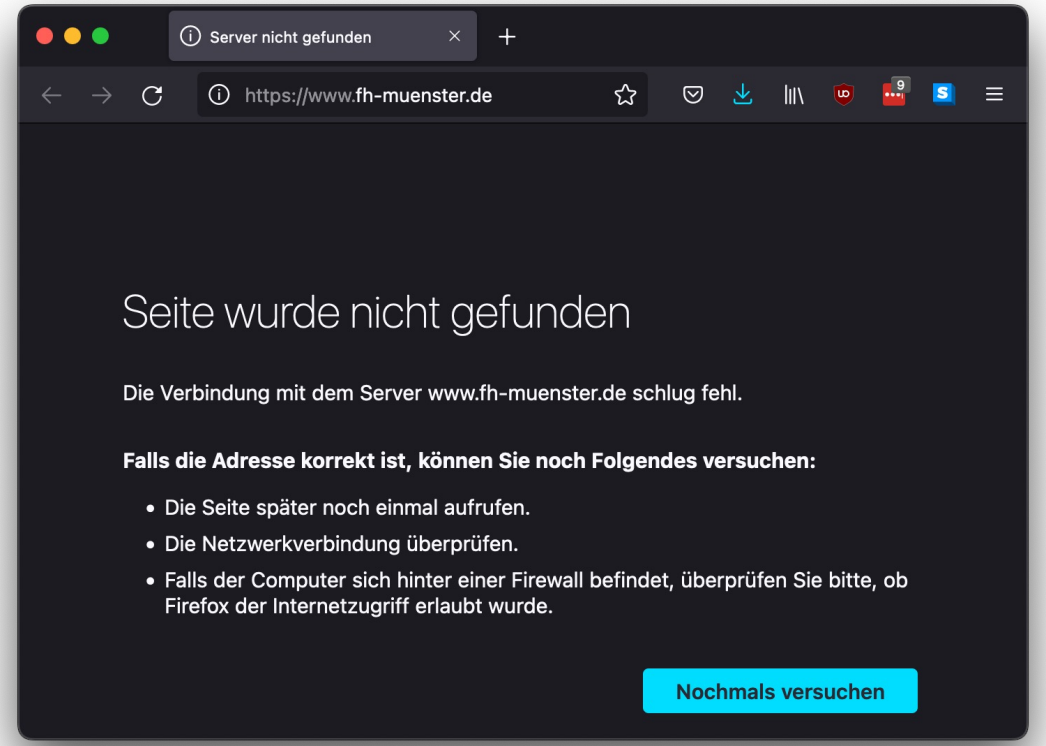
FH MÜNSTER
University of Applied Sciences

Der Cyberangriff gegen die FH Münster im Juni 2022

Prof. Dr. Sebastian Schinzel



FH MÜNSTER
University of Applied Sciences

https://www.youtube.com/watch?v=l_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-geebnet/28865720.html

Kill Chain und Mitre ATT&CK

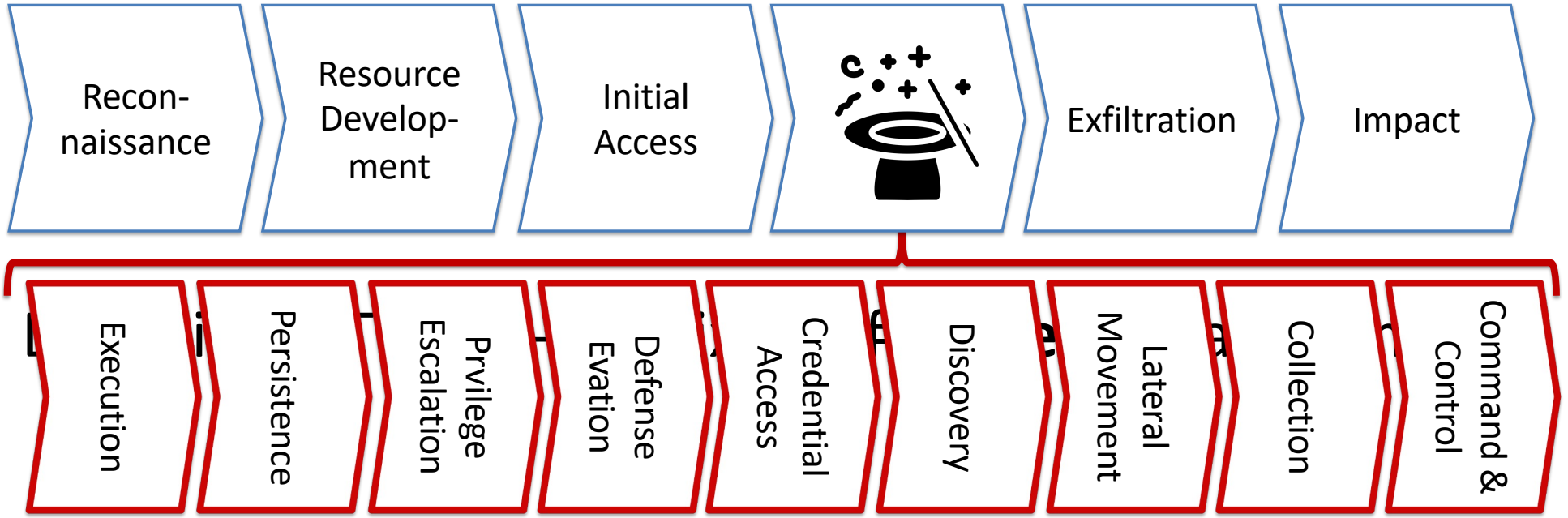
Die Mitre ATT&CK-Matrix hat fünf Taktiken.


