
elastx
Public Cloud
made in Sweden

Open infra forum

Tekniska & ”Juridiska” frågor och extern påverkan av CSP

elastx

Hello!
I’m Richard

Richard W, Grundare och VD Ancautus AB
CISSP, GISP, TSCM Btec lvl 3 (plus andra, MCP, MCSE, etc.)

Info/IT-säkerhet (”cybersäk”) +20 år,
TSU/TSCM +8 år,
Inom IT (professionellt) sedan 1993

contact@ancautus.se
https://www.ancautus.se/

Ancautus

elastx

”Allmänt kända” problem i leveranskedjor och beroenden

Förtroendeproblem (tillverkning, handel, leverans)
Livslängd/uppdateringar/support
Tredjeparts leverantörer och tjänster
Förfalskning av produkter/komponenter
”Legacy” hårdvara/mjukvara/protokoll
M.m.

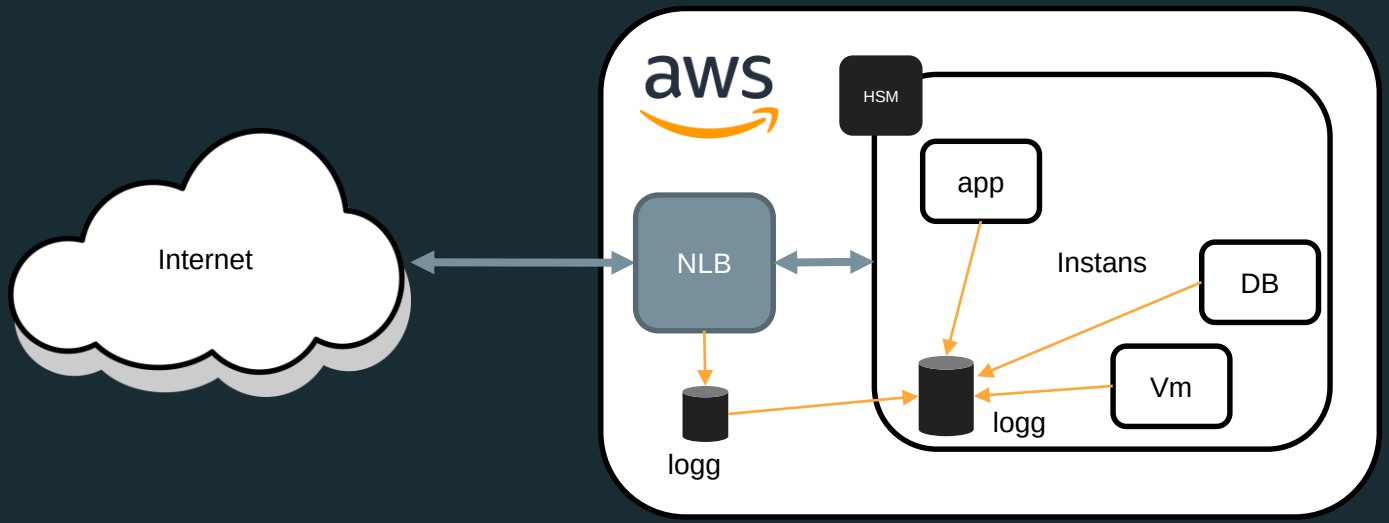
På väg ut i molnet?

- Strategi
- Teknik/säkerhet
- Processer
- Juridik

Beroendekedjor…
Extern påverkan på företag (informationsinhämtning)

Exempel AWS

Vem ”äger” informationen?
Vem tar sig rätten till informationen?



Men ärligt… delas information?

JA!

Varning! Statistik!

