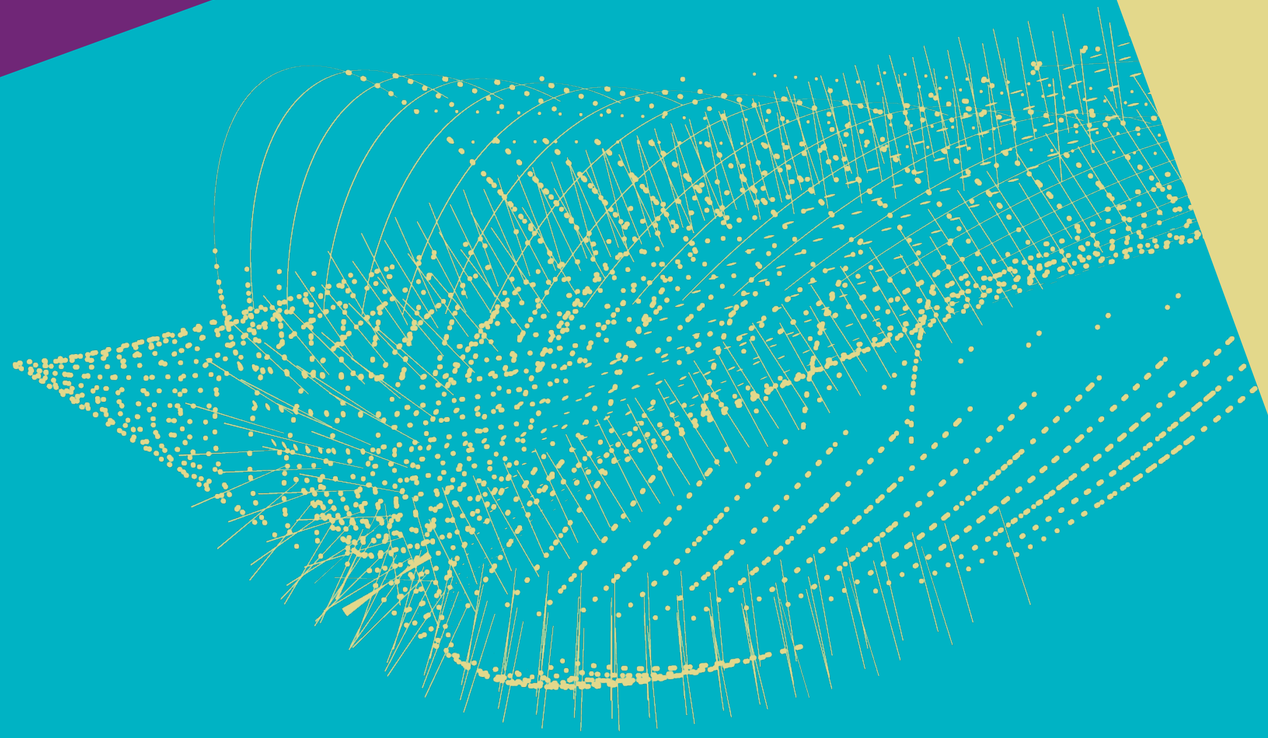
Nikhef



RONALD STARINK (CT)

CYBERSECURITY

Nikhef Staff meeting 2021-10-15

Subsidie-aanvragen bij wetenschapsinstituut NWO liggen stil na hack

NOS NIEUWS • BINNENLAND • BUITENLAND • 24-02-2021, 23:19

Wetenschapsorganisatie NWO afgeperst door bekende cybercriminelen, gaat niet in op eisen

Niet betaald? Dan lekken we je data, dreigen de internetcriminelen

Cyberaanval op UvA en HvA: 'Toegang derden tot ict-systemen'

RTL kampt met digitale aanval, mogelijk sprake van gijzelsoftware

Hacker perst hogeschool van Arnhem en Nijmegen af

NOS NIEUWS • BINNENLAND • TECH • VANDAAG, 12:05

Situatie cyberaanval VDL Groep ongewijzigd, weer geen productie bij Nedcar

Attention at Political Level

"*… bij universiteiten en hogescholen 'totaal geen bestuurlijke aandacht' is voor digitale veiligheid.*" Daarmee zetten onderwijsinstellingen volgens de topman de economische en nationale veiligheid op het spel.

Van Engelshoven [heeft] aan de instanties gevraagd om hun veiligheidsbeleid onderdeel te laten uitmaken van hun jaarverslagen en dit te bespreken met de Raden van Toezicht. "*De genomen maatregelen laten wat mij betreft zien dat de instellingen de cyberveiligheid serieus nemen. Het bereiken van honderd procent veiligheid is helaas onmogelijk, er zal altijd een risico op cyber- en kennisveiligheidsincidenten blijven bestaan*"

"Die [ransomware] betalingen zijn de Nederlandse overheid een doorn in het oog: het ministerie van Justitie en Veiligheid zoekt nu naar manieren om het te stoppen, bijvoorbeeld door verzekeraars te verbieden om losgeld te vergoeden."

Attention in NWO-I

Security

Privacy

Knowledge Safety

Business Operations optimization

Research Data Management

Nikhef

ARCNL ADVANCED RESEARCH CENTER FOR NANOLITHOGRAPHY

NIOZ

DIFFER Dutch Institute for Fundamental Energy Research

ASTRON

CWI Centrum Wiskunde & Informatica

AMOLF physics of functional complex matter

SRON Netherlands Institute for Space Research

nscr

Some tension...

