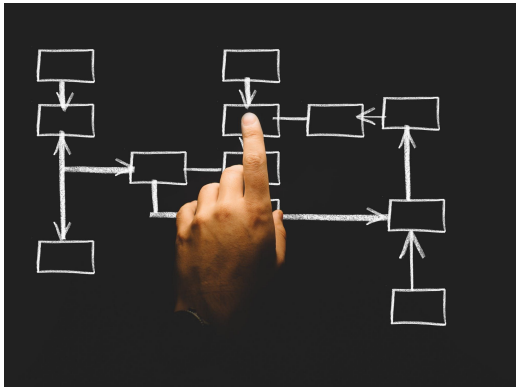
SUNET

SUNET Säkerhetscenter

Nationellt säkerhetscenter för forskning och utbildning

Agenda Onsdag 20/10



1. SUNET Säkerhetscenter
   - 09:00 - 09:15 Välkomna: Intro, David
   - 09:15 - 09:25 Svarstidsmätning och ärendestatistik, Maria
   - 09:25 - 09:55 Aktuella sårbarheter, John
   - 10:00 - 10:45 phpshell, Christoffer Alström

2. DNSSEC m.m.
   - 13:00 - 13:45 DNSLabs @ Internetstiftelsen, Niklas Pousette och Ulrich Wisser, IIS
   - 14:00 - 14:30 Mätning av sektorn, Erik
   - 14:30 - 14:45 Plats för diskussion/frågor

3. Mailfilter
   - 15:00 - 15:45 Mailfilter-NG, Peter Falck, Halon

SUNET SOC

En förändrad hotbild enligt Säkerhetspolisen

Från Säkerhetspolisens årsbok 2020

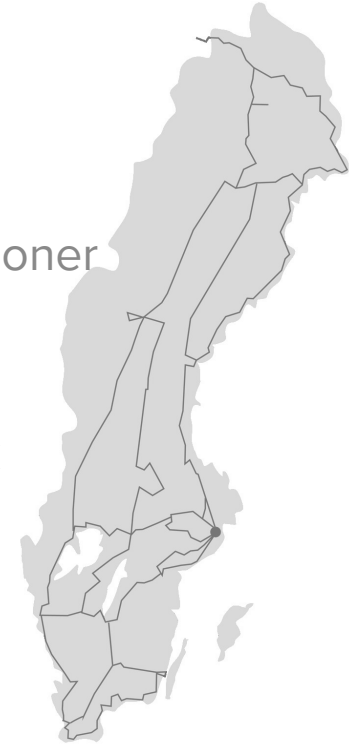
- *“ [...] Säkerhetspolisen bedömer att underrättelsehotet kommer att fortsätta vara högt de närmaste åren. Det kommer främst att rikta sig mot kommersiella mål, militära mål, teknik, forskning och utveckling och mot människor som sökt fristad i Sverige.”*
- *“ [...] Angreppen riktas bland annat mot svensk världsledande forskning och innovation med målet att stjäla kunskap och ta över företag för att olovligen bygga kompetens och förmåga. Säkerhetspolisen uppskattar att den information och kunskap som olovligen inhämtas varje år kan värderas till miljardbelopp.“*

SUNET SOC

Förändringsresan

Med hjälp av de externa finanserna har vi kunnat:

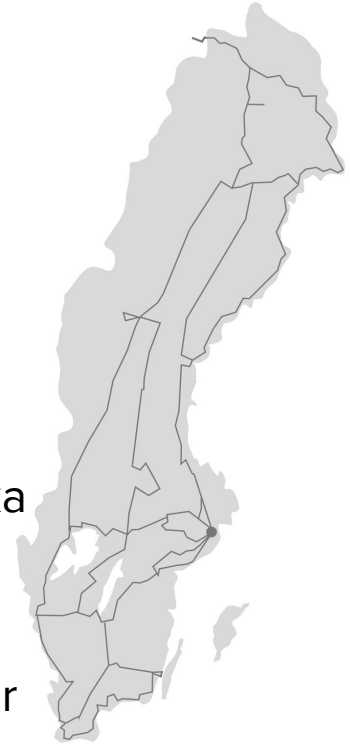
- Frigöra tid för integration och förbättringsarbeten
- Aktivt omvärldsbevakat och notifierat anslutna organisationer
- Stärkt vår förmåga att motstå avancerade angripare
- Prövat och implementerat ny teknik
- Genomfört upphandlingar och avrop inom önskad teknik
- Genomfört workshops / kunskapsspridning



