Operational security

Patrik Fältström

Senior Security Consultant


Netnod was established in 1996 and is owned by the TU foundation
We contribute to an open, secure and robust Internet

Digitized organisations must work

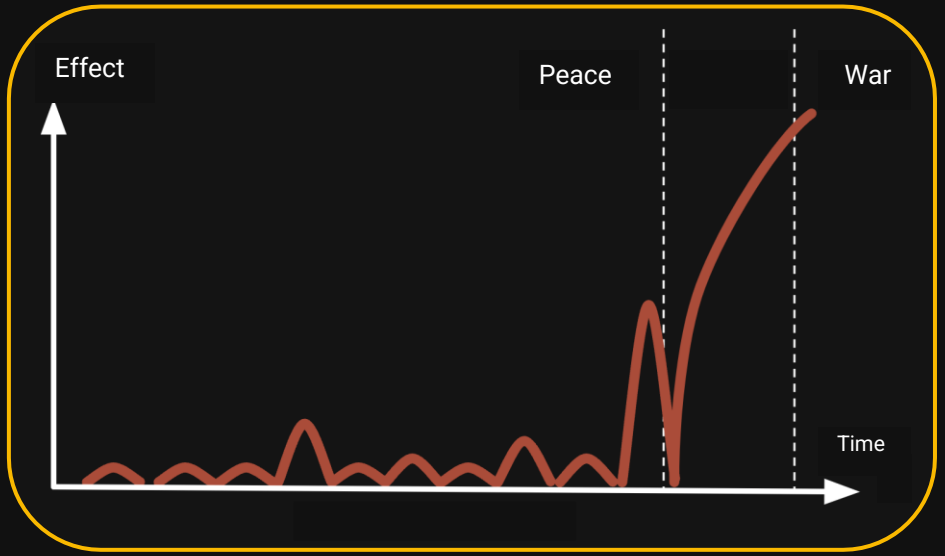
Healthcare and medication

The bank- and finance sector

The Armed Forces & cyber defence

The SAAS services, large and small

A society must be able to take a hit



Traditional attacks

IT-related attacks

Jan-feb: Military activities in the region.

17 feb: Activities in Donbas Escalates.

20 feb: Donbas and Luhansk declare themselves independent.

Putin gives order on peace mission in Donbas.

24 feb: Putin gives order on a special military operation in Ukraine.

Invasion…

13 feb: DDos towards public sector, banks, ATMs etc.

23 feb: Renewed attacks against banking and financial sector.

24 feb: HermeticWiper against organisations in Ukraine.

IsaacWiper destructive malware against Ukraine government network.