Bureaucrats: Control

- Policies
- Procedures
- Documentation
- *Compliance*

Scientists

- Openness
- Academic freedom
- Free choice of equipment
- No/minimal overhead
- *Rationality*

A Really Bad Hack™ Scenario

- Phishing attack → ransomware
- Compromising **all** systems
- No payment of the ransom

What won't work:

- email
- SSO
- logging in on any system
- website
- Stoomboot
- data on /user, /project, /data and /dcache encrypted
- network at Nikhef (wifi & wireless)

What will work

- your self-managed laptop
- your mobile phone

Can this happen at Nikhef?

Even worse… something will happen

Probably within 5-10 years

'Grootste risico dat er is'

Bedrijven nemen nog veel te weinig maatregelen tegen ransomware, zeggen deskundigen. "Dit is misschien wel het grootste bedrijfsrisico dat er nu is", zegt Dave Maasland, cybersecurity-expert bij ESET. Hij vindt dat ransomware moet worden besproken in de "boardrooms van grote bedrijven".

Het is volgens Maasland gevaarlijk dat bedrijven zich vaak niet kunnen voorstellen dat zij slachtoffer kunnen worden van een online-aanval. "Deze criminelen hebben echt een manier gevonden om zo'n hele organisatie plat te leggen. We zien nu dat bedrijven erg kwetsbaar zijn door de verregaande automatisering van hun systemen."

> **Het is een digitale hartstilstand.**
>
> — Dave Maasland, cybersecurity-expert bij ESET

En hoewel bedrijven zich dan onkwetsbaar mogen wanen, het aantal grote aanvallen neemt toe.

Steps to recovery

Action	Who	Duration
Detection	-	-
Investigation (what's happening?)	CSIRT	~1 hr
Stopping the attack	CSIRT	1hr – 1 day
Root cause analysis (prevent recurrence)	CSIRT	1-2 weeks
Rebuilding systems	CT & PDP	~1 month
Recovering data from backup	CT & PDP	1-2 months
Regenerating data not in backup (if possible!)	user groups	>6 months

Impact: long downtime of ICT services, lots of stress, reputation damage, probably loss of unrecoverable data → delays & drama

Done?

NOPE

Imposed measures for stricter control, restriction of current freedom, more policies & bureaucracy

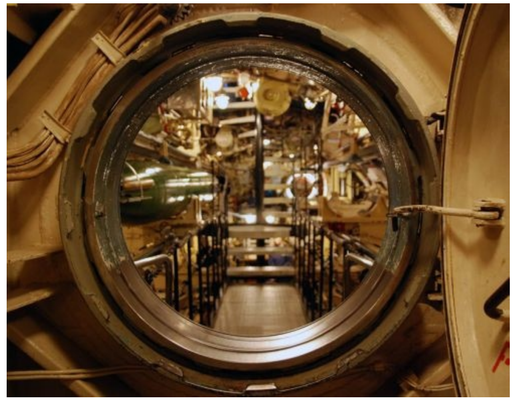
What ~~can~~ must **we** do?

$$Security = technical\ measures \otimes physical\ protection \otimes process \otimes people$$

Security is not an ICT *fest* – we need your participation!

Technical Measures

- Firewall
- Virus scanner
- Up-to-date software
- Encryption (controlled)
- Monitoring
- Backups (selected data)
- Compartments in infra



<u>What if</u> only technical measures:

- Implement more and stricter security policies
- 24x7 monitoring and follow-up
- *Exclusively* CT-managed laptops
- Requires compliance checks & auditing
- Backup all data

- Estimated annual costs:

→ Extra ICT staff needed: +5 FTE (~7 OE)
→ Offline backup (~3 PB): ~30 OE

1 OE = 1 OIO Equivalent = ~€50000 / year

Physical Protection

- Access control to the building, data centre
- Locking doors
- Locking computers

Process

- Policies
- Procedures to securely setup systems
- Forced password renewal
- Blocking remote access for untrusted devices & services

Controls known to bureaucrats!

- <u>Know which data you have!!</u>
  - Think about data quality

→ helps to prepare for Research Data Management!

Cooperate in identifying “crown jewels”:

- Data that are sensitive for espionage → protection
- Data that must not be lost / destroyed → storage type

People (you & me)

- Digital hygiene
  - Unique, personal passwords in password safe
- Awareness (group meetings?)
- Attentive to threats
- Only use authorized software & services
- Empty devices when travelling
- Accept some **necessary** small inconveniences
  - *Do not take shortcuts* (ask advice)

- Suspicious situation or suspected incident:
  - Act **immediately**, contact CSIRT (security@nikhef.nl)
  - Communicate transparently & don't hide anything

AVOID	USE INSTEAD
"Convenient mail app" retrieving mail with Nikhef password	Standard IOS app, K9-mail for Android
Gmail	Nikhef mail
Dropbox	SURFdrive
WeTransfer	SURF FileSender
...	...

Summary

- Cyberthreads are real
- Hot topic in politics and NWO(-I)
- Invest time to identify crown jewels
- All: common responsibility in
  - Preventing security incidents
  - Ensuring “business continuity” – your research!
  - Avoiding undesired policies, limitations, bureaucracy

Freedom implies taking responsibility!

Questions / incidents:

- security@nikhef.nl / 020-592 5090
- privacy@nikhef.nl
- CSIRT: Arthur, Bart, Daniel, David, Dennis, Jouke, Sven, Wilco, Ronald