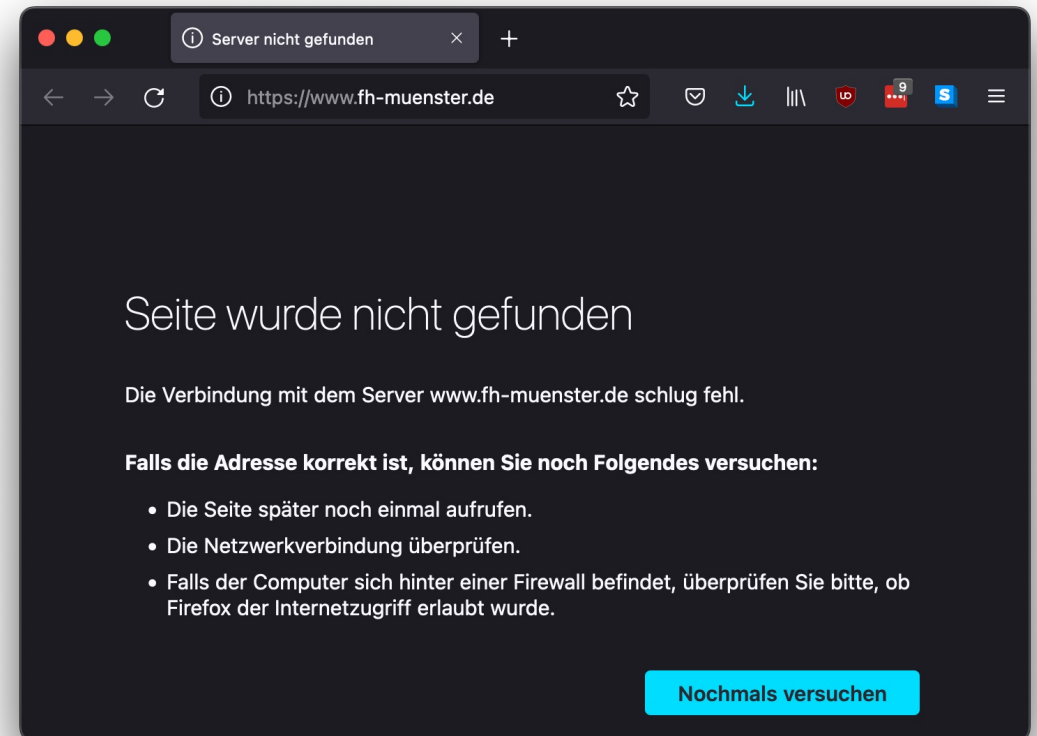




FH MÜNSTER
University of Applied Sciences

Der Cyberangriff gegen die FH Münster im Juni 2022

Prof. Dr. Sebastian Schinzel





FH MÜNSTER
University of Applied Sciences

The image shows a YouTube video player interface. The video title is "Der Cybervorfall an der FH Münster im Juni 2022" by Prof. Dr. Sebastian Schinzel, recorded on 10.11.2022. The video player shows a play button in the center of the video frame. The video frame itself has a blue and white striped background. The video player controls at the bottom show a progress bar at 0:00 / 57:41, a volume icon, and a play button. The video player is set to HD quality. The video player interface includes the YouTube logo, a search bar, and a menu icon. The video player also shows the channel name "FH Münster" with 2390 subscribers and a "Abonnieren" button. The video player also shows a like button with 81 likes, a share button, and a save button.

YouTube DE Suchen

FH MÜNSTER University of Applied Sciences

Der Cybervorfall an der FH Münster im Juni 2022

Prof. Dr. Sebastian Schinzel
Vortrag vom 10.11.2022

<https://fh-muenster.de/it-sicherheit>

0:00 / 57:41

Cybervorfall an der FH Münster im Juni 2022 - Vortrag Prof. Dr. Sebastian Schinzel

FH Münster 2390 Abonnenten Abonnieren

81 Teilen Speichern

https://www.youtube.com/watch?v=I_UzKlBLY-Q



Düsseldorf. Eine kleine Unachtsamkeit hat Continental ins Chaos gestürzt. Weil ein einzelner Mitarbeiter einen nicht autorisierten Browser aus dem Internet heruntergeladen hat, sei es Cyberkriminellen möglich gewesen, 40 Terabyte an Daten des Autozulieferers zu „exfiltrieren“. Das hat der IT-Sicherheitschef des Konzerns, [REDACTED] in einem internen Webcast gesagt, den das Handelsblatt einsehen konnte.

