Improve cybersecurity at Swiss universities

asut Member-Apero, 7. September 2023

Martin Leuthold, Head of Data, Security & Network

SWITCH

Agenda

Intro SWITCH & services history

Specific universities threat landscape

SWITCH security services evolution

Questions & discussion

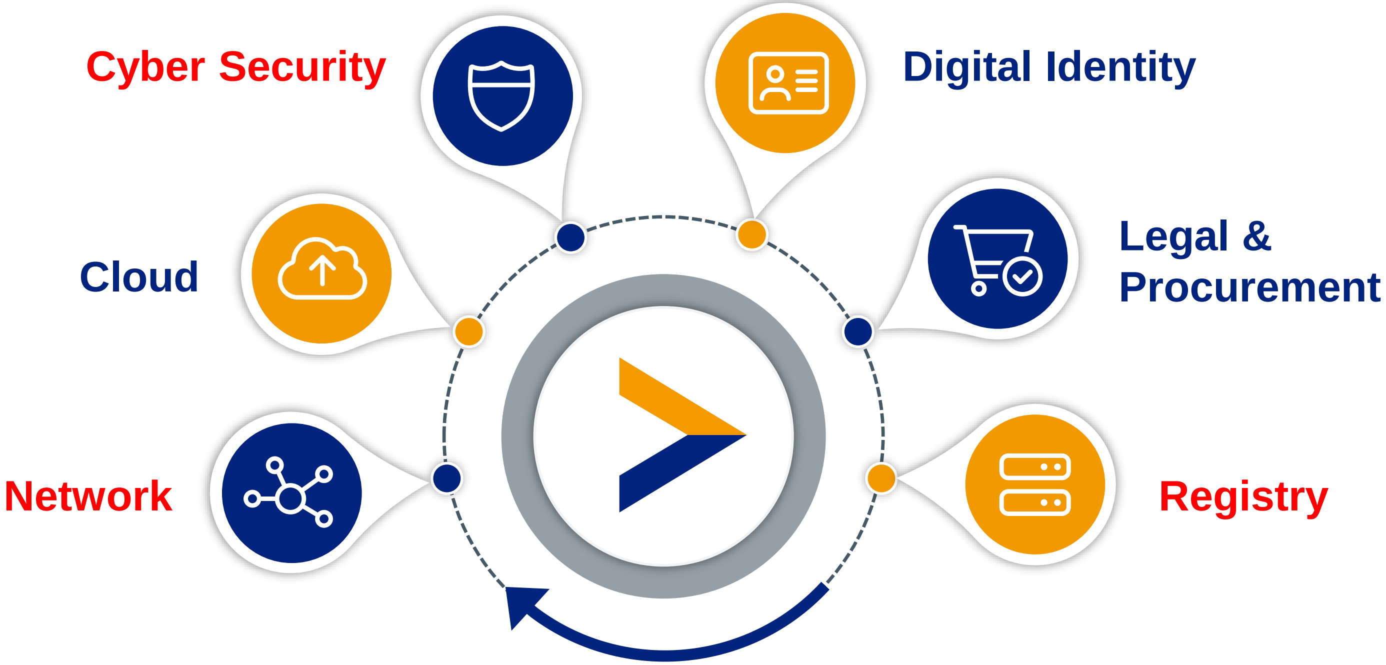
About SWITCH

Foundation

The foundation creates, promotes and offers the necessary basis for effective use of modern methods of telecomputing in teaching and research in Switzerland.

Swiss Internet & security pioneer

Our services are based on an integrated combination of our core competencies and community support, and are optimally tailored to the situation of each individual customer.



