

Security Nightmares 2.0

Ein Blick des EDUCV auf Sicherheitsprobleme
und -Albträume im letzten Jahr

Der EDUCV ist „eine Arbeitsgruppe operativer Informationssicherheitsteams, insbesondere Computer Emergency Response Teams (CERTs) und Computer Security Incident Response Teams (CSIRTs), deutscher Hochschulen, Lehr- und Forschungseinrichtungen.“

Kurzinformation

- Gründung als Subverbund des Deutschen CERT-Verbundes
- regelmäßiger Informations- und Erfahrungsaustausch
- Unterstützung sicherheitstechnischer Untersuchungen
- Konzeption und Entwicklung von Sicherheitslösungen

The same procedure as last year? -
The same procedure as every year James!


Same procedure as every year

Unsere regelmäßigen Plagegeister, mit denen wir uns beschäftigen müssen, ob wir wollen oder nicht!

- Phishing
 - Abwehr und Nacharbeiten von laufenden Phishing-Kampagnen
 - Abwicklung von kompromittierten Accounts
 - Warnungen bei gut gemachtem Phishing
 - Abuse-Meldungen bei Dienstleistern
 - Aufklärung
 - zum Beispiel durch Awareness-Kampagnen
 - In seltenen Fällen auch eine übermäßige Sensibilität, um unbequemen Inhalt von Rundmails zu ignorieren. „Ups, ich dachte das wäre Phishing/Spam“
- Angriffe auf Hochschulen und Universitäten
 - Lerneffekt und abklopfen der eigenen Systeme, sofern bekannt wurde, welche Angriffsvektoren genutzt wurden.


Same procedure as every year

30.03.2022, 09:29 Uhr

 > Cyberangriff: Technische Hochschule in Aschaffenburg offline

Cyberangriff: Technische Hochschule in Aschaffenburg offline

Die Technische Hochschule Aschaffenburg ist Opfer eines Cyberangriffs geworden. Wie die Hochschule auf ihrer Internetseite bestätigt, wurden vorsorglich alle Rechner heruntergefahren. Der Lehrbetrieb ist aktuell nur offline möglich.

Von  BR24 Redaktion

Same procedure as every year

Offline seit Pfingsten

Hackerattacke legt Pädagogische Hochschule in Freiburg lahm

Wegen eines «schwerwiegenden IT-Sicherheitsvorfalls» war die Pädagogische Hochschule in Freiburg tagelang offline. Bis das Problem behoben ist, müssen noch Hunderte Geräte neu aufgesetzt werden.

10.06.2022, 15:24 Uhr

20.03.2022, 09:29 Uhr

🏠 > Cyberangriff: Technische Hochschule in Aschaffenburg offline

Cyberangriff: Technische Hochschule in Aschaffenburg offline

Die Technische Hochschule Aschaffenburg ist Opfer eines Cyberangriffs geworden. Wie die Hochschule auf ihrer Internetseite bestätigt, wurden vorsorglich alle Rechner heruntergefahren. Der Betrieb ist aktuell nur offline möglich.

23.06.2022 12:38 | BUNDESLÄNDER > TIROL

Von  BR24 Redaktion

NACH HACKERANGRIFF

Daten als Ziel bei Attacke auf MedUni Innsbruck?

Same procedure as every year

CYBERATTACKE
Hackerangriff auf Wuppertaler Uni: Studierende können aufatmen
Keine Kommentare

3. August 2022 um 18:27 Uhr | Lesedauer: Eine Minute

Hackerattacke legt Pädagogische Hochschule in Freiburg lahm
Offline seit Pfingsten
SECURITY
Nach einem Hack ist die Pädagogische Hochschule in Freiburg lahm. Die Hochschule war die Pädagogische Hochschule. Hunderte Geräte neu.