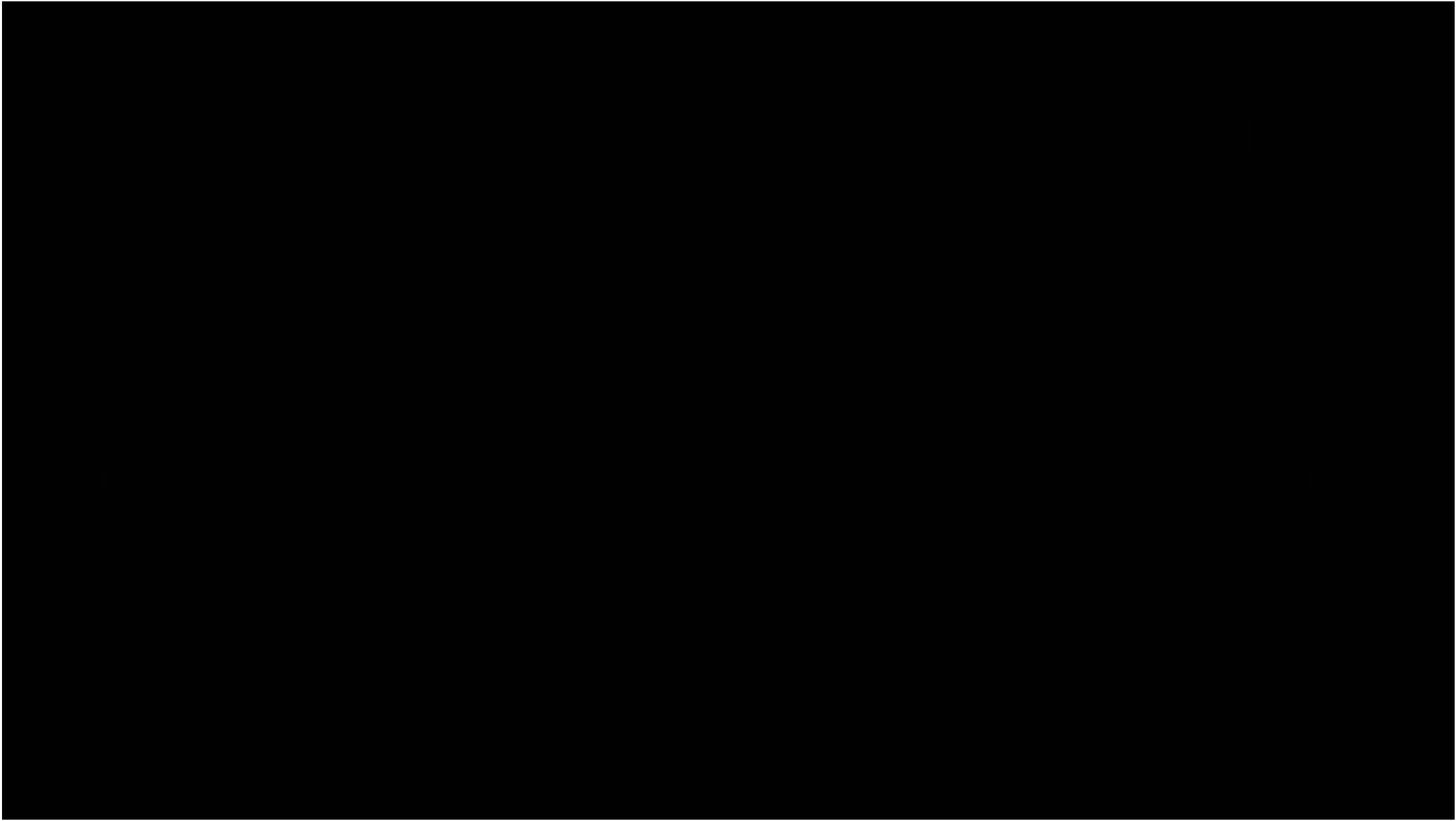
<https://www.handelsblatt.com/technik/cybersecurity/continental-so-haben-mitarbeiter-dem-hackerangriff-den-weg-geeignet/28865720.html>



Kill Chain und Mitre ATT&CK



Die Mitre ATT&CK-Matrix hat fünf Taktiken.



