

Nationellt it-brottscentrum

Polisens satsning mot it-brottslighet



IT-brott – inom Polismyndigheten

Nationellt it-brottscentrum

IT-brott

Sexuella övergrepp mot barn - internetbaserade

Nationellt bedrägericentrum

Bedrägerier

dataintrång som en del av brott mot person



Nationellt IT-brottscentrum

Swedish Cybercrime Center – SC³

- Utöva processansvar för myndighetens arbete mot komplex it-brottslighet
 - Uppnå enhetlighet för svensk polis genom att sätta förmåga på nationell, regional, och lokal nivå
- Expertfunktion för handläggning av komplexa it-brottsärenden
- Hantera hot och utredningar rörande kritisk infrastruktur
- Ansvara för kontakterna med (inkl. hantering och samordning av underrättelser) European Cybercrime Center (EC³) vid Europol
- Nationell deskfunktion för IT-relaterad brottslighet

Utredningsverksamhet vid SC³

Egna utredningar

Utredningsstöd åt polisregionerna

Internationella rättshjälpsbegäran

Komplex it-brottslighet

Sexuella övergrepp mot barn

Underrättelseverksamhet vid SC³

Förebygga

Förhindra

Upptäcka

- bygga kunskap om kriminella aktörer
 - göra bedömningar av brottsliga fenomen
 - lägesfölja utvecklingen
-
- skapa underlag för inledning av förundersökning

Komplex it-brottslighet

Sexuella övergrepp mot barn (internetbaserade)

Övrig verksamhet vid SC³

Internetinhämtning (ex. öppna källor)

IT-forensik

SPoC för vissa tjänsteleverantörer (ex. sociala medier)

Intern och extern kommunikation för ämnesområdet (ex. mediekontakter)

Samverkan med nationella och internationella partners

Metod- och teknikutveckling

Strategisk arbete avseende it-brott/it-relaterad brottslighet

Utbildningsinsatser

LÄGESBILD





The Internet Organised Crime
Threat Assessment (IOCTA)

2015



■ IOCTA 2016

INTERNET ORGANISED
CRIME THREAT ASSESSMENT



Polisen

<https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2016/>

Key findings – iOCTA 2016

- cryptoware är det allra största hotet
 - skadlig kod för mobiltelefoner ökar i antal & skadeverkan
 - omfattande kartläggning före riktade phishing-attacker
 - VD-bedrägerier (CEO fraud) / Business Email Compromise (BEC)
 - Stresser-/bootertjänster -> ökat antal DDoS-attacker
-
- Bitcoins standard som betalningsmedel
 - kommunikation via krypterade kanaler, såsom Jabber
-
- samverkan med privata sektorn måste öka
 - internationell samverkan är en nyckel till framgång
 - myndigheter bör lägga fokus på möjliggörare
 - specialiserade enheter såväl som kompetenshöjning generellt

Ransomware



Vad?

- skadlig kod som hindrar tillgång till hela eller delar av datorn
- kräver lösensumma för upplåsning
- en stor mängd varianter
- vissa krypterar informationen (Cryptoware)

Hur?

- bilagor eller länkar i e-post
- komprometterade webbsidor
- via annan skadlig kod



Polisen Polisen Enheten för databrott



Datorn är låst



All aktivitet på den här datorn har registrerats



Pressbyrån - Nu Ukash kuponger kan köpas på mer än 300 kiosker i butiksnetet «Pressbyrån» runt om hela Sverige.

7-Eleven - Ukash kuponger kan köpas på mer än 200 butiker «7-Eleven», som ligger på bensinstationer Shell.

Payzone - Ukash kuponger kan köpas vid terminaler «Payzone» runt om hela Sverige.

Datorn har blockerats

Din dator har blockerats av ett system för automatisk information kontroll. Varför?

Detta skulle kunna bero på en av följande skäl:

1. Datorn har använts för förbjudna webbsiter
2. Datorn har använts för webbsiter som innehåller barnpornografi
3. Datorn har använts för överförning av förbjuden information
4. Datorn har använts för att förvara/visa piratkopierat innehåll

Hur åtgärdar jag detta?