LOL :-)

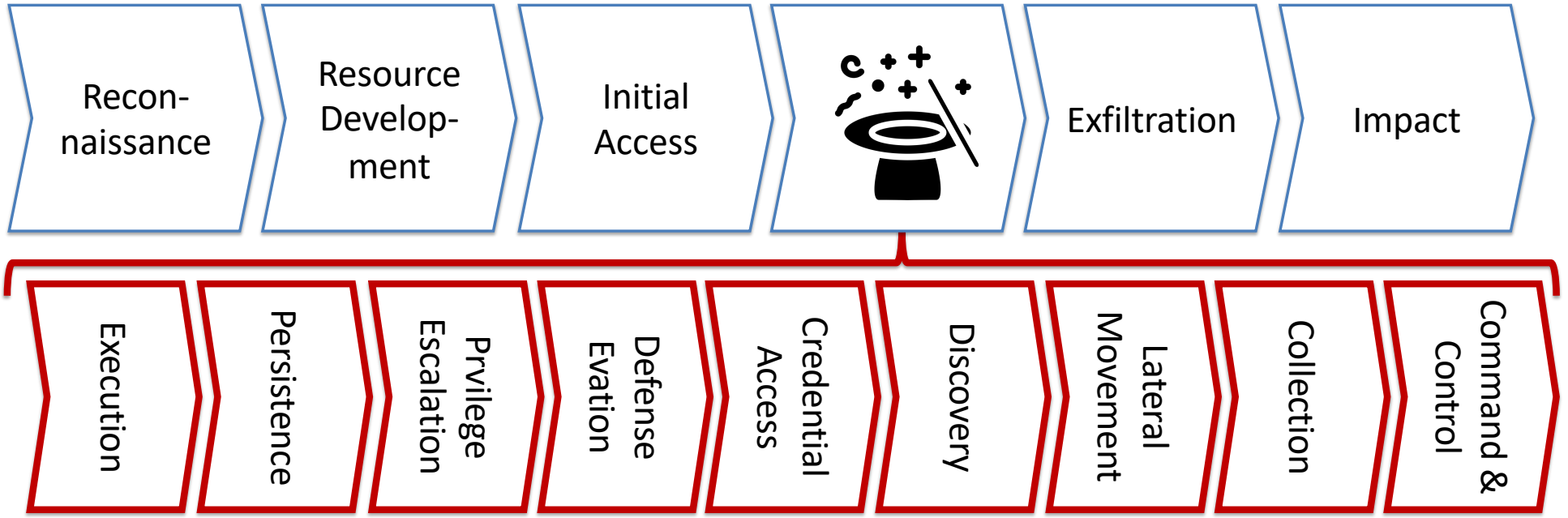
Kill Chain und Mitre ATT&CK

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

Der Mai 2022

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;

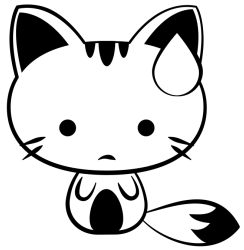
Hinter den Kulissen

- 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 Controler.
- Mutmaßlich Export aller Benutzer-Konten.
- Hintertüren der Angreifer gefunden und deaktiviert…
- Sh*t.