***LOL* :-)**



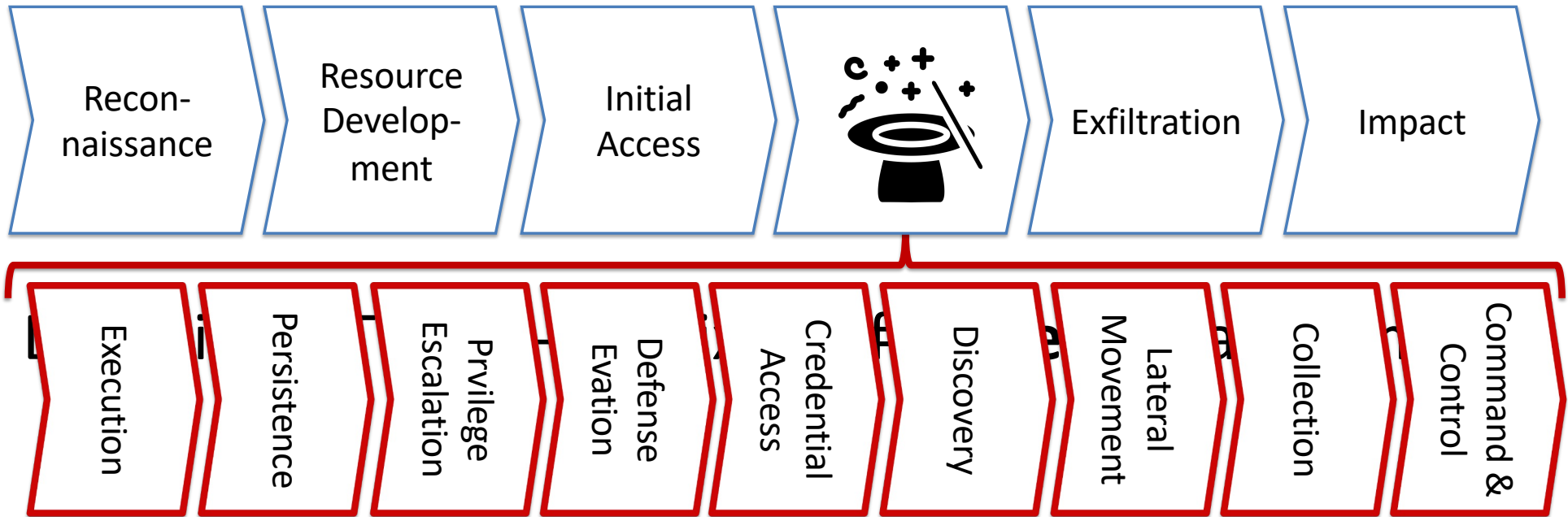
Kill Chain und Mitre ATT&CK



Die Mitre ATT&CK-Matrix hat ~~fünf~~ **sechs** Taktiken.