SWITCH

University threat landscape and legal compliance

Sector risk profiles specifics and spectrum

Swiss Universities: Similar & sector-specific risks and a wide spectrum

→ **Partial sector of Swiss critical infrastructure** (government sector)
→ **Freedom of education and research** vs sufficient information security
→ **High concentration of critical data** ((sensitive) personal data, research data, IP, …)
→ **High fluctuation** of students and researchers.
→ **Few managed devices. Risk of misuse** of (powerful) IT infrastructure
→ Sensitive for **business interruptions at specific times** (exam period, semester start)

→ **Organizations size** varies from 200 to 30‘000 students
→ **Profiles** from **strong education focus** to **strong research focus (**in critical domains)
→ **Internationally top ranked and top-visible** to **just regionally known**

Conclusions

→ Same **core business education and research**: similarities in the threat profiles and derived protection requirements
→ **No „one-size-fits-all“ approach for information security**: Must be risk based.
→ **Specific sector approach** is beneficial.
→ **Bundle efforts in a competence center** improves quality and optimizes value

Growing legal compliance requirement

Code of obligations (Art 71a OR)

→ Audit requirements includes mandatory risk management for organizations of any size
→ Accountability with the board of directors

New Swiss **data protection law** (enacted from September 2023)

→ Equivalent to GDPR; triggers (tough) data protection measures

Information security law

→ Focus on government and critical infrastructure (universities are in!)
→ 24h reporting obligation for (high-impact) security incidents
→ Requires (adequate) information security management

National Cybersecurity Strategy

→ 3rd evolution passed by the federal council. Now open ended.
→ NCSC to become federal office. Measures: SWITCH named as a key actor