Enligt lag, om Information kontroll och skydd av information' från den 2012/01/02 skyldig måste betala böter på 100 euro. För att underlätta betalning av böterna, erbjuder vi en säker form av utbetalning med hjälp av Ukash kuponger. Allt du behöver är att köpa en voucher (ar) för totalt 100 euro, och skriva dem i formen för avbetalning, sedan klicka på 'Skicka koden'.

Vad händer när jag skickat koden?

När koden har verifierats av vårt system din dator kommer omedelbart upp. Om du anger två kodar för € 50, då måste du först ange en kod, efter att ha fått bekräftelse -nästa.

Vad händer om jag har problem?

Om du av någon anledning inte kan betala böterna via en säker form av betalning, måste du skriva ett brev via e-post info@online-cyber-police.com och ange i brevet din adress och IP-numret (er) kupongen (ar) Ukash i mängden 100 euro. När koden har verifierats av vårt system din dator kommer omedelbart upp.



Var kan jag köpa Ukash?



Du kan köpa Ukash kuponger i tusentals platser runt globen, online, med hjälp av online börsen, i olika kiosker och bankomater.



SVERIGES DOMSTOLAR

Gå till [domstol webbplats](#) (länken öppnas i nytt fönster) för ytterligare information om ditt rättsfall.

För att bekräfta för domstolen att du har fått kallelsen till rättegången, ska du skriva under och skicka in det svarsbrev som följer med kallelsen. På domstolen kallas detta delgivning. Det är i många fall nödvändigt att du som tilltalad närvarar personligen vid rättegången. Om du inte kan komma, ska du alltid kontakta domstolen. Det är viktigt att du kommer i rätt tid och till rätt plats, eftersom en rättegång kostar samhället stora pengar. Om du inte kommer kan rättegången få ställas in. Detta innebär dock inte att den inte blir av, utan du och alla andra berörda blir kallade vid ett nytt tillfälle. Du kan bli skyldig att betala vite, bli hämtad av polisen eller i vissa fall häktas om du inte kommer. Du kan dessutom få betala kostnader för andra som kommit till domstolen. Den kallelse du fått gäller om inte domstolen meddelar annat. Ta gärna med dig kallelsen till domstolen.

[Gå till domstol webbplats](#)

Sveriges Domstolar använder Google Analytics som webbanalysverktyg på webbplatsen. Verkttyget använder i sin tur cookies för insamlandet av data. Den data som samlas in är anonym och används i syfte att förbättra webbplatsen och för att ge en bra användarupplevelse.



Polisen



FAKTURA

General Memory Storage Networking Console Performance Snapshots Search

DVD Drive 1: <empty>

Eject

Switch to Remote Desktop

http://pj6s.teliabills.com/g9fv.php?id=dGFhQG1ycnluY29t



DNS leak test Login



Handla Support Kontakta oss



Sök



Tjänster



Mitt Telia

Privat

Telia.se > Privat

För att ladda ner information om din faktura ber vi dig ange numret som visas i bilden nedan:

061549

Ladda ner faktura

vara kunder.

© Telia 556430-0142 Box 50077, 973 22 Luleå Säte: Stockholm



Polisen

Överbelastningsattacker



Polisen

Olika typer av aktörer

- unga "gamers"
- ideologiskt motiverade
- ekonomiskt motiverade yrkeskriminella
- statsaktörer

Trender

- utpressning
- billiga tjänster till salu (Crime-as-a-Service)



DDoS - utpressning



“

Subject: DDoS

Hello!

All your servers are going under attack unless you pay 2 Bitcoin.

Pay to [BITCOIN]

Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 200-300 Gbps.

Right now we are running small demonstrative attack on 1 of your IPs: [REMOVED]

Don't worry, it will not be hard, since we do not want to crash your server at this moment, and will stop in 60 minutes. It's just to prove that we are serious.

We are aware that you probably don't have 2 BTC at the moment, so we are giving you 24 hours to get BTC and pay us...