SUNET SOC

Behovsbild / Gå vidare med etableringen

- Fortsatt behov av effektivt informationsutbyte
- Stora mängder attacker och events
- Ökade förväntningar vid distansarbete/digitalisering
- Uppmuntra, utveckla och behålla kompetens inom sektorn
- Det är svårt för små som stora organisationer att övervaka och hantera risker i en global kontext
- Samarbete är en nyckelfaktor
- Skräddarsytt partnerskap för våra anslutna organisationer



SUNET SOC

Grundoperativ verksamhet - Säkerhetscenter

- Omvärldsbevaka och notifiera kring kritiska sårbarheter
- Samordna incidenthantering mellan organisationer och inom SUNETs egna tjänster
- Facilitera och uppmuntra nätverkande, kunskapsspridning och kompetensdelning
- Rådgivning och informationsdelning - i samarbete med organisationer
- Upprätta och underhålla relationer med andra incidenthanterande organisationer
- Förvalta och vidareutveckla kontaktregister för alla anslutna organisationer

Teknikstöd som alla får tillgång till:

- MISP och generell informationsdelning från andra verktyg/källor
- RPZ med policybaserad blockering
- Sårbarhetsscanner

Allt ovan ingår i SUNET-anslutningen

SUNET SOC

Förmågor och utvecklingsarbeten

Hot och riskanalys

Sårbarhetsmonitorering och verifiering - > notifiering

Dela data mellan och om aktörer

