NÄR KRISEN ÄR ETT FAKTUM- CYBERKRISHANTERING

SARAH BACKMAN

secana SECURITY

FÖRSTÅR VI VARANDRA?

FOKUS FÖR PRESENTATIONEN

- ~~Preventiva åtgärder –~~ reaktiva åtgärder
- ~~Tekniskt fokus –~~ management-fokus
- ~~Incidenthantering –~~ krishantering
- ~~Fokus på källan till attacken –~~ fokus på effekten av attacken
- ~~Fokus på enskilda beslutsfattare –~~ fokus på krishanterande grupper

secana SECURITY

DEFINITION AV KRIS

Kriser kännetecknas av

- Stora konsekvenser och kaskadeffekter
- Stor störning av ordinarie verksamhet
- Omständigheterna präglas av betydande turbulens
- Tidsbrist i beslutsfattande
- Osäkerhet i informationsunderlaget

Press på responsgrupper/beslutsfattare

DEFINITION AV CYBERKRIS?

Definition cyberincident

Förlust av konfidentialitet, riktighet och/eller tillgänglighet inom ICT

+

Karaktärsdrag Kris

- Stora konsekvenser och kaskadeffekter
- Stor störning av ordinarie verksamhet
- Omständigheterna präglas av betydande turbulens
- Tidsbrist
- Osäkerhet

=

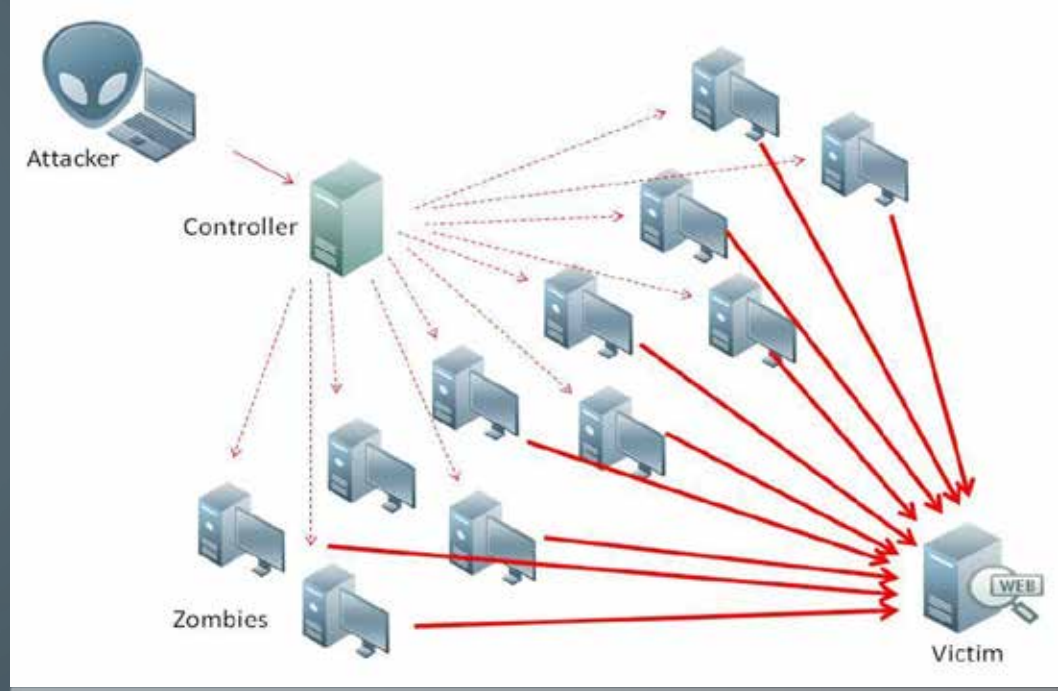
Cyberkris

secana SECURITY

FALL AV CYBERKRISER

ESTLAND 2007

- Ett av de fall som brukar refereras till som fall av ”cyber warfare”
- DDoS - attacker (distributed denial of service).
- Slog ut kritiska tjänster så som banktjänster och offentliga webbsidor, men även sajter tillhörande skolor och tidningar.
- Troligt att en statlig aktör låg bakom attacken.
- Troligt att attacken var politiskt motiverad.
- Attackerna var en av den första stora kampanjerna som riktade sig mot ett lands kritiska infrastruktur.