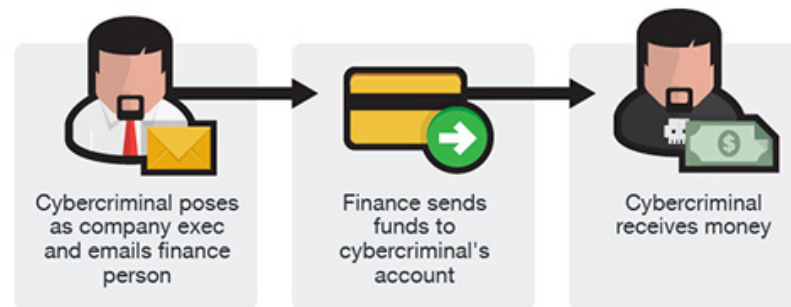
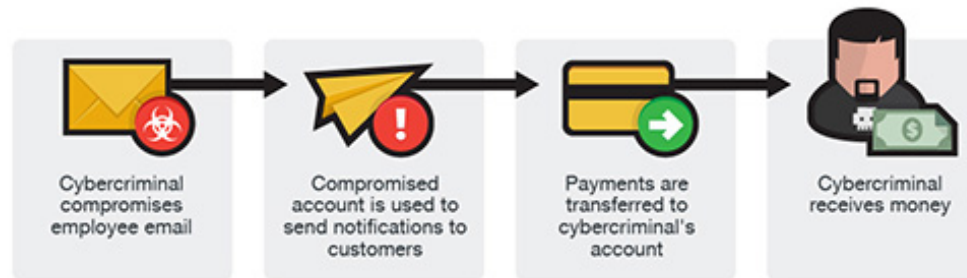


Polisen

Our Pricing

1 Month Basic	Bronze Lifetime	Gold Lifetime	Green Lifetime	Business Lifetime
5.00€ /month	22.00€ Lifetime	50.00€ Lifetime	60.00€ Lifetime	90.00€ lifetime
1 Concurrent + 300 seconds boot time 125Gbps total network capacity	1 Concurrent + 600 seconds boot time 125Gbps total network capacity	1 Concurrent + 1200 seconds boot time 125Gbps total network capacity	1 Concurrent + 1800 seconds boot time 125Gbps total network capacity	1 Concurrent + 3600 seconds boot time 125Gbps total network capacity
Resolvers & Tools 24/7 Dedicated Support	Resolvers & Tools 24/7 Dedicated Support	Resolvers & Tools 24/7 Dedicated Support	Resolvers & Tools 24/7 Dedicated Support	Resolvers & Tools 24/7 Dedicated Support

