IT-säkerhet i praktiken

Eliza Öberg

Affärsområdeschef Militär teknik, Expisoft

Expisoft

är ett svenskt programutvecklingsföretag

- Utvecklar säkerhetsprodukter
- Försvarsentreprenör
- Erfaren i hög säkerhet
- Erfaren i hög assurans

Adobe hackad i 2013

Stulen användar-information:

38 miljoner konton hackades;

150 miljoner kunduppgifter tillgängliga on-line

Under Armours MyFitnessPal app hackad i februari 2018

användarnamn, e-postadressee och lösenord för appen;

150 miljoner användare påverkades

Facebook hackades i september 2018

50 miljoner konton på Facebook hackades;

90 miljoner användare har loggats ut p.g.a. risk för hackning

WannaCry (2017)

Ransomware – via phishing e-mail
Över 300 000 organisationer påverkade
150 länder

Petya (2016)

Spridning via pdf-filer
Riktad mot Windowsanvändare
Kryptering av hårddisken

NotPetya (2017)

Riktad mot Ukraina – politiska motiv?
EthernalBlue – utnyttjade sårbarhet i Windows Server Message Block (SMB) protocol
$10 miljarder

19 494

hospital appointments had to be cancelled because of the WannaCry ransomware attack.

Vad kan hända?

Det finns många olika risker och olika sårbarheter som utnyttjas.
Ofta fler än en sårbarhet utnyttjas.

- Dataläcka
- Malware (skadliga program)
- Dataförlust

- Bristande cyberhygien
- Loggning och revision
- Bristande patchning
- IT-system, hårdvara och mjukvara

Vad ska man göra?

Expisoft

Gör nåt!

2 DO

1. **Medvetandegöra och utbilda**
2. **Kartlägga riskerna**
3. **Från prat till verkstad: implementera lösningar**

I. Medvetandegöra och utbilda

- All personal, inte bara IT-personal bör ha tillräcklig kunskap om datasäkerheten.
- Tydliga processer för hur information och system hanteras.
- Förståelse att både fysiska åtgärder och administrativa rutiner behövs för att förbättra cybersäkerheten.
- ”Den svagaste länken…” – förståelse för den mänskliga faktorn.

Källa: MSB

I'll begin by saying that I hacked this mailbox (please look on 'from' in your header) more than six m
through it I infected your operating system with a virus (trojan) created by me and have been monitoring you for a
long time.

Even if you changed the password after that - it does not matter, my virus intercepted all the caching data on your
computer
and automatically saved access for me.

I have access to all your accounts, social networks, email, browsing history.
Accordingly, I have the data of all your contacts, files from your computer, photos and videos.

I was most struck by the intimate content sites that you occasionally visit.
You have a very wild imagination, I tell you!

During your pastime and entertainment there, I took screenshot through the camera of yo
with what you are watching.
Oh my god! You are so funny and excited!

I think that you do not want all your contacts to get these files, right?
If you are of the same opinion, then I think that $500 is quite a fair price to destroy the dirt I created.

Send the above amount on my bitcoin wallet: 1MN7A7QqQaAVoxV4zdjdrnEHXmjhzcQ4Bq
As soon as the above amount is received, I guarantee that the data will be deleted, I do not need it.

Otherwise, these files and history of visiting sites will get all your contacts from your device.
Also, I'll send to everyone your contact access to your email and access logs, I have carefully saved it!

Since reading this letter you have 48 hours!
After your reading this message, I'll receive an automatic notification that you have seen the letter.

I hope I taught you a good lesson.
Do not be so nonchalant, please visit only to proven resources, and don't enter your passwords anywhere!
Good luck!

Ilse
Ilse
Heike
Anja
Gertrud
Sandrine

I could not resist and pass by!

But here you are, and I'm ready to unveil to you

Even your eyes can tell me how confident you are.

In any case, I am happy that we met

You seem to know how to make a girl turn on

Hands-free (autopilot) profits system

2. Kartlägga riskerna

Viktigt att ställa sig följande frågor:

- **Varför** ska man skydda sig?
- **Vad** kan vi förlora och hur mycket skulle det **kosta** oss?
- **Vad** ska man **skydda**? = Vad ska prioriteras att skyddas?
- Vad är **kritiskt viktigt att skydda** i en organisation?
- Gör vi **rätt saker** med pengarna?

3. Implementera lösningar

- Cyberhygien
- Implementera rutiner och tydliga processer för hur information och system hanteras
- Tänk på helheten (den svagaste länken i kedjan)
- Tvåfaktorsautentisering istället för lösenord

Expisofts teknologi

Smartkortssystem

- Kortutgivning
- Tillfälliga kort

PKI- och CA-system

- Utfärdande av certifikat
- Digitala signaturer

Stark autentisering

- SSO (Single-Sign-On)

Single sign-on
till applikationer

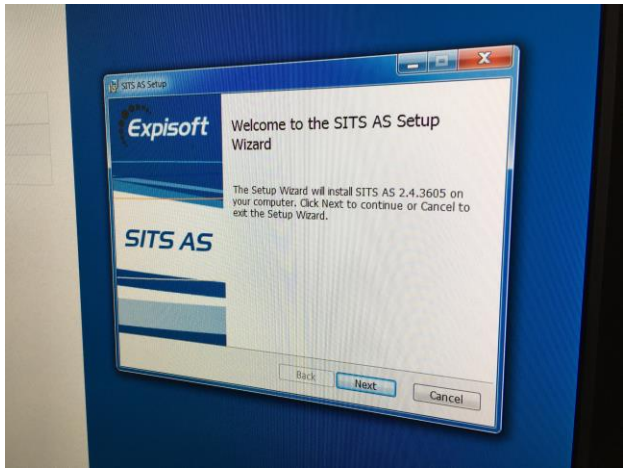
krypterad och signerad
e-post

elektroniska
signaturer

smartkort
inloggning

hårddisk/fil
kryptering

3. Implementera lösningar



- Olika säkerhetsnivåer för olika innehåll
- Arkitektur med tunna klienter istället för tjocka
- Skapa förutsättningar så att det blir **lätt att göra rätt**.

Eliza Öberg

eliza.oberg@expisoft.se

+46 76-314 14 47