



IT SECURITY AWARENESS

Experiences and Discussion on Training Strategies

Feb. 26th 2018 | Ralph Niederberger, rrn@fzj.de

SOME FACTS ILLUSTRATING JÜLICH

What has been done in the past

- Founded in Dec. 11th 1956
- Shareholder: BRD (90%) & NRW (10%)
- 2,2 square kilometers
- budget >500 M€/y incl. third party funds
- 6.500 employees
- 80 instituts coming from nine research areas
- Many projects, publications, and patents
- Several branch offices spread throughout Germany



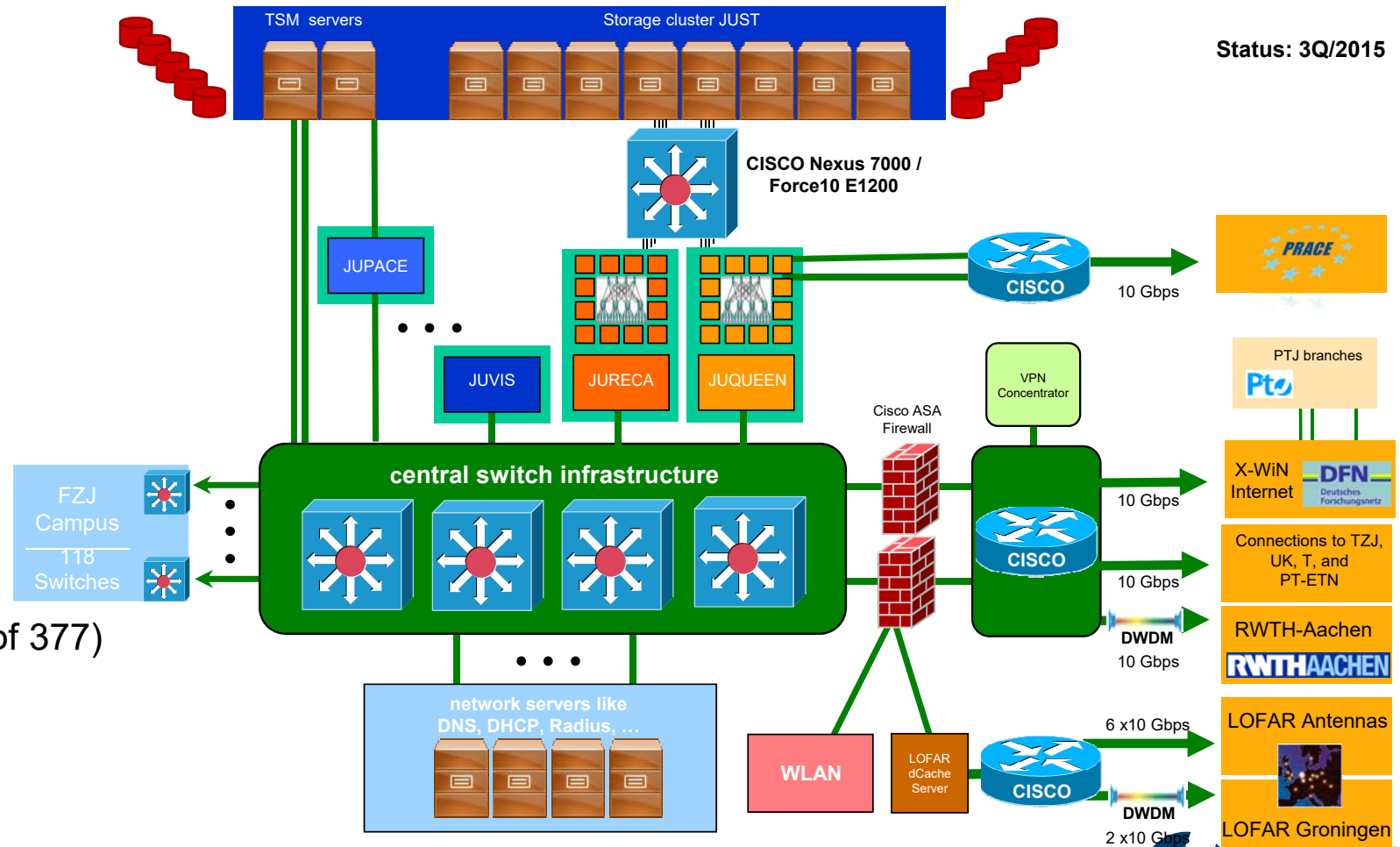
Energy and Environment



Information and the brain

THE CAMPUS NETWORK

- # hosts: 21298
- # admins: 986
- # IP addresses: 24328
- # IP addresses: 21502
- # IP-Subnets: 499
- # official subnets: 163
- # (sub)domains: 377
- # ext. domains: 284 (out of 377)



Status: 3Q/2015

THE IT SECURITY AWARENESS CHALLENGE

Central question: How to make employees IT security aware?

Employees: gardener, cleaning personal,
administrative, trading and secretary personal,
technical personal, researchers, up to nobel price winners

Behaving and personal biases: Nothing to find on my computer.
Passwords have to be easy to remember.
Anyone can know my personal data.
Click on anything and „feel free“

IT SECURITY ACTIVITIES / EVENTS AT JÜLICH

What has been done in the past

- IT security information for administrators for several years
Replaced by IT security declaration to be signed by admins
- Phishing attacks for awareness and advertising events
- IT security presentations (always 6 times 90 minutes) last 5 years
- IT security breakfast (90 mins) 2 times (2016 and 2017)
- IT security day / Cyber Security day (2017)
- JuNet Internet Security day (14-17 afternoon) / yearly

BEING HACKED MAKES SENSITIVE

Sending two mail: a Phishing and resolution mail as invitation

“Phishing Mail” was an IT Security Test

1 October 2014.

Yesterday everyone received an e-mail from support@fz-juelich.de requesting volunteers to test Apple products. In return, the testers could keep the iPhones and iPads used in the test. In order to participate, one had to click on a link in the e-mail and then submit user name and password.