Business Email Compromise



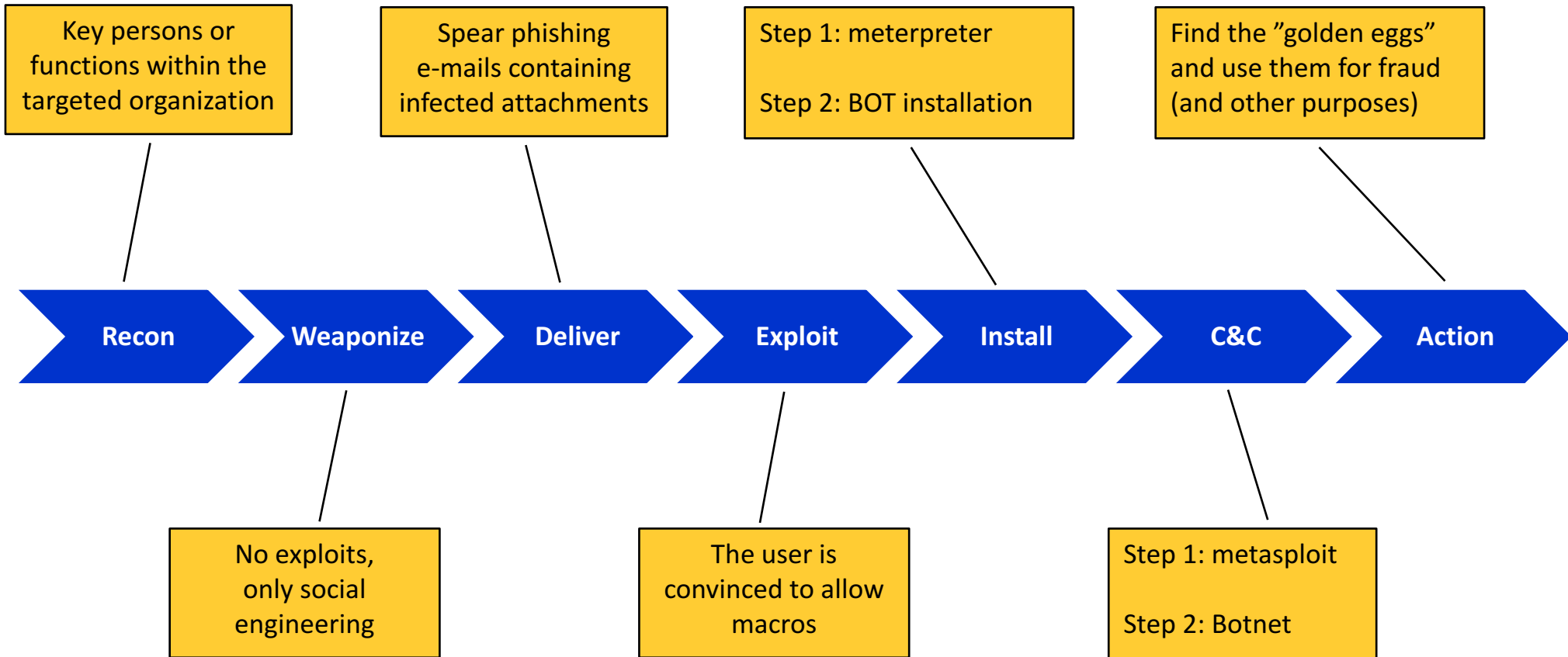
Vad?

- infekterar en organisations e-postsystem
- tar över befintliga konton eller skapar nya
- skickar bedräglig e-post i organisationens namn

Hur?

- bilagor eller länkar i e-post
- social engineering

Case study



Hot/attacker mot kritisk IT-infrastruktur



Kritisk infrastruktur (IT)

”de gemensamma it-resurser hos en samhällsviktig verksamhet som är nödvändiga för att upprätthålla verksamhetens förmåga och kontinuitet”

Definition

En samhällsviktig verksamhet definieras som
en samhällsfunktion av sådan betydelse att ett bortfall av eller en svår störning i funktionen skulle innebära stor risk eller fara för befolkningens liv och hälsa, samhällets funktionalitet eller samhällets grundläggande värden.

Kritisk infrastruktur i praktiken - exempel

Betalningssystem

Distribution av elektricitet

Sjukvård

Telefoni & radiokommunikation

Trafik (väg, sjö, luft, spårbunden)

Vattenförsörjning

Viktig information till allmänheten



Exempel på incidenter

Elförsörjning

strömavbrott Gotland (40 000 abonnenter) - 14 februari 2015

brand i ställverk Borlänge (100 000 abonnenter) – 9 augusti

Mobilnät (Tele2, Telia, Telenor)

avbrott 3G/4G – mars 2015

Spårbunden trafik

omfattande växelfel – 27 april

SOS Alarm

störning i kommunikation med räddningstjänst och ambulans – 19 maj

Luftfartsverket

solstorm – 4 november 2015

kommunikationsproblem – 19 maj

tekniska problem – 30 maj

Världen

Tyskt stålverk utslaget av hackare – masugn förstörd

PUBLICISRAID 2014-12-21



Varför är samhället sårbart?