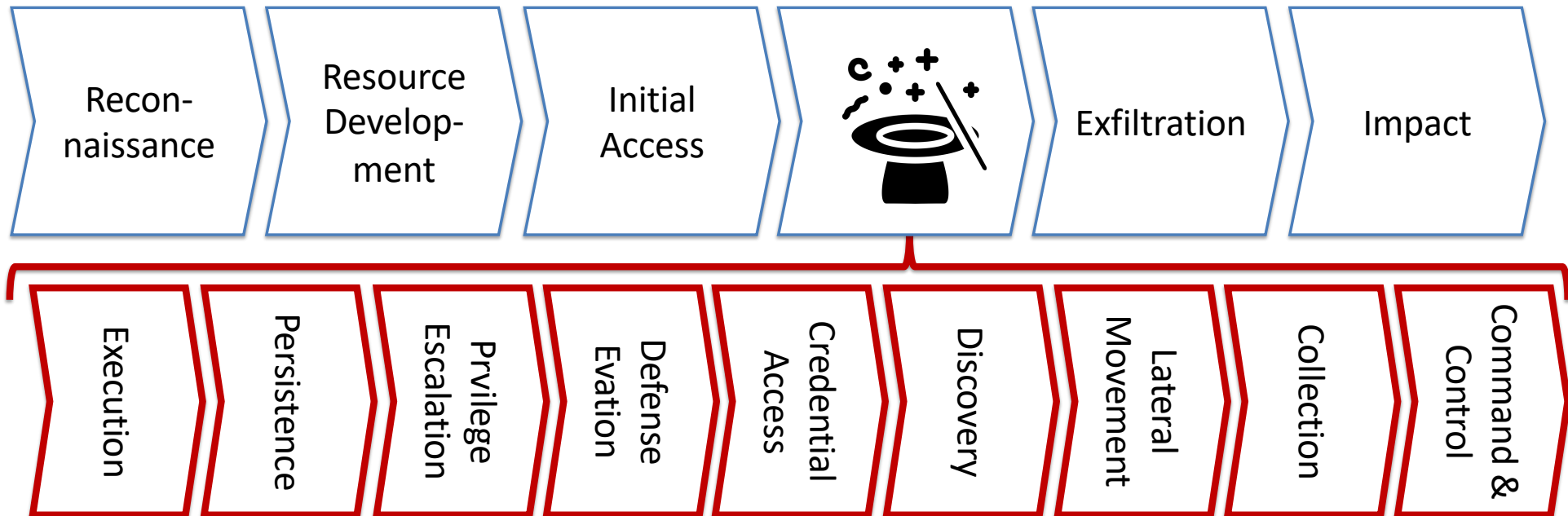


Kill Chain und Mitre ATT&CK





Kill Chain und Mitre ATT&CK



Die Mitre ATT&CK-Matrix hat ~~fünf~~ **sechs** Taktiken.
vierzehn



1. Zugriff über VPN und gestohlenen Benutzerkonten (Studierende, Mitarbeitende).
2. Dann Scannen von Intranet.
3. Detektion durch fehlgeschlagene Loginversuche.
4. Sperren des Benutzerkontos.
5. ...
6. goto 1;



- MFA-Authentifizierungsdienst:
 - technisch praktisch fertig, aber
 - noch nicht ausgerollt.
- Jump-Host für administrativen Zugriff auf Server:
 - technisch praktisch fertig, aber
 - noch nicht ausgerollt.
- Rahmenvertrag mit Incident Response-Dienstleister:
 - abgeschlossen,
 - On-boarding abgeschlossen.



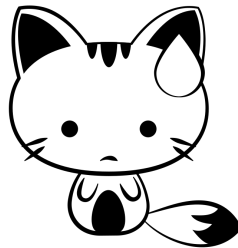
Der 20. Juni 2022

Traffic-Anomalie aufgefallen, Incident Response gestartet.

Ergebnisse:

- Angreifer bekamen Zugriff auf Domain-Admin-Konto.
- Laterale Bewegung auf Windows Active Directory und die Windows Domain Controller.
- Mutmaßlich Export aller Benutzer-Konten.
- Hintertüren der Angreifer gefunden und deaktiviert...

- Sh*t.





Der 21. Juni 2022

- Bilden von Krisenstäben
- Entscheidungsfindung: wie geht es weiter? (Prüfungsphase und Einschreibephase stehen unmittelbar bevor)?





Passwort-Reset von 18.000 Konten

- Einmal-Passwort an priv. Post- und E-Mail-Adresse
 - Geburtsdatum als „zweiter Faktor“
- Schalten einer „Hotline“
- Passwort-Reset-Container an allen großen Campus
 - Personalausweis, Reisepass
- Video-Ident.