xx % of our colleagues fell for this so-called “phishing” attack and submitted their personal data. Even more – yy % - clicked on the link in the e-mail. Had the e-mail actually been from a cyber-criminal, she would now be able to misuse the sensitive data of many colleagues. However, the mail was in fact a test by our IT security management in order to raise awareness for the threat of such phishing attacks. The website linked in the e-mail was harmless and no user data was recorded or transmitted.

How phishing mails work and how they can be recognized is explained in a video in the newly designed intranet webpages on IT security:

Phishing Video

Hacking-Day on November 5th 2014

Cyber attacks on companies are increasing steadily and the Forschungszentrum is no exception. Successful attackers can access sensitive research and employee data. Thus, it's important to know the threats and how to defend oneself. At the Hacking Day on Nov. 5th in the large auditorium of the central library ZB, IT security experts will give live demonstrations of how cyber attackers forge e-mails or crack passwords.

As part of the IT-Security Awareness Campaign, the intranet webpages on IT security were redesigned. They give users and administrators assistance and numerous tips on how to use the network securely.

IT SECURITY AWARENESS IN THE WEB

The web info for

- users
- administrators

Info on

- contact persons
- hints for practice
- documentation
- videos and e-learnings

Links to

- IT security guideline
- and IT security rules
- basic protection for guests

IT-THEMEN

IT-Standards

IT-Sicherheit >

Für Anwender v

E-Mail und Phishing

Sichere Passwörter

Viren und Trojaner

Cloud und Social Media

Ransomware

Zu Hause und unterwegs

Für Administratoren

Ansprechpartner

Dokumentation

Videos und E-Learnings

Praxistipps

SecurityINFO Aktuell

Cyber Security Day 2017

Datenschutz

IT-Strategie

IT-Rahmenkonzept

IT-Gesamtplanung

Webauftritte

Video- und Webkonferenzen

SERVICE

Selfservice

Stichwortliste IT-Belange

Tipps für die sichere Nutzung der IT

Technische Lösungen funktionieren nur, wenn Mitarbeiterinnen und Mitarbeiter sowie Führungskräfte sie korrekt anwenden und nicht - bewusst oder unbewusst - umgehen.