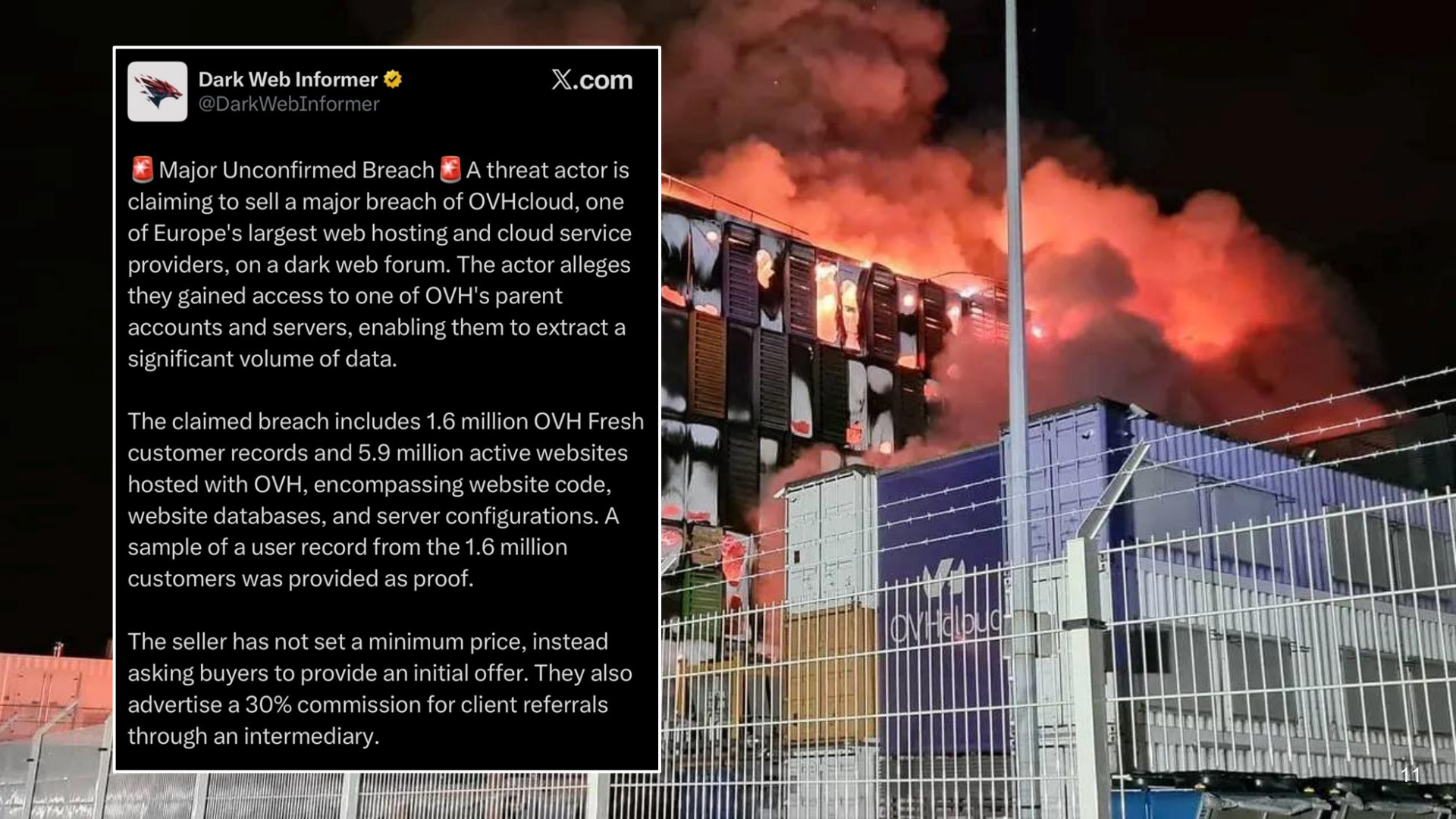
AcidRain against ViaSat, and attack against Triolan ISP.