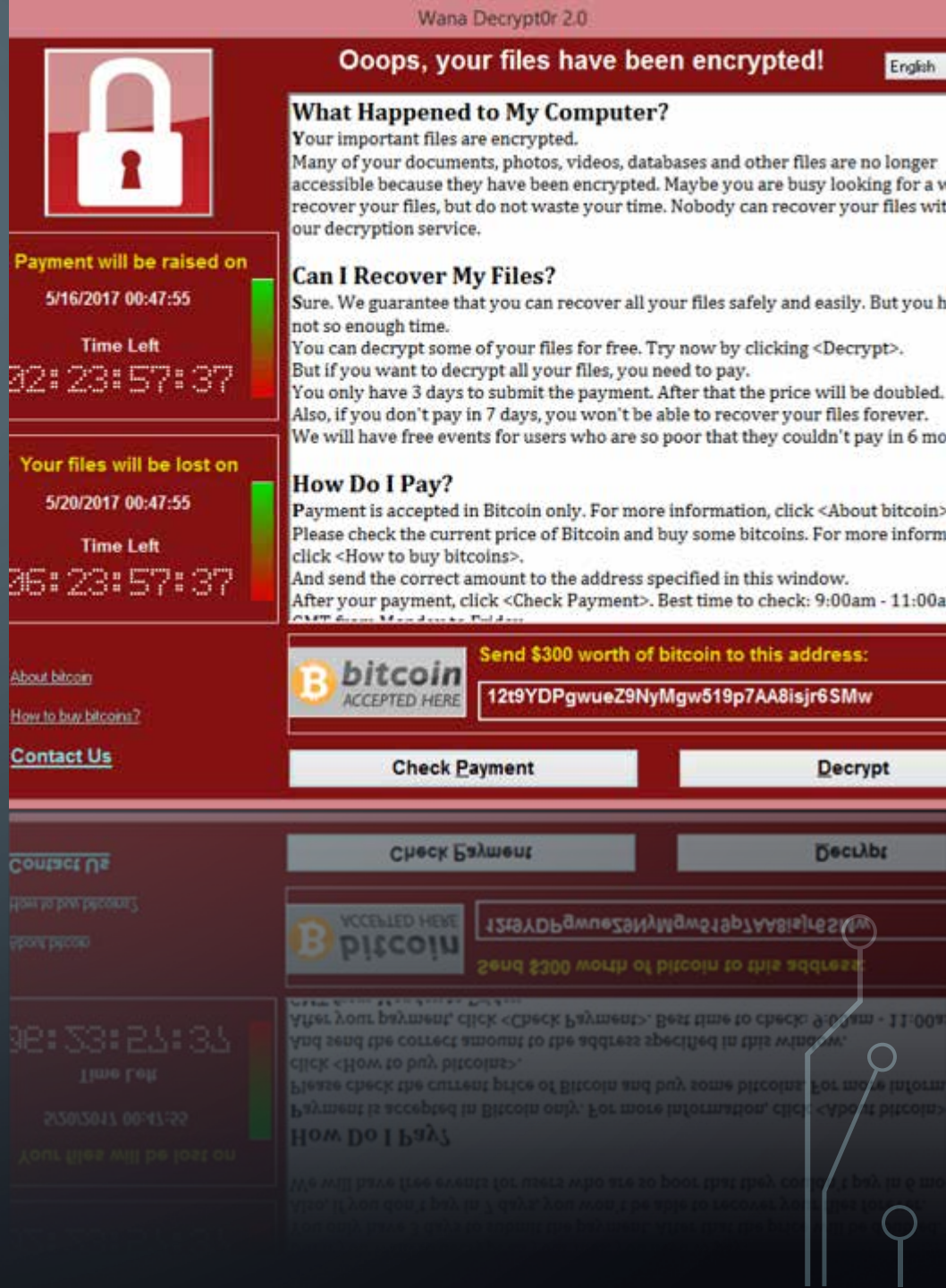


UKRAINA POWER GRID 2015

- Flera energidistruberings-företag i Ukraina blev hackade (via spear-phising).
- Ledde till strömavbrott hos flera hundra tusen människor i mellan 1-6 timmar.
- En av de första kända framgångsrika cyberattackerna på SCADA-system i ”power grids” (energidistribuering).
- Möjligt ”test av sårbarhet och respons” från statlig aktör.
- Energisektorn i Europa är mycket sammankopplad, likartad och beroendet av energi konstant = stor sårbarhet.

WANNACRY 2017

- Ett ransomwareprogram som inriktar sig mot datorer med operativsystemet Windows.
- Med hjälp av bland annat phising och maskar infekterade WannaCry över 230 000 datorer i 150 länder under 2017.
- Sjukhus och sjukvårdssektorn hårt drabbade, en sedan tidigare känd sårbar sektor.
- Största attacken av sitt slag någonsin.
- Hade varit lätt att förhindra genom basal cyberhygien.
- Troligt att vi kommer se mer av detta.



VAD HAR DESSA FALL GEMENSAMT?

- Visade att de samhällsfunktioner vi är mest beroende av är mycket sårbara för cyberattacker.
- Suddiga gränser (civilt/militärt, mellan sektorer, geografiska gränser och nivåer).
- Gränslöshet/snabb spridning/beroenden (uppkopplat ihopkopplat).
- Orsaken dåligt försvar (i form av undermålig cyberhygien) snarare än bra attack.
- Motivation till ökade preventiva åtgärder kommer först efter krisen, trots att varningarna, risk/hotbilder samt sårbarheter funnits där innan.