Auf diesen Seiten sind die wichtigsten Verhaltensregeln, Tipps und Tricks im sicheren Umgang mit den IT-Systemen des Forschungszentrums zusammengestellt.



E-Mail und Phishing

→ Top Thema Phishing und Tipps zum Umgang mit E-Mails



Sichere Passwörter

→ Tipps für den Umgang mit Passwörtern



Viren und Trojaner

→ Schutz gegen Viren und Trojaner



Ransomware

→ Schutz vor Erpressungssoftware und Verhalten im Ernstfall



Cloud und Social Media

→ Hinweise zur sicheren Nutzung von Cloud Diensten und Sozialen Netzwerken



Zu Hause und Unterwegs

→ IT-Sicherheit zu Hause und Unterwegs



NOTFALL?

Wie erkennt man einen Notfall und was ist zu tun?

VIDEOS

Einzelne themenspezifische Videos sind auf den jeweiligen Webseiten platziert. Alle Videos finden Sie in der IT-Sicherheitsmediathek.

DOKUMENTE

- IT-Sicherheitsrichtlinie des Forschungszentrums Jülich (PDF, 467 KB)
- IT-Sicherheitsregeln für den Grundschutz (PDF, 122 KB)
- Merkblatt IT-Grundschutz für Gäste (PDF, 60 KB)
- Folien der Informationsveranstaltung zur IT-Sicherheit 2014 (PDF, 988 KB)
- Weitere Dokumente IT-Sicherheit

ENGLISH VERSION

This site in english

IT SECURITY VIDEOS ON JÜLICH WEB PAGE

Live recordings from presentations:

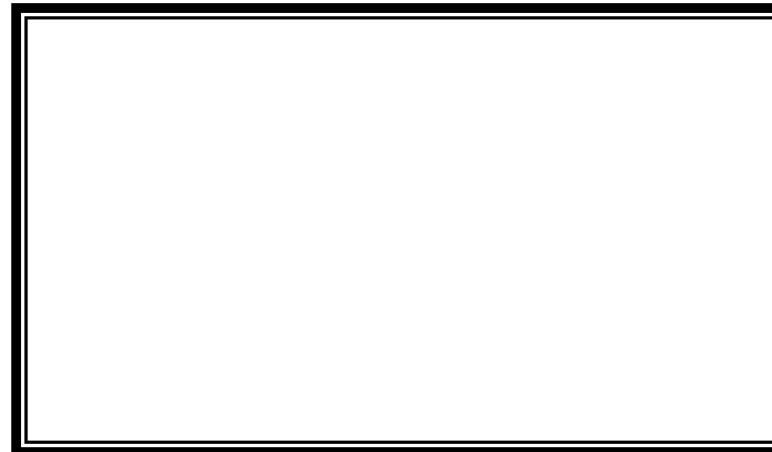
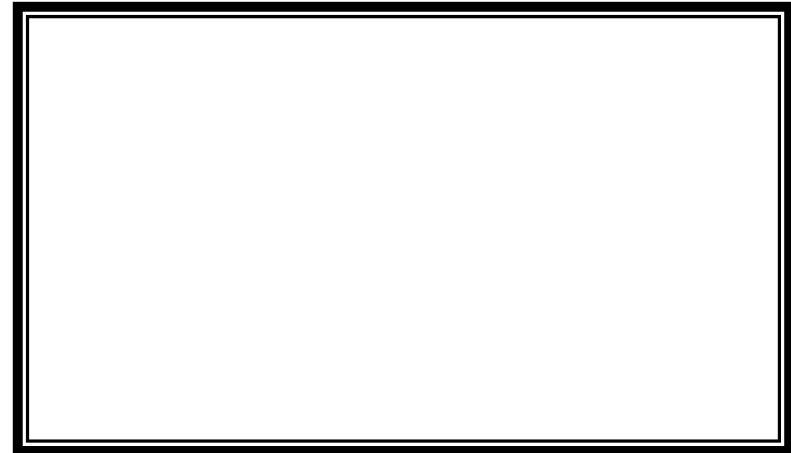
- Social Media
- Passwords
- Desktop
- Mobile Devices
- Trojans and Viruses