Der 21. Juni 2022

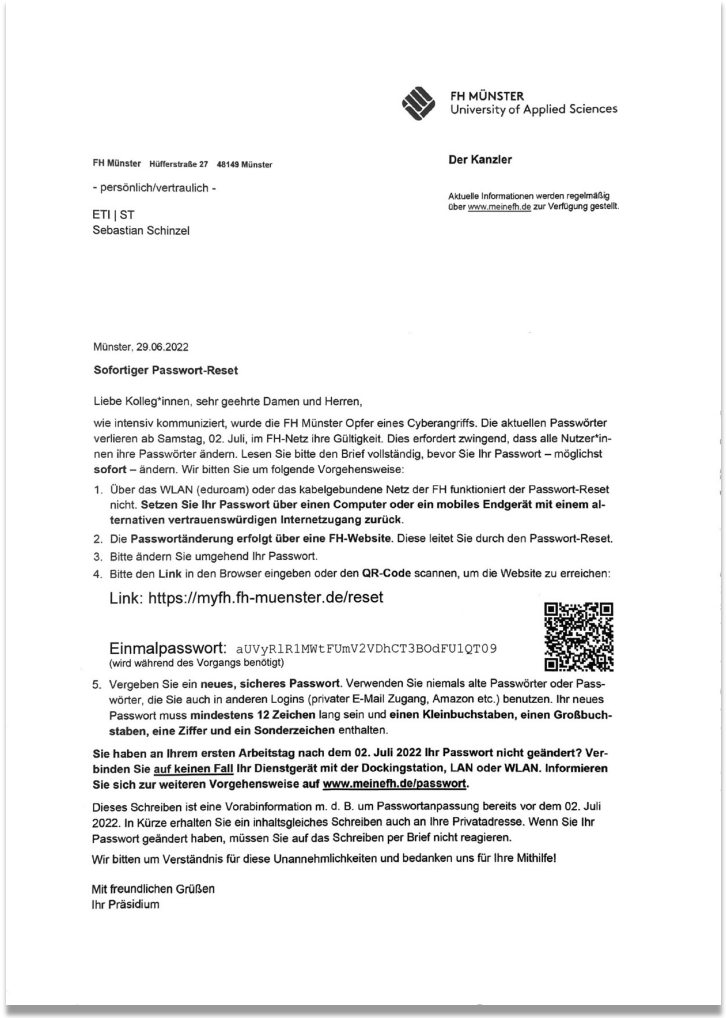
- Bilden von Krisenstäben
- Entscheidungsfindung: wie geht es weiter? (Prüfungsphase und Einschreibephase stehen unmittelbar bevor)?

FH MÜNSTER
University of Applied Sciences

Der 30. Juni 2022

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.



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: `aUVyRlR1MWtFUmV2VDhCT3BOdFU1QT09`
   (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

Post-Incident

- 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.

Der Wiederaufbau

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

FH MÜNSTER
University of Applied Sciences

Security Awareness an der FH Münster

Studis, Mitarbeitende schulen

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

<u>Aber:</u>

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


Die folgenden acht einfachen Schritte unterstützen Sie bei
E-Mails. Bestenfalls reichen bereits die ersten beiden Schrit
Sobald Sie in einem der Schritte misstrauisch werden, hanc
Phishing-E-Mail und sie brauchen die folgenden Schritte ni