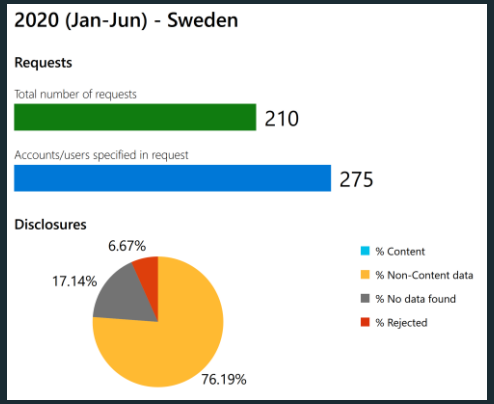
AWS Law enforcement & FISA requests

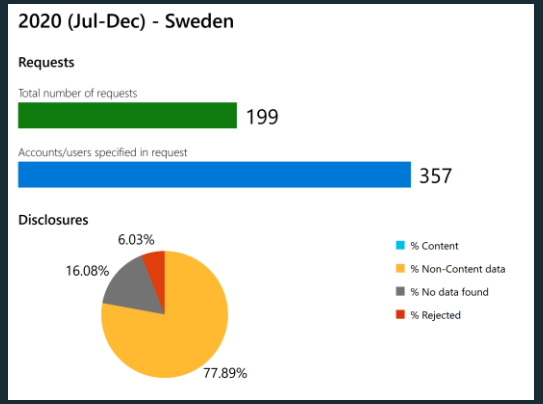
January 1, 2019, through June 30, 2019 (AWS only)	
Subpoenas:	216
Full response:	149
Partial response:	18
No response:	49
Search warrants:	31
Full response:	19
Partial response:	7
No response:	5
Other court orders:	23
Full response:	10
Partial response:	3
No response:	10
National security requests:	0-249
Non-U.S. requests:	8
Full response:	1
Partial response:	0
No response:	7

January 1, 2020, through June 30, 2020 (AWS only)	
Subpoenas:	269
Full response:	46
Partial response:	146
No response:	77
Search warrants:	37
Full response:	8
Partial response:	23
No response:	6
Other court orders:	38
Full response:	13
Partial response:	15
No response:	10
National security requests:	0-249
Non-U.S. requests:	18
Full response:	3
Partial response:	5
No response:	10

Källa 1: https://d1.awsstatic.com/certifications/Information_Request_Report_June_2019.pdf
Källa 2: https://d1.awsstatic.com/certifications/Information_Request_Report_June_2020.pdf

Microsoft, Law enforcement & FISA requests





Foreign Intelligence Surveillance Act (FISA) Orders

Reporting period	Orders seeking disclosure of content	Accounts impacted by orders seeking content	Orders seeking disclosure of only non-content	Accounts impacted by non-content orders
Jan - June 2020	0 - 499	14,000 - 14,499	0 - 499	0 - 499
July - Dec 2019	0 - 499	14,500 - 14,999	0 - 499	0 - 499
Jan - June 2019	0 - 499	14,000 - 14,499	0 - 499	0 - 499
July - Dec 2018	0 - 499	13,500 - 13,999	0 - 499	0 - 499
Jan - June 2018	0 - 499	13,000 - 13,499	0 - 499	0 - 499

Källa 1: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report
Källa 2: https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report?activetab=pivot_1%3aprimaryr2

Google, FISA requests

A FISA request can include a demand for a user's content, such as Gmail messages, documents, photos, and videos.

Reporting period	Number of requests	Number of accounts
Jan 2020 – Jun 2020	Data subject to six month reporting delay	
Jul 2019 – Dec 2019	0 – 499	74500 – 74999
Jan 2019 – Jun 2019	0 – 499	69500 – 69999
Jul 2018 – Dec 2018	500 – 999	63000 – 63499
Jan 2018 – Jun 2018	500 – 999	54500 – 54999
Jul 2017 – Dec 2017	500 – 999	44000 – 44499
Jan 2017 – Jun 2017	500 – 999	35000 – 35499

Källa 1: https://transparencyreport.google.com/user-data/us-national-security

Apple, Sverige req

Privacy

Government Requests January - June 2020

Requests Received

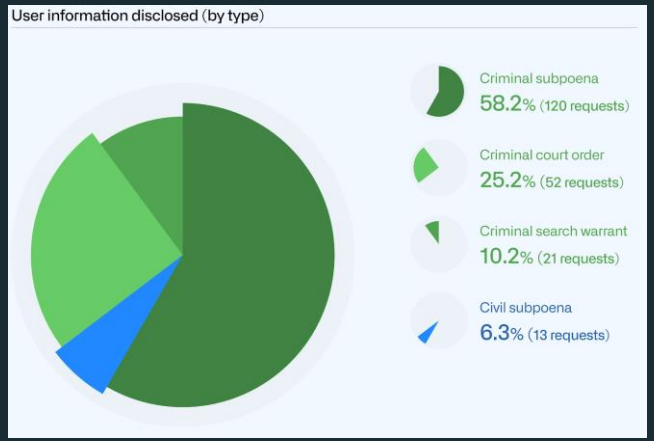
180	9	77	0
Device	Financial Identifier	Account	Emergency