Videos:

- Phishing
- Cloud
- Mobile Devices
- Ransomware

In preparation:

- Why Security
- Phishing advanced



IT SECURITY AWARENESS – ADVERTISING EVENTS

Hacking Day *Reloaded* im Forschungszentrum Jülich

am 23. Juni 2015 im großen Hörsaal der ZB

Trojaner bauen **Passwort knacken**
Phishing E-Mail
E-Mail Absender fälschen

Watch out – protect your data!

Hacking Slots
09:00 – 09:45 Uhr 13:00 – 13:45 Uhr
10:00 – 10:45 Uhr 2:00 – 2:45 p.m. (english)
11:00 – 11:45 Uhr 15:00 – 15:45 Uhr

IT-Security Awareness Kampagne 2015: ein Projekt von IKM, JSC und UK
<http://intranet.fz-juelich.de/IT-Sicherheit>

Crash Kurs Cyber Security – so schützen Sie sich!

Alle Mitarbeiterinnen und Mitarbeiter sind eingeladen!

Social Engineering aufdecken
Sichere Passwörter wählen
Cloud-Dienste und mobile Geräte sicher nutzen
Trojaner abwehren
Phishing-E-Mails erkennen

Watch out – protect your data!

Im großen Hörsaal der ZB – mögliche Termine:

18. August	19. August	20. Oktober	21. Oktober
09:30 – 12:00 Uhr	09:30 – 12:00 Uhr	09:30 – 12:00 Uhr	09:30 – 12:00 Uhr
13:30 – 16:00 Uhr	13:30 – 16:00 Uhr	13:30 – 16:00 Uhr	13:30 – 16:00 Uhr

IT-Security Awareness Kampagne 2015: ein Projekt von IKM, JSC und UK
<http://intranet.fz-juelich.de/IT-Sicherheit>

Coffee Break Cyber Security Thema “E-Mail” – so schützen Sie sich !

21. Juni 2016 im Seecasino, 9:00 – 10:00 Uhr

Watch out – protect your data!

Alle Mitarbeiterinnen und Mitarbeiter sind eingeladen!
Bringen Sie Ihr Frühstück mit. Wir sorgen für den Kaffee.

Nächster Coffee Break „Mobile Geräte“ im September 2016.

IT-Security Awareness Kampagne 2016: ein Projekt von IKM, JSC und UK
<http://intranet.fz-juelich.de/IT-Sicherheit>

THE CYBER SECURITY DAY

Advertisement

- Posters within campus
- Flyers in post box and at lunch locations
- Newsletter
- Intranet web pages

Mitglied der Helmholtz-Gemeinschaft

IT Security Awareness – Experiences and Discussions
WISE WS, Abingdon, Feb. 26th 2018, rrn@fzj.de

Cyber Security Day - Mit Keynote Verfassungsschutz



am 21. September 2017 von 9:00 Uhr bis 16:00 Uhr
im Foyer der ZB
Alle Infos im Intranet

IT-Security Awareness Kampagne: ein Projekt von IKM, JSC und UK
<http://intranet.fz-juelich.de/IT-Sicherheit>

Wechselnde Vorträge + Livedemos + Experten-Stände + Interaktiver Infopoint

THE CYBER SECURITY DAY

Presentations and booths

Presentations:

- „Cyber security Breakfast“: Detect and defend phishing (incl. President Scam)
- Federal Office of Cyber security: Travels abroad and related risks
- Cloud / „Personal Outsourcing“
- Protecting your smartphones
- Trojans and Viruses
- Cracking passwords and how to secure
- Security @ Home: Net and PC (Wireless, router, child protection, antivirus, updates, etc.)