Upptäcka intrång och intrångsförsök

Kunskapsspridning och best-practise

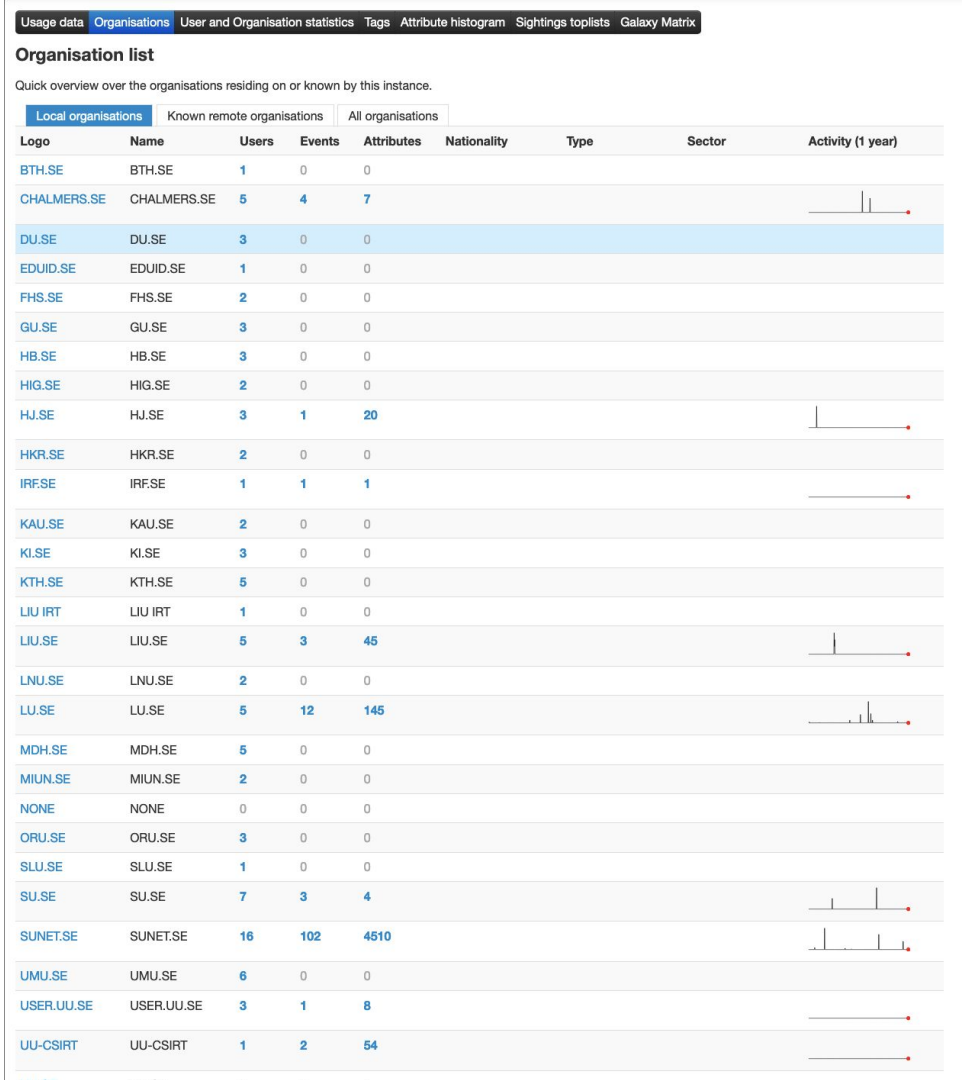
SUNET SOC

Informationsdelning

Tillhandahålla möjlighet för informationsutbyte

- Dela data om IOCs
- Tillhandahålla förädlade block-listor
- Threat feeds

MISP Threat Sharing



Logo	Name	Users	Events	Attributes	Nationality	Type	Sector	Activity (1 year)
BTH.SE	BTH.SE	1	0	0				
CHALMERS.SE	CHALMERS.SE	5	4	7				
DU.SE	DU.SE	3	0	0				
EDUID.SE	EDUID.SE	1	0	0				
FHS.SE	FHS.SE	2	0	0				
GU.SE	GU.SE	3	0	0				
HB.SE	HB.SE	3	0	0				
HIG.SE	HIG.SE	2	0	0				
HJ.SE	HJ.SE	3	1	20				
HKR.SE	HKR.SE	2	0	0				
IRF.SE	IRF.SE	1	1	1				
KAU.SE	KAU.SE	2	0	0				
KI.SE	KI.SE	3	0	0				
KTH.SE	KTH.SE	5	0	0				
LIU IRT	LIU IRT	1	0	0				
LIU.SE	LIU.SE	5	3	45				
LNU.SE	LNU.SE	2	0	0				
LU.SE	LU.SE	5	12	145				
MDH.SE	MDH.SE	5	0	0				
MIUN.SE	MIUN.SE	2	0	0				
NONE	NONE	0	0	0				
ORU.SE	ORU.SE	3	0	0				
SLU.SE	SLU.SE	1	0	0				
SU.SE	SU.SE	7	3	4				
SUNET.SE	SUNET.SE	16	102	4510				
UMU.SE	UMU.SE	6	0	0				
USER.UU.SE	USER.UU.SE	3	1	8				
UU-CSIRT	UU-CSIRT	1	2	54				

Proaktivt arbete

- ❑ Rådgivning
- ❑ Checklistor
- ❑ Teknisk sårbarhetsanalys
- ❑ Systemhärdning
- ❑ Blockeringsregler
- ❑ Skydd mot skadlig kod
- ❑ Penetrationstester
- ❑ Kodgranskning / Review