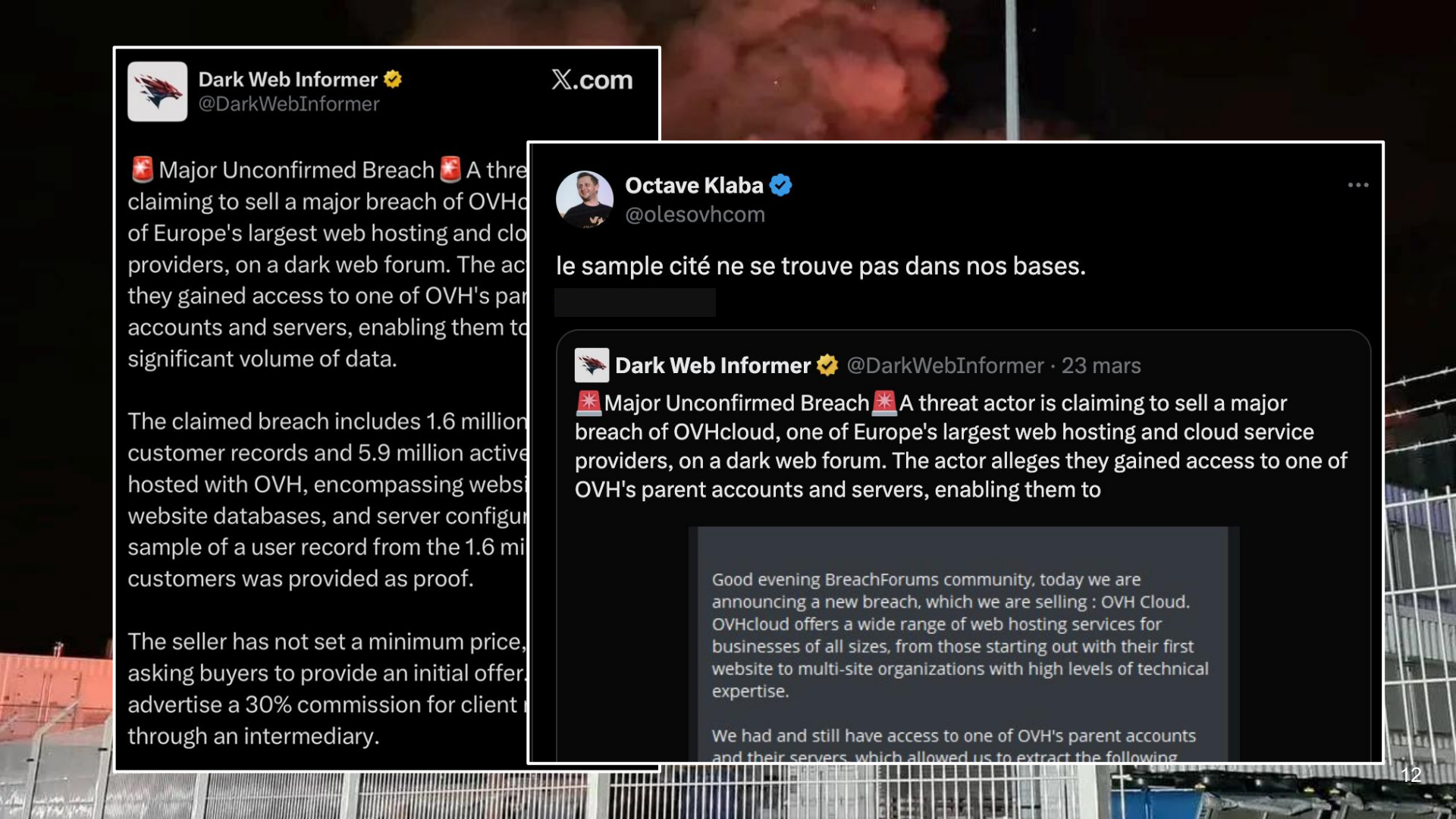
These attacks against ViaSat and Triolan has impact on Internet in Ukraine.


Black
АНІ ЛОРАК


BEST
Твій інтернет


OVHcloud


Dark Web Informer
@DarkWebInformer
𝕏.com
🚨 Major Unconfirmed Breach 🚨 A threat actor is claiming to sell a major breach of OVHcloud, one of Europe's largest web hosting and cloud service providers, on a dark web forum. The actor alleges they gained access to one of OVH's parent accounts and servers, enabling them to extract a significant volume of data.
The claimed breach includes 1.6 million OVH Fresh customer records and 5.9 million active websites hosted with OVH, encompassing website code, website databases, and server configurations. A sample of a user record from the 1.6 million customers was provided as proof.
The seller has not set a minimum price, instead asking buyers to provide an initial offer. They also advertise a 30% commission for client referrals through an intermediary.