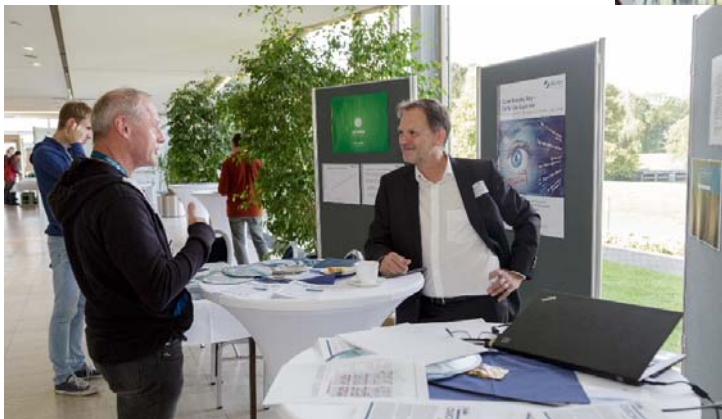
Booths „Meet the expert“

- FZJ-CERT
- Protecting mobile devices
- Cyber security in general
- Physical security

Learning stations / mini e-learning / videos

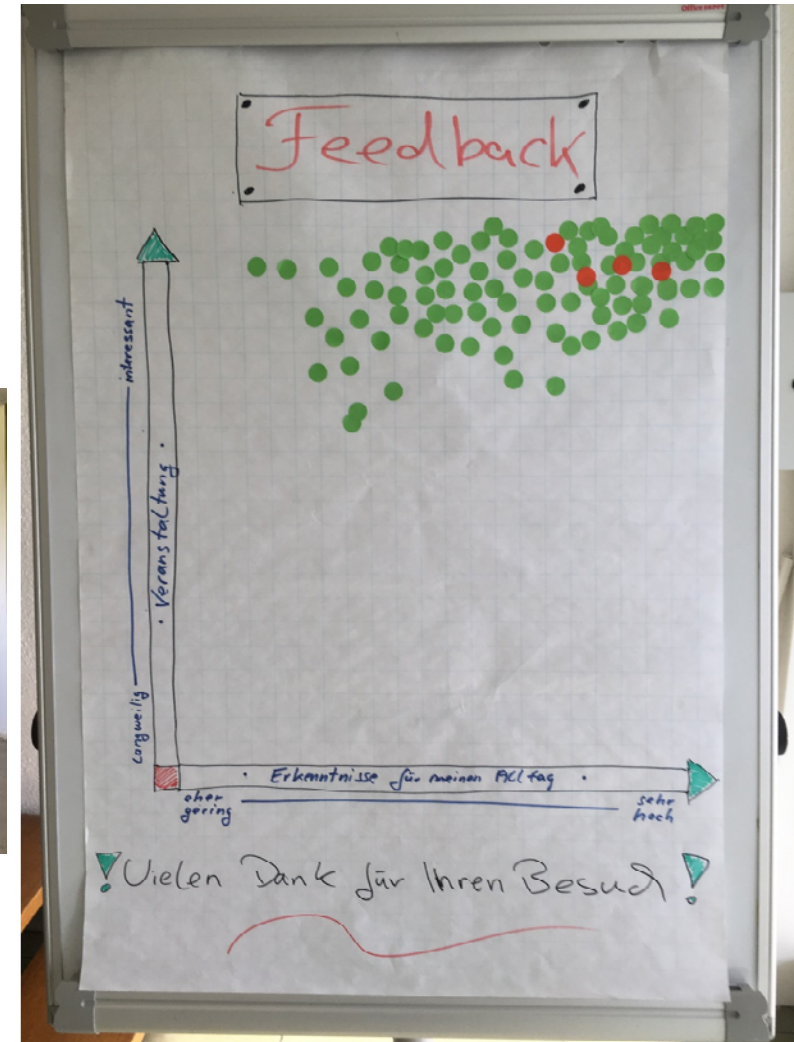
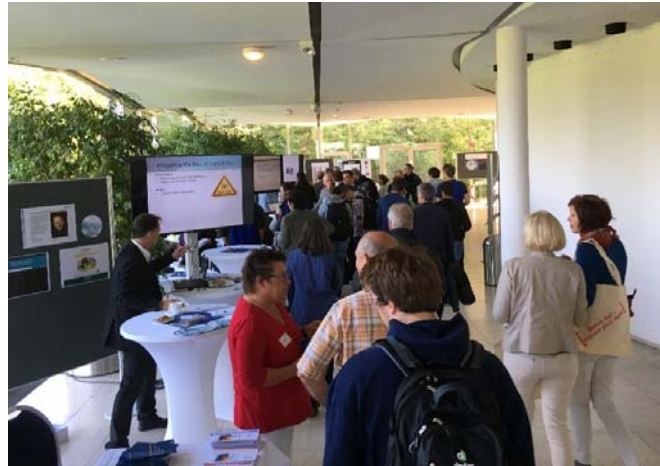
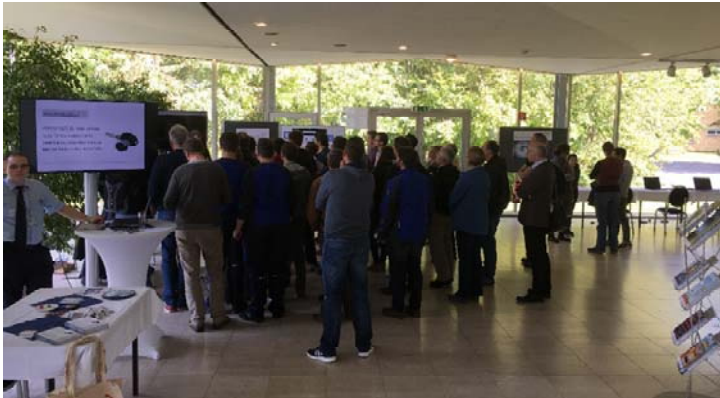
THE CYBER SECURITY DAY