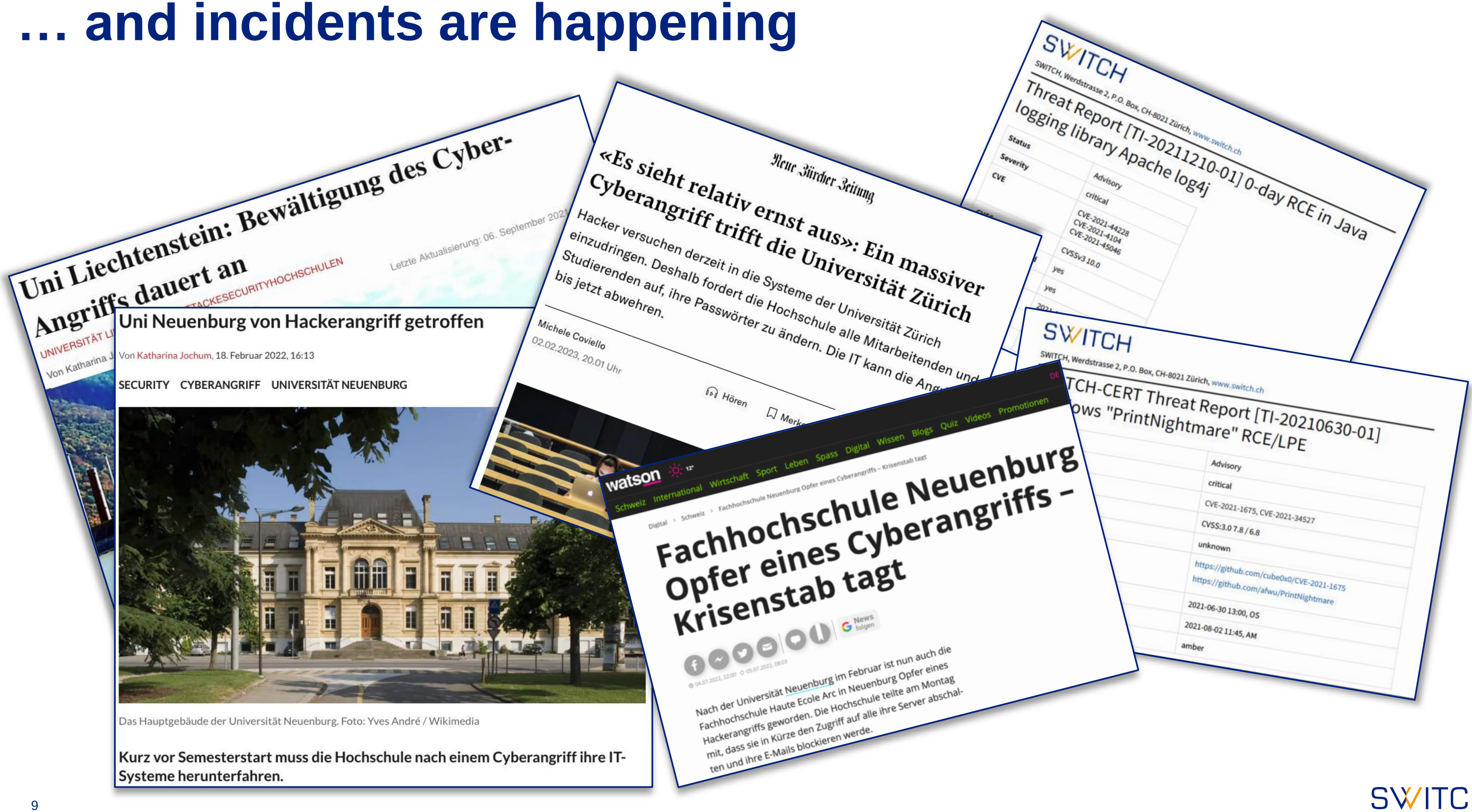
Minimum standard for ICT security

→ Developed by the Federal Office of National Economic Supply (FONES)
→ Based on NIST CSF (specific adaptations to some CI-sectors)
→ Currently recommendation (mandatory minimum standards for CI discussed (e.g. Energy)

Strategy for Critical Infrastructure

→ Owned by the Federal Office of Civil Protection (they do as well the sector risk assessments)

… and incidents are happening



Uni Liechtenstein: Bewältigung des Cyber-Angriffs dauert an

UNIVERSITÄT LI… …TTACKESECURITYHOCHSCHULEN

Von Katharina J…

Letzte Aktualisierung: 06. September 2021

Uni Neuenburg von Hackerangriff getroffen

Von Katharina Jochum, 18. Februar 2022, 16:13

SECURITY CYBERANGRIFF UNIVERSITÄT NEUENBURG

Das Hauptgebäude der Universität Neuenburg. Foto: Yves André / Wikimedia

Kurz vor Semesterstart muss die Hochschule nach einem Cyberangriff ihre IT-Systeme herunterfahren.

Neue Zürcher Zeitung

«Es sieht relativ ernst aus»: Ein massiver Cyberangriff trifft die Universität Zürich

Hacker versuchen derzeit in die Systeme der Universität Zürich einzudringen. Deshalb fordert die Hochschule alle Mitarbeitenden und Studierenden auf, ihre Passwörter zu ändern. Die IT kann die Ang… bis jetzt abwehren.

Michele Coviello
02.02.2023, 20.01 Uhr

SWITCH
SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich, www.switch.ch

Threat Report [TI-20211210-01] 0-day RCE in Java logging library Apache log4j

Status	Advisory
Severity	critical
CVE	CVE-2021-44228 CVE-2021-4104 CVE-2021-45046
CVSS…	CVSSv3 10.0
…d	yes
	yes
	2021…

SWITCH
SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich, www.switch.ch

…TCH-CERT Threat Report [TI-20210630-01] …ows "PrintNightmare" RCE/LPE

	Advisory
	critical
	CVE-2021-1675, CVE-2021-34527
	CVSS:3.0 7.8 / 6.8
	unknown
	https://github.com/cube0x0/CVE-2021-1675 https://github.com/afwu/PrintNightmare
	2021-06-30 13:00, OS
	2021-08-02 11:45, AM
	amber

Digital › Schweiz › Fachhochschule Neuenburg Opfer eines Cyberangriffs – Krisenstab tagt