Väl utbyggd it-infrastruktur

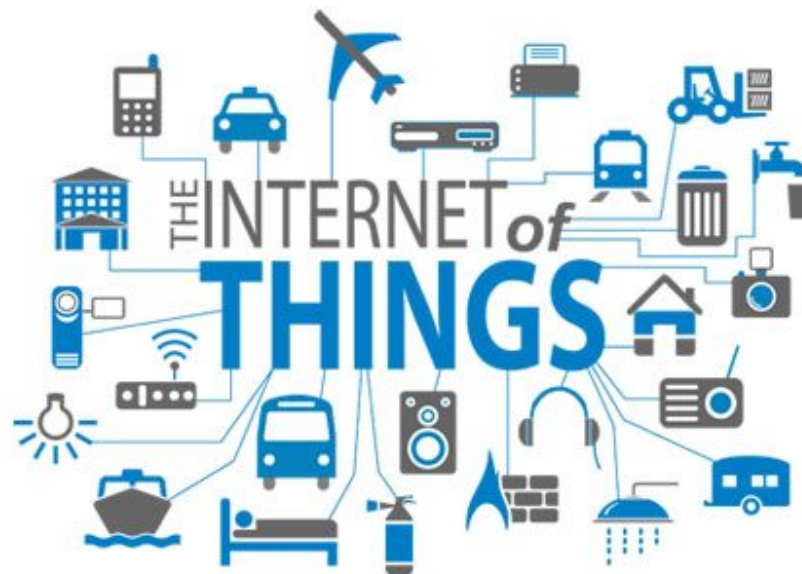
Hög uppkopplingsgrad

Hög tilltro till information

Hög tilltro till människor

Outsourcad skyddsvärd data

Personlig information hos olika tjänsteleverantörer



Exempel – hackade användardatabaser

MySpace – 2008

360 miljoner användaruppgifter

Dropbox - 2012

68 miljoner användaruppgifter

LinkedIn - 2012

6,5 miljoner användaruppgifter

Adobe - 2013

153 miljoner användaruppgifter (minst 400 000 svenska)

eBay + Gmail - 2014

5 miljoner användaruppgifter

Ashley Madison – 2015

30 miljoner användaruppgifter

Flashback Forum – 2015

40 000 användaruppgifter



Exempel – Utredningar

Hackerattacken mot Telia slog ut 112

Publicerad 13 dec 2014 kl 06.19



Rekommendera

0



Tweeta



Dela



Mejla

Sveriges största teleoperatör Telia har attackerats igen.

Myndigheten Post- och telestyrelsen har kallat till krismöte efter en rapport från Telia där det framgår att kunder inte kunnat nå larmnumret 112 under attackerna.



Polisen

[Aktuellt](#)[Service](#)[Utsatt för brott](#)[Lagar och regler](#)[Om polisen](#)[Kontakt](#)Du är här: / [Aktuellt](#) / Nyheter**Aktuellt**[Händelser](#)**Nyheter**[Nyheter hela landet](#)[Tillfällig gräs- och id-kontroll](#)[Pressmeddelanden](#)[Tipsa och hjälp polisen](#)[Lediga jobb](#)[Sociala medier](#)[Publikationer](#)[Aktuella upphandlingar](#)[Kungörelser](#)

En gripen efter attacker mot Swedbank och Nordea

En person greps i går, onsdag, i samband med en husrannsakan och är nu misstänkt för ett flertal ddos-attacker mot Swedbank och Nordea. "Jag bedömer att det är fråga om systemhotande brottslighet", säger förundersökningsledaren Mats Ljungqvist.

Under oktober har ett flertal ddos-attacker genomförts mot Swedbank och Nordea. Under onsdagen har en husrannsakan genomförts i Växjö av Nationellt It-brottscentrum i samverkan med nationella utredningsenheten vid Nationella operativa avdelningen samt lokala resurser i region Syd. En person som har varit anhållen in sin utevaro greps i samband med husrannsakan. Ett flertal beslag har gjorts.

Kammaråklagare Mats Ljungqvist vid Internationella åklagarkammaren i Stockholm är förundersökningsledare.

– Den gripne personen är misstänkt för grovt dataintrång samt försök till utpressning. Jag bedömer att det är fråga om systemhotande brottslighet, säger han.