Dark Web Informer
@DarkWebInformer
X.com
🚨 Major Unconfirmed Breach 🚨 A thre
claiming to sell a major breach of OVHc
of Europe's largest web hosting and clo
providers, on a dark web forum. The ac
they gained access to one of OVH's par
accounts and servers, enabling them to
significant volume of data.
The claimed breach includes 1.6 million
customer records and 5.9 million active
hosted with OVH, encompassing websi
website databases, and server configur
sample of a user record from the 1.6 mi
customers was provided as proof.
The seller has not set a minimum price,
asking buyers to provide an initial offer.
advertise a 30% commission for client
through an intermediary.
Octave Klaba
@olesovhcom
le sample cité ne se trouve pas dans nos bases.
Dark Web Informer @DarkWebInformer · 23 mars
🚨 Major Unconfirmed Breach 🚨 A threat actor is claiming to sell a major breach of OVHcloud, one of Europe's largest web hosting and cloud service providers, on a dark web forum. The actor alleges they gained access to one of OVH's parent accounts and servers, enabling them to
Good evening BreachForums community, today we are announcing a new breach, which we are selling : OVH Cloud. OVHcloud offers a wide range of web hosting services for businesses of all sizes, from those starting out with their first website to multi-site organizations with high levels of technical expertise.
We had and still have access to one of OVH's parent accounts and their servers, which allowed us to extract the following

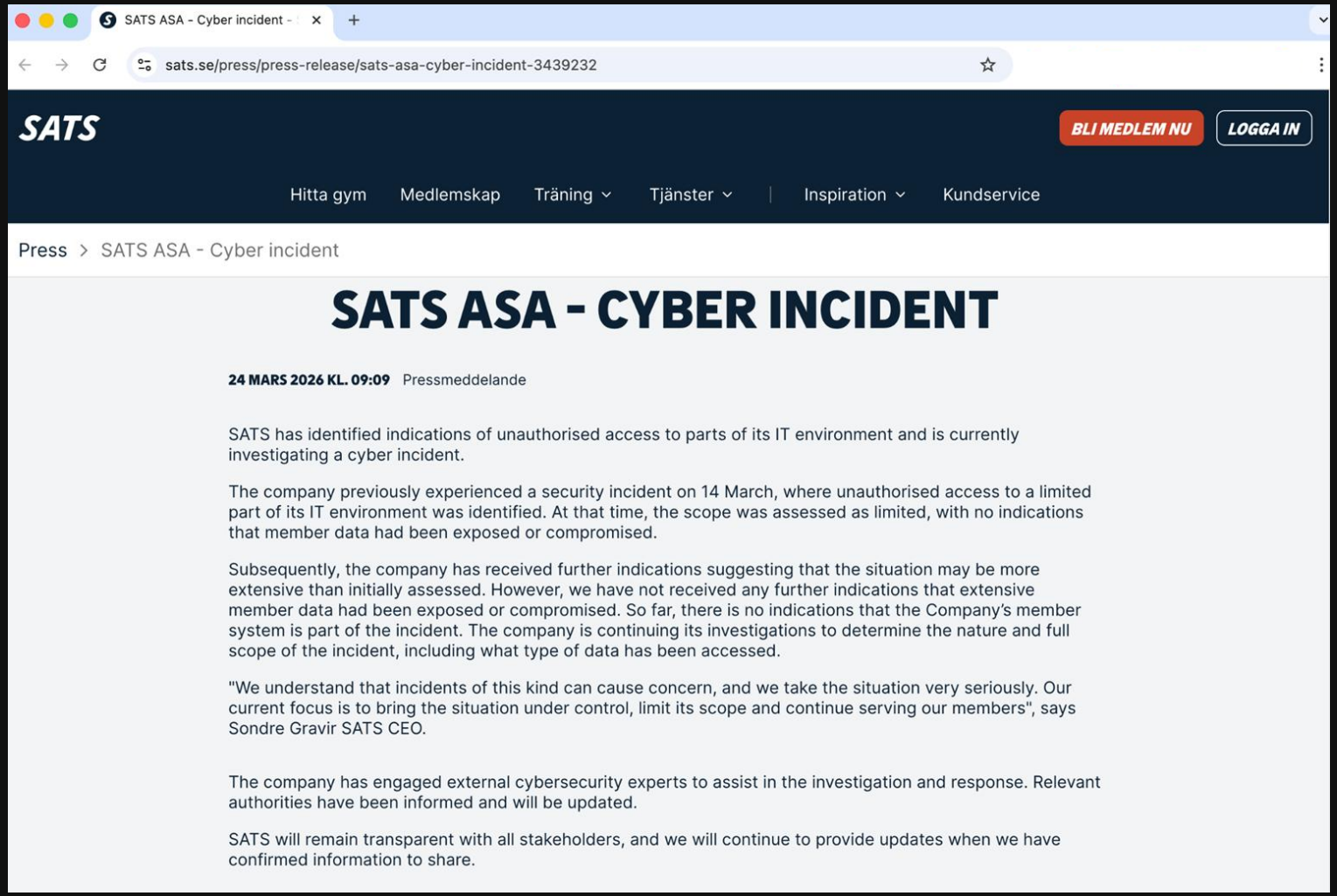
SOURCE CODE **SE Sweden E-Gov (CGI Sverige AB)**