LEDARSKAP I CYBERKRISHANTERING

UPPGIFTER OCH UTMANINGAR

secana
SECURITY

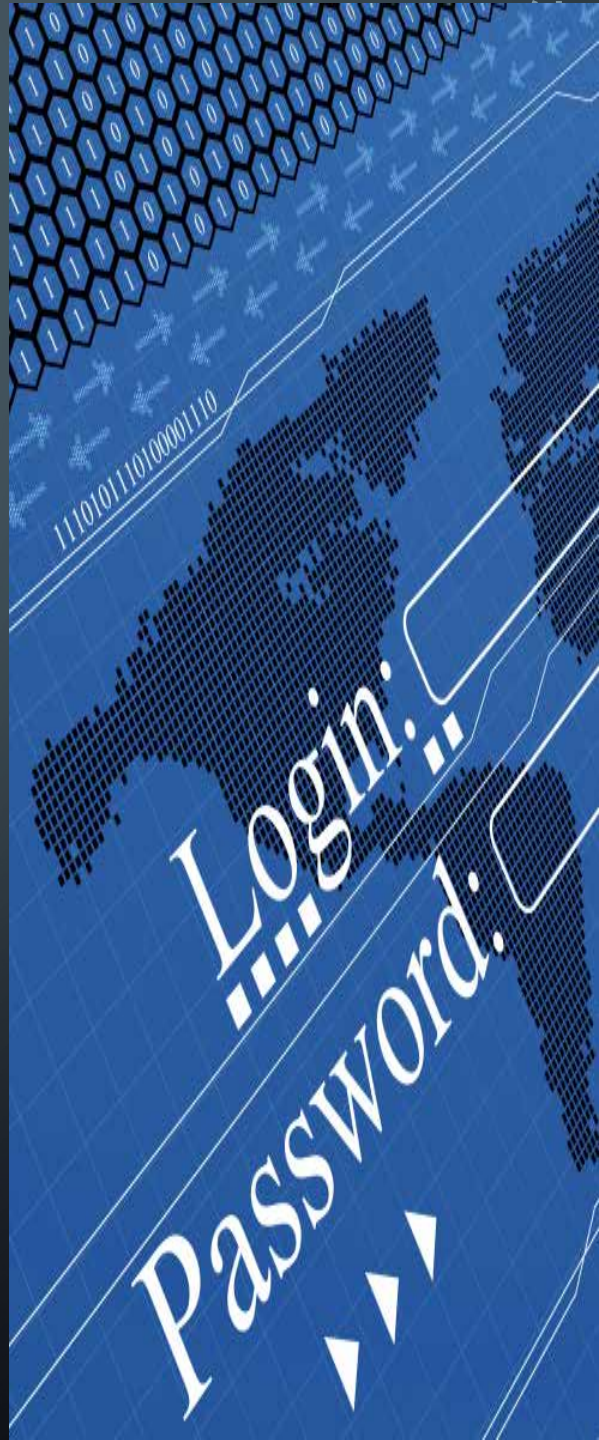
KRISHANTERINGSPROCESSEN

Prevention, Preparation, Response and Recovery (Comfort 2002)

(Boin, 't Hart, Stern & Sundelius 2005)

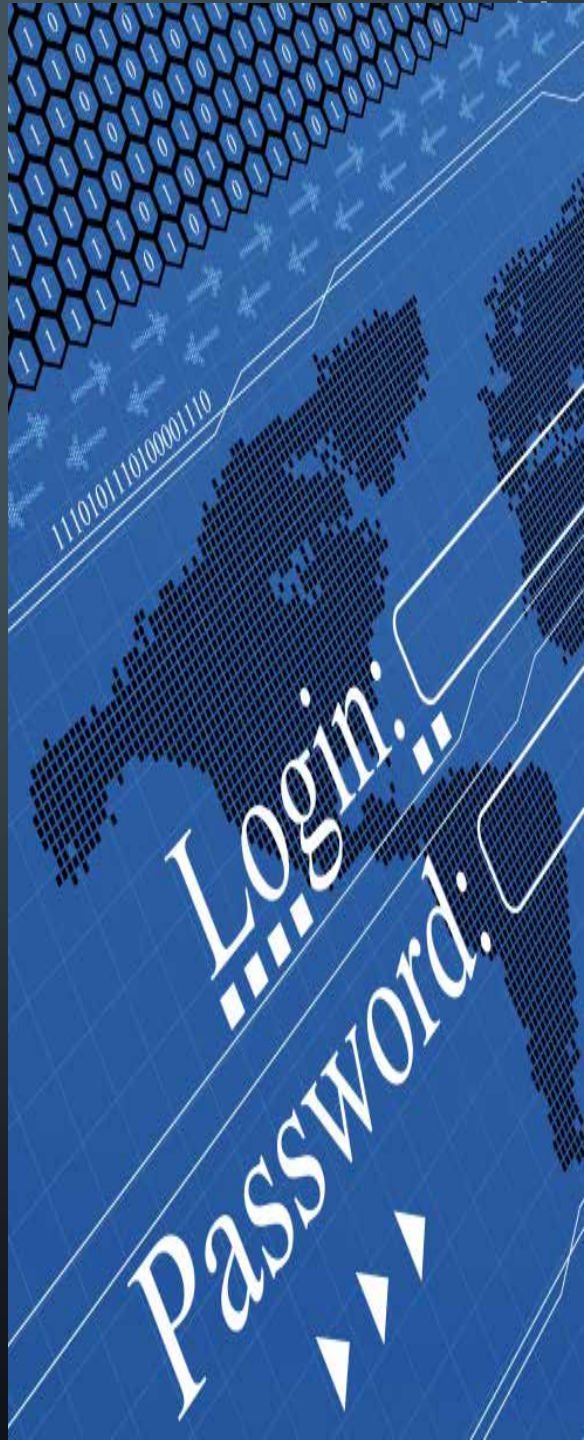
DETECTION & SENSE-MAKING

- Osäkerhet i rapportering av cyberincidenter som kan förvarna cyberkriser.
- Tillitsbrist förhindrar informationsdelning.
- Tekniskt språk och olika termer för samma fenomen skapar kommunikationssvårigheter.
- Extremt många involverade aktörer både horisontellt och vertikalt, ej nödvändigtvis vana att samarbeta.
- Brister gällande förståelse av cyberincidenters möjliga kaskadeffekter.