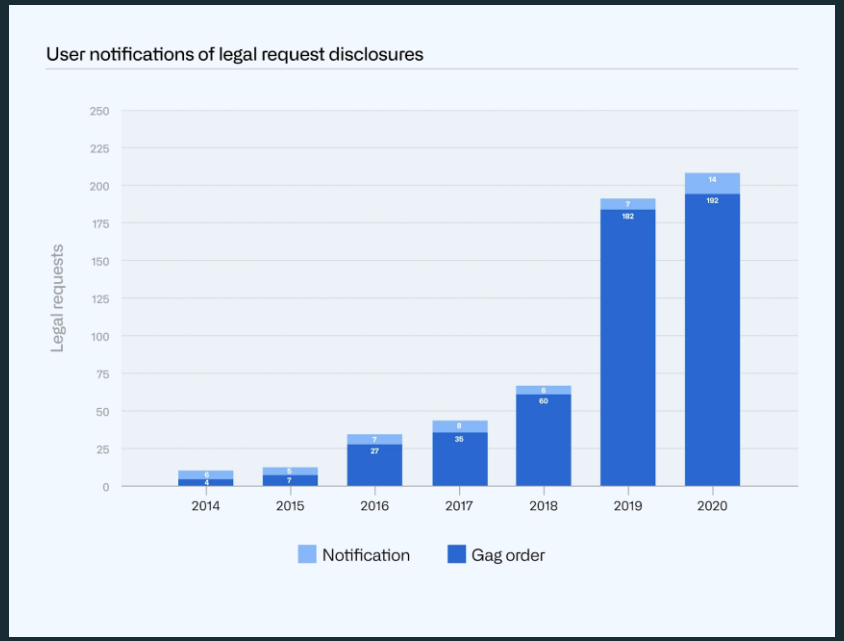
Requests for Customer Data

Request Type ⊕	Requests Received ⊕	Identifiers Specified in Requests ⊕	Requests where Data Provided ⊕	Percentage of Requests where Data Provided ⊕
Device	180	4,889	168	93%
Financial Identifier	9	10	6	67%
Account	77	116	67	87%
Emergency	0	-	0	-

Källa: https://www.apple.com/legal/transparency/se.html

GitHub req





Källa: https://github.blog/2021-02-25-2020-transparency-report

Slack req

Reporting Period	Type of request	Number of requests	Content data and non-content data disclosed	Only non-content data disclosed
United States				
January 1 - December 31, 2020	Search Warrants	10	10	0
	Court Orders	10	0	8
	Subpoenas	18	0	14
	National Security Requests	0	0	0
Non-US Entities				
	Foreign requests pursuant to MLAT	0	0	0

Men…
Vilka leverantörer nyttjar Slack då?

Källa: https://slack.com/intl/en-se/trust/data-request/transparency-report

Extern påverkan på företag

- FISA Act

  Foreign **I**ntelligence **S**urveillance **A**ct of 1978
- USA Patriot Act

  Uniting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism **Act**
- USA Freedom Act

  Uniting and **S**trengthening **A**merica by **F**ulfilling **R**ights and **E**nsuring **E**ffective **D**iscipline **O**ver **M**onitoring Act of 2015
- Cloud Act

  Clarifying **L**awful **O**verseas **U**se of **D**ata **Act**

FISA,

informationsinhämtning

- Omfattar & reglerar fysiskt och elektroniskt underrättelsearbete riktat mot "främmande makter" inklusive ”agenter.”

Lagen innan justeringar/tillägg av Patriot Act, Protect America Act, FISA Amendmends Act och Freedom Act omfattade först enbart underrättelseverksamhet inom USA, inklusive ”agenter” då det riktas mot amerikanska medborgare.