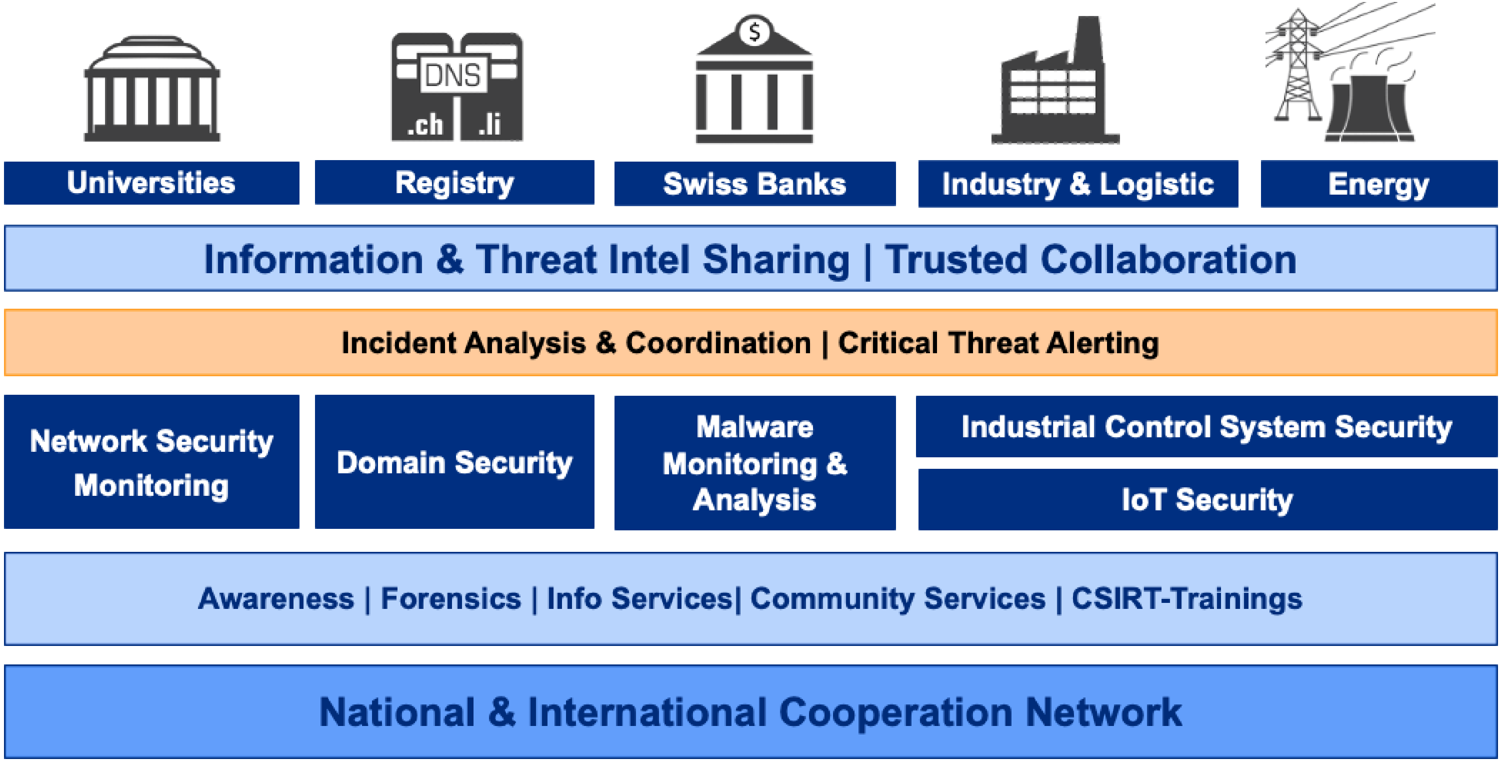
Fachhochschule Neuenburg Opfer eines Cyberangriffs – Krisenstab tagt

04.07.2022, 22:00 05.07.2022, 08:03

Nach der Universität Neuenburg im Februar ist nun auch die Fachhochschule Haute Ecole Arc in Neuenburg Opfer eines Hackerangriffs geworden. Die Hochschule teilte am Montag mit, dass sie in Kürze den Zugriff auf alle ihre Server abschalten und ihre E-Mails blockieren werde.

