Security Nightmares 2.0

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

EDUCV

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

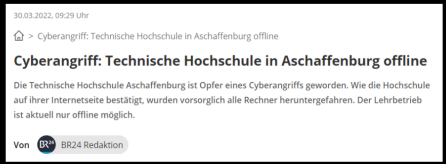
The same procedure as last year? -
The same procedure as every year James!

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

Same procedure as every year

Skurile Infrastruktur

"Der Betonmischer muss ins Internet."

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

Mehr skurile Infrastruktur

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

SUN 4/260

Spaß mit dem Datenschutz

- **Problem:** Kompromittierte Accounts an Unis sind leider kein Einzelfall ...
- ... aber jeder kompromittierte Account ist ein potentieller meldepflichtiger Datenschutzvorfall
- $\rightarrow$ 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!

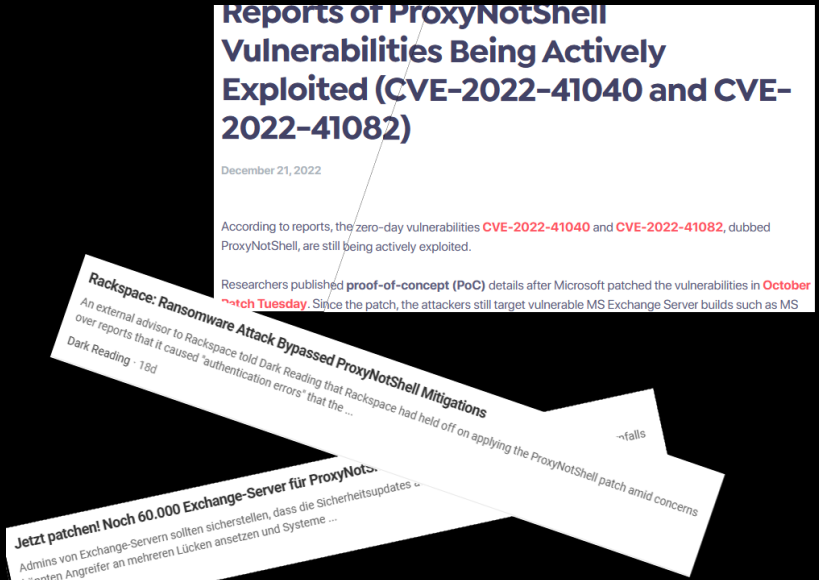
Proxy(Not)?Shell

- 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. . .

Proxy(Not)?Shell cont.



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