Hackerangriff auf Hochschule Heilbronn
Nach einem Hack ist die Hochschule Heilbronn eingeschränkt per E-Mail erreichbar. Das LKA und die Cybersicherheitsagentur untersuchen den Vorfall.
3. November 2022, 10:56 Uhr, Moritz Tremmel

Cyberangriff: Technische Hochschule in Aschaffenburg offline
Die Technische Hochschule Aschaffenburg ist Opfer eines Cyberangriffs geworden. Wie die Hochschule auf ihrer Internetseite bestätigt, wurden vorsorglich alle Rechner heruntergefahren. Der Betrieb ist aktuell nur offline möglich.
23.06.2022 12:38 | BUNDESLÄNDER > TIROL

Hackerangriff auf Fachhochschule Münster
Stand: 23.06.2022, 18:26 Uhr
Die Fachhochschule Münster ist Opfer eines Hackerangriffs geworden. Die FH hat ihre Internetseite vom Netz genommen. Die Schäden sind aber wohl nicht so schlimm wie befürchtet.

NACH HACKERANGRIFF
Daten als Ziel bei Attacke auf MedUni Innsbruck?

Skurile Infrastruktur



"Der Betonmischer muss ins Internet."



"Ja, unser Gewächshaus schickt E-Mails an die Gärtnerin."

Fund des Schwachstellenscanners:

Detection Result

The "SunOS" Operating System on the remote host has reached the end of life.

```
CPE:                cpe:/o:sun:sunos:4.1
Installed version,
build or SP:        4.1
EOL date:           2003-09-01
```



- **Problem:** Kompromittierte Accounts an Unis sind leider kein Einzelfall . . .
- . . . aber jeder kompromittierte Account ist ein potentieller meldepflichtiger Datenschutzvorfall
- → führt zu länglichen Diskussionen mit den Kolleg:innen vom Datenschutz, ob wir jetzt wirklich **jeden** kompromittierten Account melden müssen

Falls jemand ein gutes Argument für uns hat, warum ein kompromittierter Account **kein** meldepflichtiger Datenschutzvorfall ist - bitte unbedingt nachher bei uns melden!

Proxy(Not)?Shell

- Neues Jahr neue Microsoft Exchange RCE
- Behoben durch Exchange Auto Reparatur Hexerei
- Zig Iterationen von minimal abweichenden RegEx

```
V1: {.*autodiscover\.json.*\@.*Powershell.*}  
V2: {.*autodiscover\.json.*Powershell.*}  
V3: {UrlDecode{.*autodiscover\.json.*Powershell.*}}  
[...]
```

- Der Patch war relativ schnell da
- Gut... “Relativ” schnell hieß in dem Fall halt 1,5 Monate
- und trotzdem...

Reports of ProxyNotShell Vulnerabilities Being Actively Exploited (CVE-2022-41040 and CVE-2022-41082)

December 21, 2022

According to reports, the zero-day vulnerabilities **CVE-2022-41040** and **CVE-2022-41082**, dubbed ProxyNotShell, are still being actively exploited.

Researchers published **proof-of-concept (PoC)** details after Microsoft patched the vulnerabilities in **October patch Tuesday**. Since the patch, the attackers still target vulnerable MS Exchange Server builds such as MS

Rackspace: Ransomware Attack Bypassed ProxyNotShell Mitigations

An external advisor to Rackspace told Dark Reading that Rackspace had held off on applying the ProxyNotShell patch amid concerns over reports that it caused "authentication errors" that the ...

Dark Reading · 18d

Jetzt patchen! Noch 60.000 Exchange-Server für ProxyNotShell

Admins von Exchange-Servern sollten sicherstellen, dass die Sicherheitsupdates ...
Angriffe an mehreren Lücken ansetzen und Systeme ...

Proxy(Not)?Shell cont.

- Auch vor zwei Wochen erschienen immer noch Artikel die dringend zum Patchen raten
- Zeitnahes Patchen scheint ein generelles Problem zu sein

Der EDUCV besteht aus

- DFN-CERT, Hamburg
- KIT-CERT, Karlsruhe
- WWU-CERT, Münster
- RUS-CERT, Stuttgart
- TUD-CERT, Dresden
- GU-CERT, Frankfurt
- FUB-ART, Berlin
- ZIM-CERT, Duisburg/Essen
- JMU-CERT, Würzburg

Sie finden uns unter

<https://www.educv.de>