SWITCH cybersecurity services for universities

Competence center & sector approach



Universities | Registry | Swiss Banks | Industry & Logistic | Energy

Information & Threat Intel Sharing | Trusted Collaboration

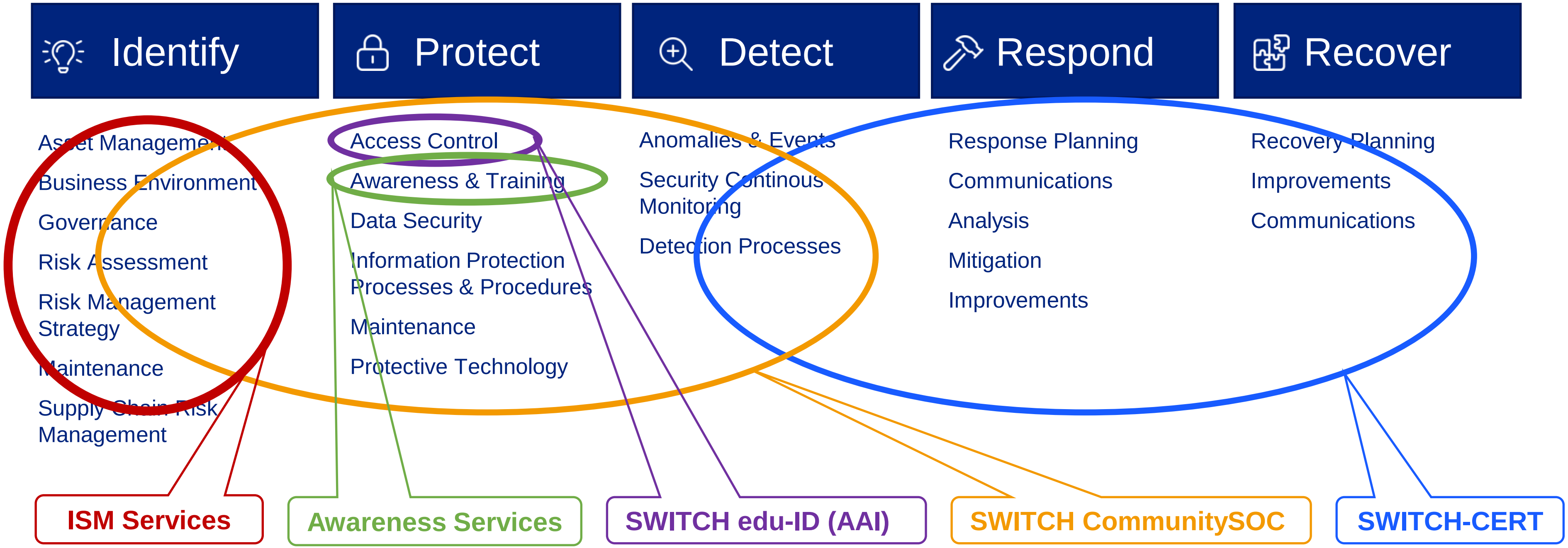
Incident Analysis & Coordination | Critical Threat Alerting

Network Security Monitoring | Domain Security | Malware Monitoring & Analysis | Industrial Control System Security | IoT Security

Awareness | Forensics | Info Services| Community Services | CSIRT-Trainings

National & International Cooperation Network

Security & identity services evolution



Identify

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy
- Maintenance
- Supply Chain Risk Management

Protect

- Access Control
- Awareness & Training
- Data Security
- Information Protection Processes & Procedures
- Maintenance
- Protective Technology

Detect

- Anomalies & Events
- Security Continous Monitoring
- Detection Processes

Respond

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Recover

- Recovery Planning
- Improvements
- Communications

ISM Services

Awareness Services

SWITCH edu-ID (AAI)

SWITCH CommunitySOC

SWITCH-CERT

Grown from less than 20 (2016) to more than 50 (2023) specialists

Questions?
Discussion!

Thank you for your interest.

Martin Leuthold
Head of Data, Security & Network
Deputy Managing Director

mobile +41 79 276 25 71
martin.leuthold@switch.ch

Disclaimer

SWITCH is liable neither for the completeness, accuracy, correctness and continuous availability of the information given, nor for any loss incurred as a result of action taken on the basis of information provided in this or any other SWITCH publication. SWITCH expressly reserves the right to alter prices or composition of products or services at any time.