Der 30. Juni 2022



FH MÜNSTER
University of Applied Sciences

FH Münster Hüfferstraße 27 48149 Münster

- persönlich/vertraulich -

ETI | ST
Sebastian Schinzel

Der Kanzler

Aktuelle Informationen werden regelmäßig
über www.meinefh.de zur Verfügung gestellt.

Münster, 29.06.2022

Sofortiger Passwort-Reset

Liebe Kolleg*innen, sehr geehrte Damen und Herren,

wie intensiv kommuniziert, wurde die FH Münster Opfer eines Cyberangriffs. Die aktuellen Passwörter verlieren ab Samstag, 02. Juli, im FH-Netz ihre Gültigkeit. Dies erfordert zwingend, dass alle Nutzer*innen ihre Passwörter ändern. Lesen Sie bitte den Brief vollständig, bevor Sie Ihr Passwort – möglichst **sofort** – ändern. Wir bitten Sie um folgende Vorgehensweise:

1. Über das WLAN (eduroam) oder das kabelgebundene Netz der FH funktioniert der Passwort-Reset nicht. **Setzen Sie Ihr Passwort über einen Computer oder ein mobiles Endgerät mit einem alternativen vertrauenswürdigen Internetzugang zurück.**
2. Die **Passwortänderung erfolgt über eine FH-Website**. Diese leitet Sie durch den Passwort-Reset.
3. Bitte ändern Sie umgehend Ihr Passwort.
4. Bitte den Link in den Browser eingeben oder den **QR-Code** scannen, um die Website zu erreichen:

Link: <https://myfh.fh-muenster.de/reset>

Einmalpasswort: aUVyR1R1MwtFUmV2VdhCT3BodFU1QT09
(wird während des Vorgangs benötigt)



5. Vergeben Sie ein **neues, sicheres Passwort**. Verwenden Sie niemals alte Passwörter oder Passwörter, die Sie auch in anderen Logins (privater E-Mail Zugang, Amazon etc.) benutzen. Ihr neues Passwort muss **mindestens 12 Zeichen** lang sein und **einen Kleinbuchstaben, einen Großbuchstaben, eine Ziffer und ein Sonderzeichen** enthalten.

Sie haben an Ihrem ersten Arbeitstag nach dem 02. Juli 2022 Ihr Passwort nicht geändert? **Verbinden Sie auf keinen Fall Ihr Dienstgerät mit der Dockingstation, LAN oder WLAN.** Informieren Sie sich zur weiteren Vorgehensweise auf www.meinefh.de/passwort.

Dieses Schreiben ist eine Vorabinformation m. d. B. um Passwortanpassung bereits vor dem 02. Juli 2022. In Kürze erhalten Sie ein inhaltsgleiches Schreiben auch an Ihre Privatadresse. Wenn Sie Ihr Passwort geändert haben, müssen Sie auf das Schreiben per Brief nicht reagieren.

Wir bitten um Verständnis für diese Unannehmlichkeiten und bedanken uns für Ihre Mithilfe!

Mit freundlichen Grüßen
Ihr Präsidium



- VPN-Zugriff nur mit MFA für alle.
- Strikte Umstellung auf MS Multi-Tier-Modell.
- Zugriff auf zentrale Server nur über dedizierte Clients, mit dedizierten Benutzerkonten.
- Administrativer Zugriff auf Server nur über Jump-Host.
- Zusätzliches manuelles Offline-Backup.
- Hilfreiche Tools: Bloodhound, Pingcastle.



Besondere Herausforderungen:

- Kommunikationssysteme (inkl. E-Mail und Mattermost) nur noch am Campus verfügbar.
- Offizielle Kommunikation über Signal App:
 - Vorteile: Datenschutz gewährleistet, komplett losgelöst von FH-Infrastruktur, Vermeidung von „Wildwuchs“.
 - Nachteile: private Telefonnummern, Dateiaustausch umständlich, Welche Nummer hat welche Person?
- Interne Informationsflüsse?
- Kommunikation mit Studierenden?



FH MÜNSTER
University of Applied Sciences

Ablenkung & Prokrastination



Cobalt Strike

**Security
Awareness
Training
Penetration-
tests**

Mimikatz



Security Awareness an der FH Münster

Studis, Mitarbeitende schulen

- Reduziert Initial Access.
- Holt Zielgruppe „mit ins Boot“.