[Hem](#) » [Driftmeddelande](#) » Driftstörning Sverige

2016-03-19

Driftstörning Sverige

IP-Only NOC informs about a current network disturbance event:

All times are presented in CET

Event start date/time: 2016-03-19 19:30

Current ETR: Not determined

Affected geographical area: Sweden

Cause of disturbance: DDoS-Attack





DDOS-ATTACK MOT SVENSK MEDIA

20-03-2016

Lördag den 19 mars omkring kl 19:30 drabbades ett antal tidningssiter i Sverige av en välregisserad DDoS-attack. Några av företagen har Basefarm som driftleverantör. DDoS-attacken var av oerhörd dignitet och kom från servrar över hela världen. Vårt säkerhetsteam hanterade situationen i enlighet med alla våra inarbetade rutiner och processer. Vi samarbetade med våra internationella partners för att stoppa angreppet



Lizard Squad

@LizardLands

In the event of suspension, check lizardsquad.org for updates. Lizard Squad forever. Jabber: nympho@riseup.net

TWEETS
76

FÖLJER
23

FÖLJARE
98,6 tn

GILLADE
39

Tweets

Tweets & svar

Foton & videoklipp



Lizard Squad @LizardLands · 1 tim

Hello to the Swedish Media



13



53



Lizard Squad Retweetade



Crusher Joe @kizadnaga · 15 min

Visa alla



Polisen

| Sverige

Attack mot Skolverkets server

UPPDATERAD 2015-01-28 PUBLICERAD 2015-01-28

En större virusattack slog nyligen ut en server på Skolverket som innehöll 20 miljoner interna dokument. Under nästan en veckas tid kunde myndighetens medarbetare inte komma åt sina filer.

Landstinget utsatt för cyberattack

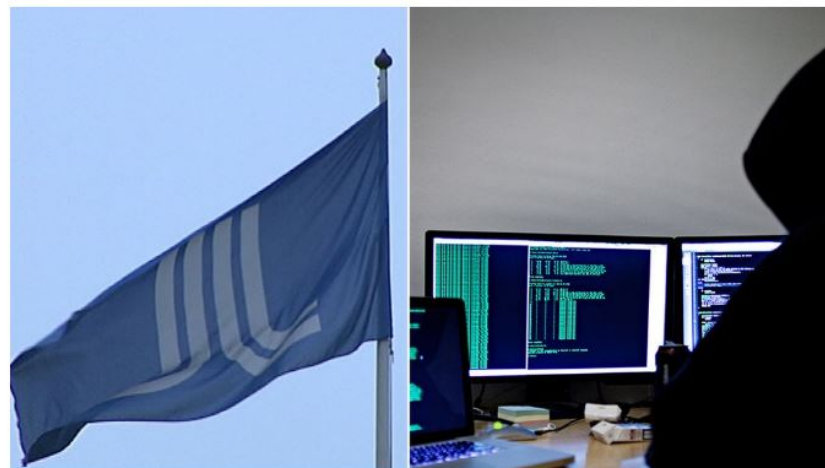


Foto: SVT / Thomas Winje Øijord/TT

I mars drabbades Stockholms läns landsting av en cyberattack. Någon eller några lyckades med hjälp av ett så kallat ransomware, eller utpressningstrojan, att kryptera en del av landstingets filer.



Polisen

Obligatorisk it-incidentrapportering



CERT SE



Polisen



Polisen

Rapportera brott

Polisanmäl skyndsamt vid konkret brott



Ring 114 14 eller besök polisen

För att anmäla ett brott kan du ringa [114 14](tel:11414) eller besöka en [polisstation](#).



Anmäl brott via internet

Du kan anmäla: inbrott, kontokortsbedrägeri, stöld och förlust (inte pass eller nationellt id-kort). **Har du skyddad identitet ska du inte anmäla brott via internet.**

Kontakta Nationellt it-brottscentrum

Tips och information

Frågor

Desken Nationellt it-brottscentrum

itbrott.desk.noa@polisen.se

010-56 417 30