FISA ursprungliga syfte var att låta domstolar och kongressen få ökad insikt i USA:s hemliga underrättelsearbete.

Källa: https://www.govinfo.gov/content/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf

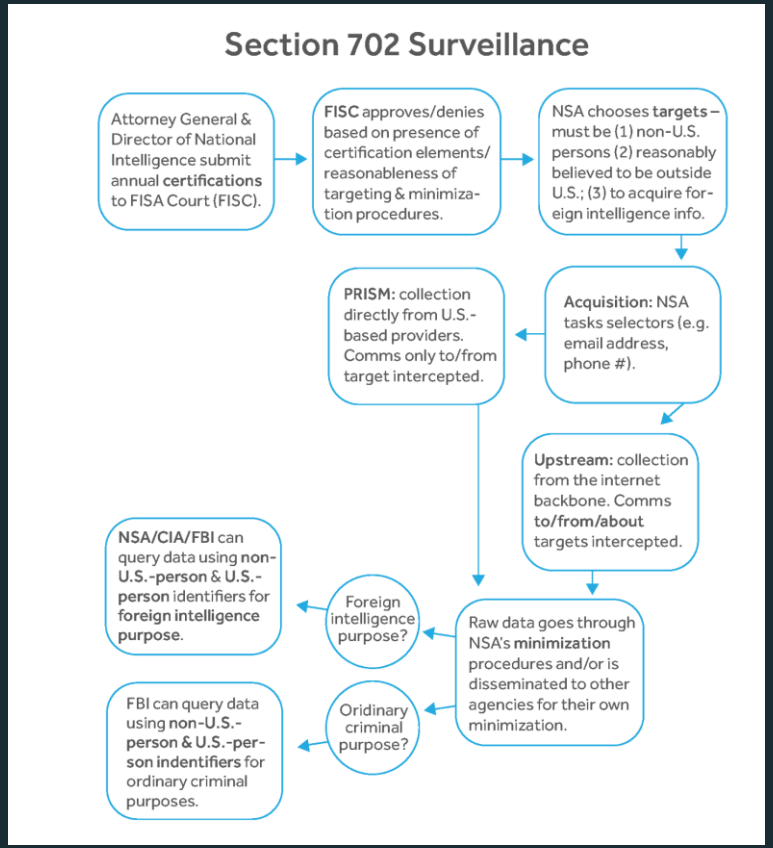
FISA 702

Section 702 of the Foreign Intelligence Surveillance Act (FISA) is a statute that authorizes the:
- collection, use, and dissemination of electronic communications content stored by U.S. internet service providers (such as Google, Facebook, and Microsoft),

or traveling across the internet's "backbone" (with the compelled assistance of U.S. telecom providers such as AT&T and Verizon).

FISA 702

Section 702 does not require that the surveillance target be a suspected terrorist, spy, or other agent of a foreign power.
Section 702 only requires that the targets **be non-U.S. persons located abroad**, and that a **"significant purpose"** of the surveillance be to obtain **"foreign intelligence information"** (the primary purpose of the surveillance can be something else entirely).



Cloud act,

Brottsbekämpning

“To amend title 18, United States Code, to improve law enforcement access to data stored across borders, and for other purposes.”

”…electronic communication service (ECS) or remote computing service (RCS) provider must comply with existing requirements to preserve, backup, or disclose the contents of an electronic communication or noncontent records or information pertaining to a customer or subscriber, regardless of whether the communication or record is located within or outside the United States. ”

“In response to an order from a foreign government with which the United States has an executive agreement on data access, an ECS or RCS provider may:

- intercept or disclose the contents of an electronic communication, and
- disclose the contents of a stored electronic communication or noncontent records or information pertaining to a subscriber or customer. ”