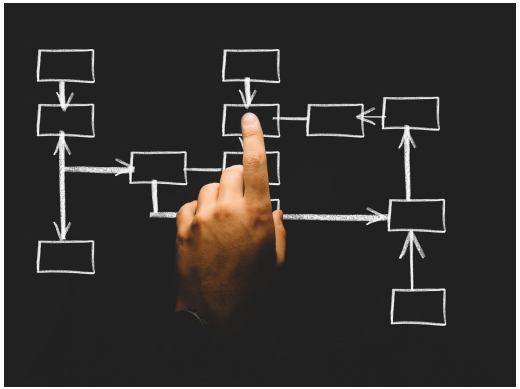
SUNET SOC

Analysarbete i nuet

- ❏ Passiv nätverksanalys
- ❏ Aktiv nätverksanalys
- ❏ Loggaggregering
- ❏ Informationsdelning
- ❏ Intrångsdetektering
- ❏ Visualisering
- ❏ Säkerhetskontroller
- ❏ Registrering/Eskalering

SUNET SOC

Händelsestyrda - Incidenthantering



- ❑ Incidenthantering
- ❑ Forensik
- ❑ Automation
- ❑ Malwareanalys
- ❑ Problemrapportering
- ❑ Ärendehantering
- ❑ Eskalering
- ❑ Rapportering / Lessons learned

SUNET SOC

Större investeringar (utöver personal och fasta utgifter)

2019	Sårbarhetsscanner - (Outscan)
2020	Lockbetesteknik - (Attivo Network)
2021	Intrång och anomalidetektering - (Vectra AI)
2022	Upptäcka nätverksbaserade intrång

Pågående utvärderingar/upphandlingar:

- Trafikaggregering, tap-data, ids-infra
- IDS - Suricata/Corelight m.fl.
- Samarbeten eller avtal kring Threat Feeds
- Loggservrar

SUNET SOC

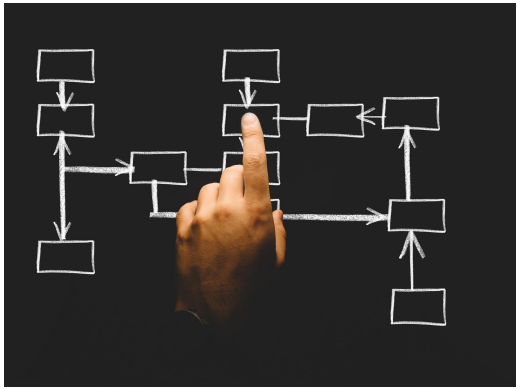
Öka samarbetet och informationsutbyten

- Verifiera och notifiera specifikt om aktuella lokala sårbarheter
- Trafikdataanalys WAN (metadata) gentemot IOC (C2, botnet, DDOS m.m.)
- Kompetensstöd vid incidenthantering

- Skapa ett avtal för “Uppdraget” - alltså att behandla och lagra IP-adresser/personuppgifter

SUNET SOC

Agenda Onsdag 20/10



1. SUNET Säkerhetscenter
   - 09:00 - 09:15 Välkomna: Intro, David
   - 09:15 - 09:25 Svarstidsmätning och annat?
   - 09:25 - 09:55 Aktuella sårbarheter, John
   - 10:00 - 10:45 phpshell, Christoffer Alström

2. DNSSEC m.m.
   - 13:00 - 13:45 DNSLabs @ Internetstiftelsen, Niklas Pousette och Ulrich Wisser, IIS
   - 14:00 - 14:30 Mätning av sektorn, Erik
   - 14:30 - 14:45 Plats för diskussion/frågor

3. Mailfilter
   - 15:00 - 15:45 Mailfilter-NG, Peter Falck, Halon

SUNET SOC

Ge oss feedback!

- Vad tyckte du om detta pass?
- Vad är ditt intryck av höstens Sunetdagar i sin helhet?
- Har du någon annan åsikt du vill dela med dig av?

Vi skickar länken i chatten!

https://sunet.artologik.net/sunet/sunetdagarnaHT21

SUNET

Kommande aktiviteter

Torsdag:

09:00 Öppet hus kring säkerhetsfrågor

13:00 CSIRT forum (för incidenthanterande kontaktpersoner inom SUNET)

2021-11-11 10:00 Webscanning med Detectify - Öppet webinar

FLER WORKSHOPS?

SUNET