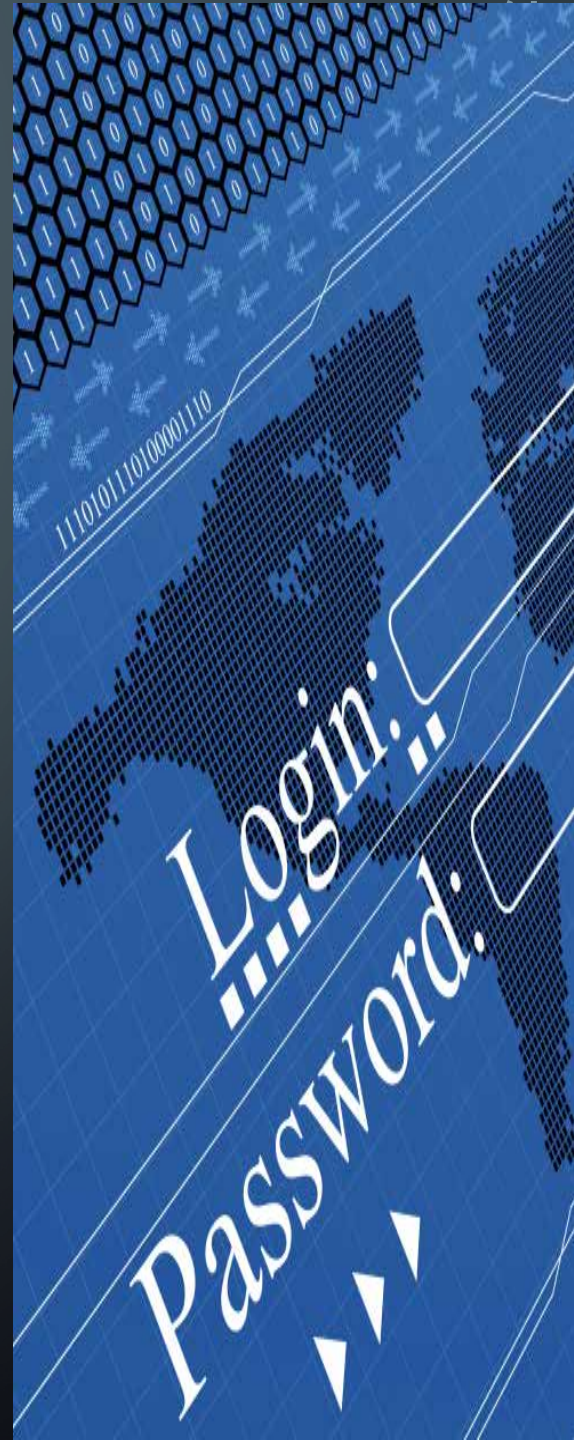
DECISION MAKING & COORDINATION I CYBERKRISER

- Beslutsunderlag kan ta längre tid än vanligt att få fram på grund av additionell komplexitet.
- Vem äger krisen, vem fattar besluten?
- Svårigheter för beslutsfattare att förstå de tekniska komponenterna av cyberkriser, även på mycket grundläggande nivå. Skapar stort beroende av rådgivare och experter för att kunna fatta beslut.
- Bristen på erfarenhet och gemensamma ramverk (SOP) gällande cyberkriser ett problem för beslutsfattare och responsgrupper.