Aber:

- Weiterhin gestohlene Zugangsdaten, klicken auf böartige Anhänge & Links!
- Gutes Gefühl: „man tut was“

Die folgenden acht einfachen Schritte unterstützen Sie bei der Identifizierung von Phishing-E-Mails. Bestenfalls reichen bereits die ersten beiden Schritte. Sobald Sie in einem der Schritte misstrauisch werden, handelt es sich um eine Phishing-E-Mail und Sie brauchen die folgenden Schritte nicht.

- Tipp 1: Absender prüfen
- Tipp 2: Links mit "Mouse-over" prüfen
- Tipp 3: Die "Domäne" einer Webadresse
- Tipp 4: Irreführende Rechtschreibfehler in Domäne
- Tipp 5: Der "Google-Test"
- Tipp 6: E-Mail digital signiert?
- Tipp 7: Anhang plausibel?
- Tipp 8: Passwort-Manager verwenden



Penetration Testing an der FH Münster

[Startseite](#) > [Unsere Hochschule](#) > [Modernes Management](#) > [IT-Sicherheit](#)

Sicherheitsüberprüfung

Das Informationssicherheitsteam bietet für kostenfrei die Möglichkeit, Laborgeräte und Systeme zu untersuchen. Auf dieser Seite finden Sie ein

Kontaktdaten

Name *

E-Mailadresse *

Anfragetext *

Internes Angebot, kostenlos Pentests durchzuführen

- Wird sehr gut angenommen
- Reduziert Sicherheitslücken
→ erhöht Gesamtsicherheit.

Aber:

- Weiterhin >0 Sicherheitslücken vorhanden.
- Gutes Gefühl: „man tut was“



Krisenkommunikation

PM Präsident der FH Münster [FH-Bedienstete] IT-Sicherheit: Signiert

[→ see english version below](#)

Liebe Studierende, liebe Kollegen und Herren,

wie gestern bereits angekündigt, aktualisieren wir die Prozessoren unter Hochdruck und externer Unterstützung über <https://meinefh.de> informiert. Eine Telefonhotline ist eingerichtet.

Wir bemühen uns um Ihr Verständnis.

Mit freundlichen Grüßen
Ihr Präsidium

Dear students, dear colleagues,

As announced yesterday...

Quicklinks

Kontakt
Pressestelle
Hüfferstraße 27,
48149 Münster
Raum: B 126

Tel: 0251 83-64090
pressestelle@fh-muenster.de

FH Münster r... massiven Hack

FH Münster: Nahezu normale Präsenzprüfungen finden wie geplant statt

Die Hochschule schaltet dem Internet verbunden gehend ab – eine Info...
nefh.de ist eingerichtet

Hochschulbetrieb, Vorlesungen, Veranstaltungen und Forschung laufen an...
plant statt. (Foto: FH Münster)

[\(Download\)](#)

Münster (24. Juni 2022). Am Dienstag hatte sich die...
entschieden, die Hochschulsysteme vom Internet ab...
angriff, den die IT-Spezialist*innen der FH Münster...
Die FH Münster hatte und hat aber jederzeit vollen Z...

Münster (22. Juni 2022). Aufgrund eines massiven Hackerangriffs san...

PM Präsident der FH Münster 24. Juni 2022 um 18:29

[FH-Bedienstete] Aktuelle Lage: Details zum IT-Sicherheitsvorfall un... [Details](#)

An: FH-Bedienstete & 6 weitere

Sicherheit: Signiert (GRP - Praesident)

[→ see english version below](#)

Liebe Studierende, liebe Kolleg*innen, sehr geehrte Damen und Herren,

eine ereignisreiche Woche liegt hinter uns. Wir sind, wie bereits viele andere Institutionen und Hochschulen in der letzten Zeit leider auch schon, Opfer eines IT-Angriffs geworden.

Was ist eigentlich beim IT-Sicherheitsvorfall passiert?