Källa: https://www.congress.gov/bill/115th-congress/house-bill/4943

Dags nu att jämföra…

Lagar att känna till

- Cybersäkerhetslagen
- NIL
- DSL
- PIPL

National Intelligence Law (“NIL”),

Bl.a Informationsinhämtning

- NIL gäller globalt för **kinesiska företag**, där alla dotterbolag, även de utanför Kina, kan omfattas av NIL
- NIL gäller alla ”**organisationer**” i Kina, en term som verkar omfatta alla typer av företag etablerade i Kina, oavsett ägande, dvs. privata och offentliga kinesiska aktieägare såväl som utländska aktieägare.
- NIL skulle endast gälla de **kinesiska dotterbolagen till en icke-kinesisk grupp.** Ett moderbolag utanför Kina skulle inte omfattas av kinesisk jurisdiktion enligt internationell offentlig rätt.
- NIL gäller för **alla kinesiska medborgare**, och eftersom NIL inte verkar ha en uttrycklig geografisk begränsning kan det tolkas så att det gäller alla kinesiska medborgare även när de är bosatta utanför Kina.

Källa1: http://www.npc.gov.cn/npc/c30834/201806/483221713dac4f31bda7f9d951108912.shtml
Källa 2: https://www.mannheimerswartling.se/globalassets/nyhetsbrev/msa_nyhetsbrev_national-intelligence-law_jan-19.pdf

Observera!

Vid en mer korrekt översättning av NIL är termen ”organisation” mycket bredare än just ett ”företag”.

Med ”organisation” avses alla typer av sammansatta grupperingar, exempelvis: Fackförbund, intresseorganisationer, lobbyorganisationer, bokklubbar, etc.

National Intelligence Law (“NIL”),

Bl.a Informationsinhämtning

Article 7:
All organizations and citizens shall support, assist and cooperate with national intelligence work in accordance with the law, and keep the secrets of national intelligence work that they know. The state protects individuals and organizations that support, assist, and cooperate with the national intelligence work.

Article 9:
The state commends and rewards individuals and organizations that have made major contributions to national intelligence work.

Article 14:
National intelligence work agencies carrying out intelligence work in accordance with the law may request relevant agencies, organizations and citizens to provide necessary support, assistance and cooperation.

Källa1: http://www.npc.gov.cn/npc/c30834/201806/483221713dac4f31bda7f9d951108912.shtml
Text ovan är översatt och verifierad av personal på Ancautus AB

National Intelligence Law (“NIL”),

Bl.a Informationsinhämtning

Article 16
When performing tasks in accordance with the law, the staff of the national intelligence work agency, in accordance with relevant state regulations, after approval and proof of identity can enter the restricted areas and places, and can ask relevant agencies, organizations and individuals for information and inquiries. Staff can consult or retrieve related files, materials, and articles.

Article 17
According to work needs and in accordance with relevant national regulations, the staff of the national intelligence work agency may preferentially use or requisition the vehicles, communication tools, venues and buildings of relevant agencies, organizations and individuals in accordance with the law. When necessary, they may set up relevant workplaces and equipment, the facilities shall be returned or restored in time after the tasks are completed, and corresponding expenses shall be paid in accordance with relevant regulations; if losses are caused, compensation shall be made.

Källa1: http://www.npc.gov.cn/npc/c30834/201806/483221713dac4f31bda7f9d951108912.shtml
Text ovan är översatt och verifierad av personal på Ancautus AB

Vad betyder detta då?

- ”Alla” som har något att vinna, bedriver någon form av informationsinhämtning för att skydda och stärka sig och de ”sina”.

Detta inkluderar stater, leverantörer, konkurrenter och kriminella

- Vid nyttjade av produkter/lösningar/tjänster som har någon koppling till en annan part/stat, måste detta hot tas i beaktning.

Vad kan göras?

- Inse att hotet och riskerna med informationsinhämtning och extern påverkan är reellt
- Inse att det är inte **om** verksamheten är intressant, utan **när** och **vad** i verksamheten som är intressant
- Vid behov, analysera, kontrollera och verifiera produkter/lösningar utifrån identifierade risker
- Segmentera/separera produkter/lösningar, kontrollera och verifiera kommunikation (ingress och egress)
- Analysera tillgänglighetskrav och eventuellt säkerställ redundant säker kommunikation om trådlöskommunikation ska nyttjas
- Agera systematiskt, deterministiskt och spårbart… Men! inte samma fel på samma sätt varje gång.

Thank you!