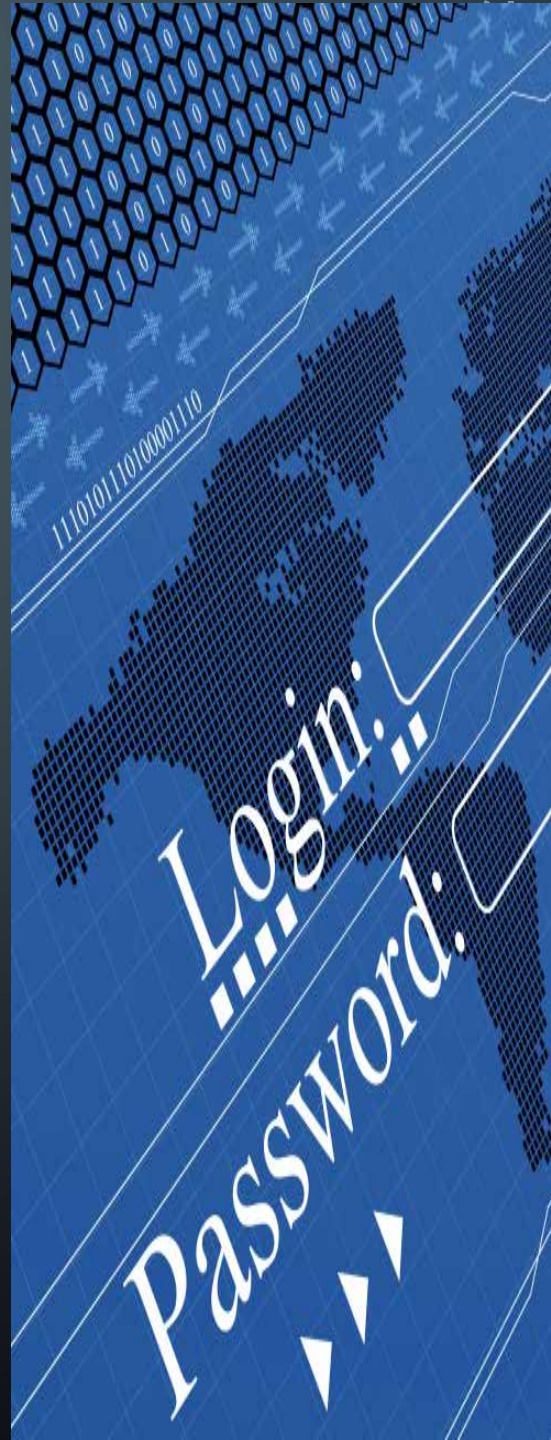
MEANING MAKING & COMMUNICATION CYBERKRISER

- Cyberkriser kan vara svåra att förklara och rama in.
- Vem komponerar ett gemensamt budskap?
- Om ordinarie kanaler för kriskommunikation är otillgängliga, hur når man ut?



ACCOUTABILITY & LEARNING CYBERKRISER

- Hur vet man att krisen är över? Sårbarheten kan finnas kvar. Krisen kan blossa upp igen.
- Vilka ska ställas till svars när många är inblandade i bristande förebyggande arbete och rutiner?
- Att analysera cyberattacker och efterföljande kriser kan vara utmanande (inte minst fastställandet om var attacken kommer ifrån, motivation till attacken och kritiska mänskliga och tekniska sårbarheter).
- Kriser kan utnyttjas och ”framas” i politiskt syfte.



FRÅN UTMANINGAR TILL ÖKAD KAPACITET

- Förståelse för att det inte är en fråga om OM utan NÄR en cyberkris inträffar
- Bättre preventivt arbete – det är värt det!
- Ökad medvetenhet & cyberhygien av största betydelse
- Ökat engagemang från ledningar (top-down approach)
- Ökad övningsverksamhet
- Mer forskning på management- och samverkansaspekter av cybersäkerhet och cyberkrishantering
- Bättre strukturer både nationellt och internationellt för samverkan, förtroendeskapande, informationsdelning och lägesbildsskapande mellan responsgrupper och andra involverade aktörer

FRÅGOR?

KONTAKT: SARAH.BACKMAN@SECANA.SE