Im Kern haben wir Gewissheit, dass unbekannte Angreifer*innen Zugriff auf die zentrale Benutzer*innenverwaltung der FH Münster erlangt haben. Dabei konnten sie die Zugangsdaten aller aktiven FH-Benutzer*innen stehlen. Konkret sind das jeweils Vorname und Nachname, E-Mailadresse der FH inklusive Alias, akademischer Titel und Passwort-Hash. Diese Information wurde bereits an das Landesamt für Datenschutz gemeldet. Es muss daher angenommen werden, dass die Angreifer*innen über den Passwort-Hash auch Ihr Passwort erraten können. Das war einer der Hauptgründe, warum wir die Netze der FH vom Internet getrennt haben.

Was bedeutet dies für Sie?

Wir arbeiten in verschiedenen fachlichen Krisenstäben mit Hochdruck daran, unsere IT-Infrastruktur wieder ans Laufen zu kriegen und stehen dazu rund um die Uhr in engem Austausch mit unseren hochschuleigenen IT-Spezialist*innen, externen Berater*innen eines IT-Security-Dienstleisters



Krisenkommunikation

Viele Unklarheiten an der FH

WN 22.06.2022

Wann genau der Cyberangriff stattgefunden habe, könne aktuell ebenso wenig gesagt werden, wie wann die Probleme behoben sein werden. "Wir befinden uns aktuell noch in der Analyse und arbeiten mit Hochdruck an einer Lösung", sagt Pressesprecher [redacted]. Die Attacke auf die IT der Fachhochschule fand allerdings wahrscheinlich am Dienstag statt. Seitdem treten Probleme im System der FH auf.

WN+ Etwas Frust und viel Solidarität

WN 30.06.2022


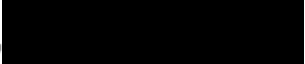
Was der Hackerangriff auf die FH für Studierende bedeutet

Münster - Die FH ist Opfer eines Hackerangriffs geworden. Die Hochschule arbeitet eifrig daran, ihre Netze wieder mit dem Internet verbinden zu können. Doch was heißt das für die Studierenden? Zwei Studentinnen schildern die Situation aus ihrer Sicht. Von Pjer Biederstädt

ter handelt. Schon
ten Unbekannte das
s vereinzelte

oder warum die FH
ner [redacted]



Düsseldorf. Eine kleine Unachtsamkeit hat Continental  ins Chaos gestürzt. Weil ein einzelner Mitarbeiter einen nicht autorisierten Browser aus dem Internet heruntergeladen hat, sei es Cyberkriminellen möglich gewesen, 40 Terabyte an Daten des Autozulieferers zu „exfiltrieren“. Das hat der IT-Sicherheitschef des Konzerns,  in einem internen Webcast gesagt, den das Handelsblatt einsehen konnte.

<https://www.handelsblatt.com/technik/cybersecurity/continental-so-haben-mitarbeiter-dem-hackerangriff-den-weg-geeignet/28865720.html>



Zusammenfassung

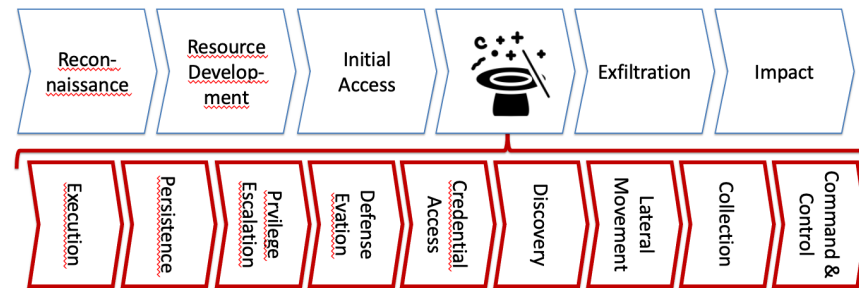
Diskussion! Fragen?

Prof. Dr. Sebastian Schinzel

schinzel@fh-muenster.de

@seecurity@infosec.exchange

<https://fh-muenster.de/it-sicherheit>



Die MITRE ATT&CK-Matrix hat ~~fünf~~ ~~sechs~~ Taktiken.

vierzehn