by ByteToBreach - 12-03-26, 11:06 PM

12-03-26, 11:06 PM (This post was last modified: 11 hours ago by ByteToBreach. *Edit*

ByteToBreach

CGI


SATS ASA - Cyber incident -
sats.se/press/press-release/sats-asa-cyber-incident-3439232
SATS
BLI MEDLEM NU
LOGGA IN
Hitta gym
Medlemskap
Träning
Tjänster
Inspiration
Kundservice
Press > SATS ASA - Cyber incident
SATS ASA - CYBER INCIDENT
24 MARS 2026 KL. 09:09 Pressmeddelande
SATS has identified indications of unauthorised access to parts of its IT environment and is currently investigating a cyber incident.
The company previously experienced a security incident on 14 March, where unauthorised access to a limited part of its IT environment was identified. At that time, the scope was assessed as limited, with no indications that member data had been exposed or compromised.
Subsequently, the company has received further indications suggesting that the situation may be more extensive than initially assessed. However, we have not received any further indications that extensive member data had been exposed or compromised. So far, there is no indications that the Company's member system is part of the incident. The company is continuing its investigations to determine the nature and full scope of the incident, including what type of data has been accessed.
"We understand that incidents of this kind can cause concern, and we take the situation very seriously. Our current focus is to bring the situation under control, limit its scope and continue serving our members", says Sondre Gravir SATS CEO.
The company has engaged external cybersecurity experts to assist in the investigation and response. Relevant authorities have been informed and will be updated.
SATS will remain transparent with all stakeholders, and we will continue to provide updates when we have confirmed information to share.

NETNOD

Start local

If the internet is to hold up for healthcare, payment services and other critical things, we must start from what's local.

Local Fiber, Local Networks,
Local Information, Local Services

Local Survival

Everyone has an important role.

Education?

You have two options:

1. **Educate**
    a. **Collect questions**
    b. **Create documentation, videos etc**
    c. **Train the users**
2. **Make better software**
    a. **Collect questions**
    b. **Pass it to developers**
    c. **Fix the code**

Do organizations know what they are doing?

Do organizations know what IT systems and functions they need to do that?

Does the legislature know what is required to increase the capabilities of these systems?

Compliance is one thing, survival is another!

The correct path forward (RDO)

Step 1: Agree on what you are doing

Step 2: Do an inventory on what services are essential

Step 3: Ensure they stay alive

Step 4: Exercise, exercise, exercise


LOCKED SHIELDS 26
FRANCE SWEDEN


“Everyone thinks they have a plan
until they get punched in the face.”
– Mike Tyson

Ultimately, it’s all about

Humans

Patrik Fältström
paf@netnod.se

https://netnod.se/
info@netnod.se

Greta Garbos väg 13
169 40 Solna
Sweden