Some impressions



THE CYBER SECURITY DAY

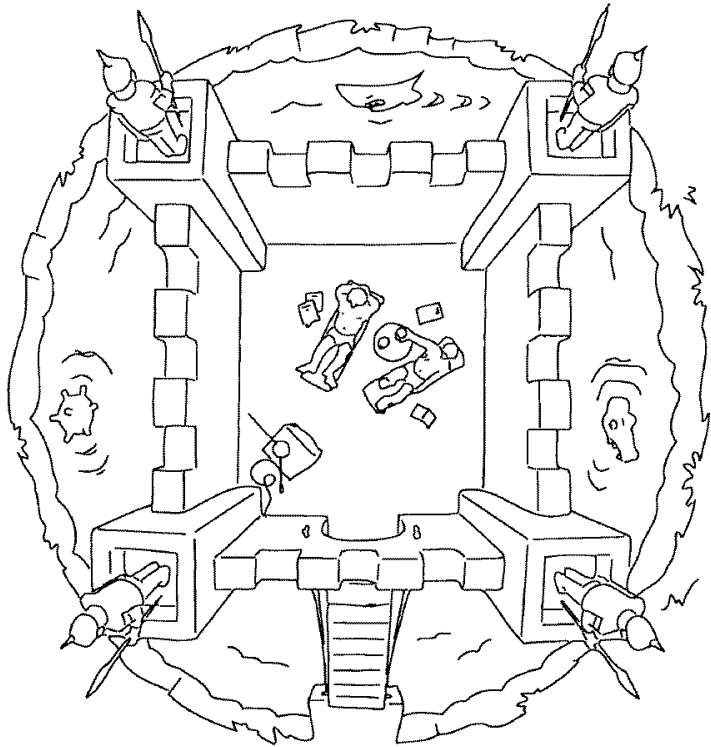
More impressions



WHAT NEXT

- PC drivers licence for local users and administrators?
- IT security awareness for community users?
- More videos, moodles, info material?
- Webinars, presentations by external security expert?
- Working together with others with similar problems...

DISKUSSIONS



“Sure, I’m paranoid.

But am I paranoid enough? “

The Security manager

Internet - Everyday