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

FH MÜNSTER
University of Applied Sciences

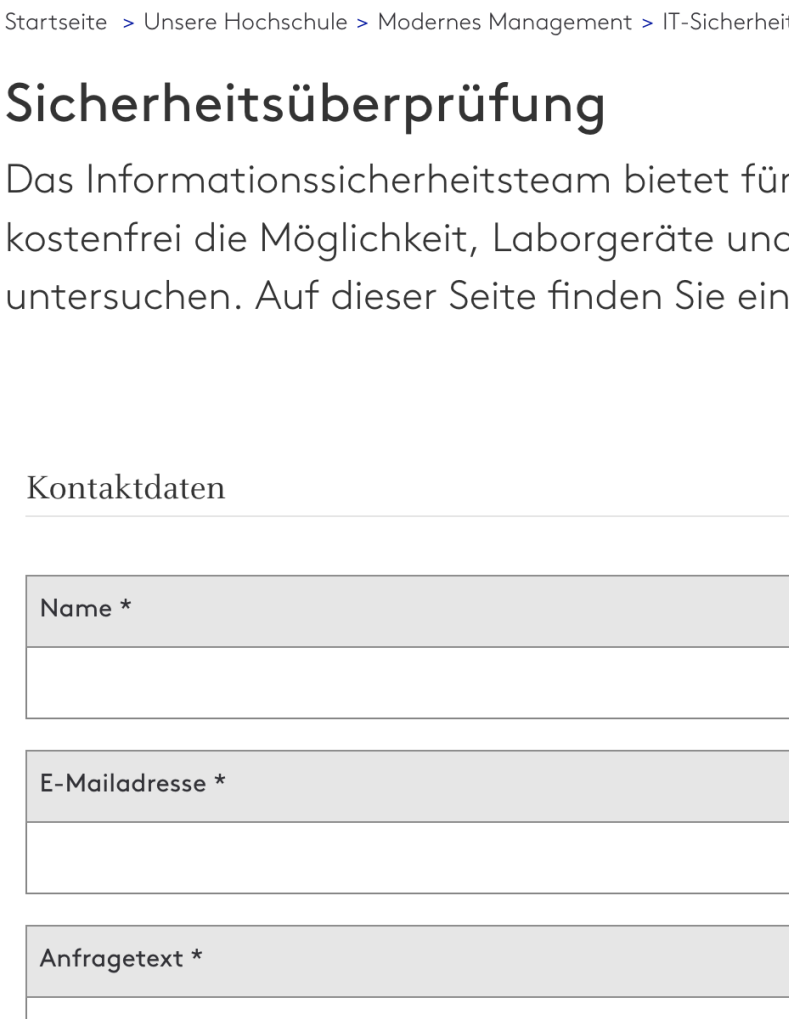
Penetration Testing an der FH Münster

Internes Angebot, kostenlos Pentests durchzuführen

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

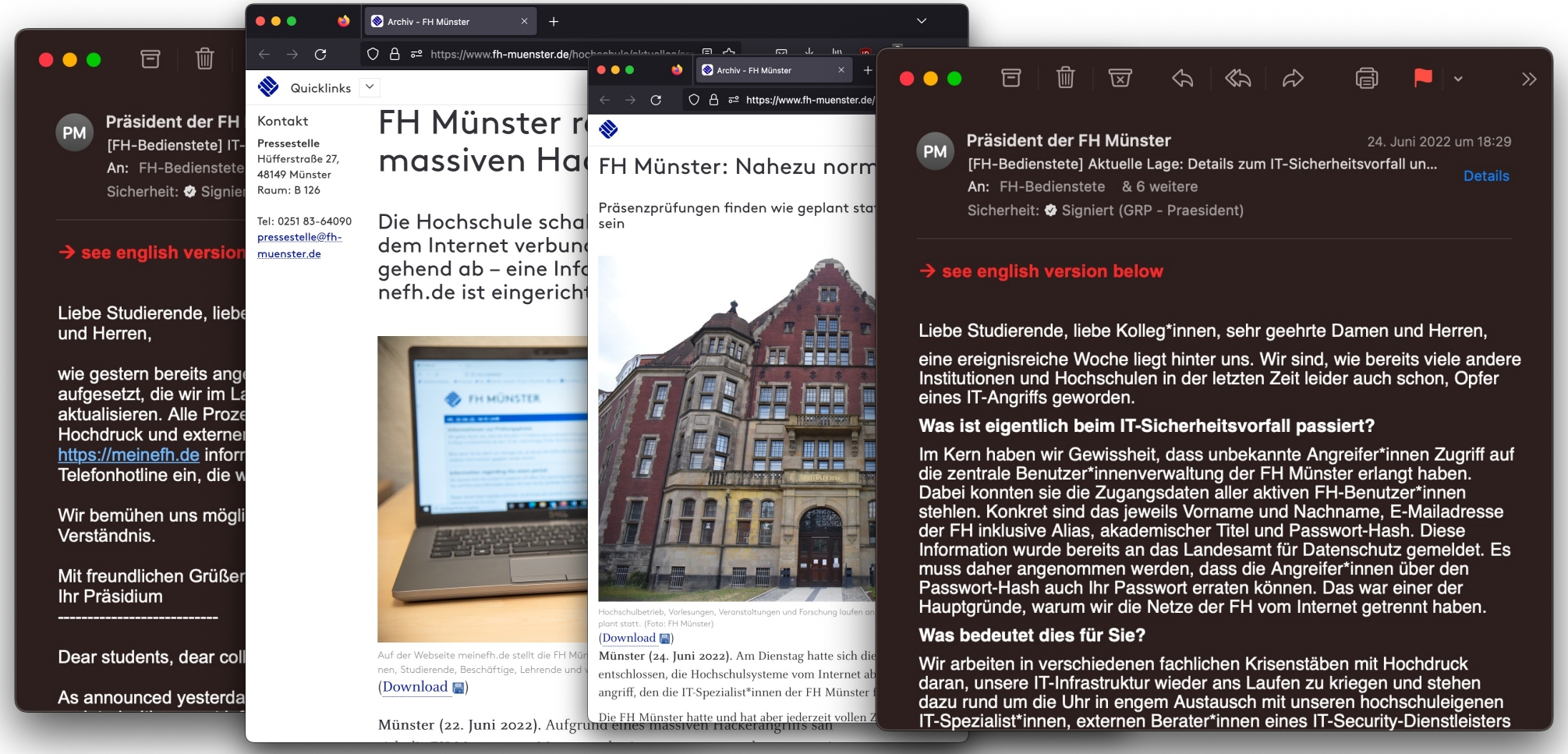
<u>Aber:</u>

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



FH MÜNSTER
University of Applied Sciences

Krisenkommunikation



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]

FH MÜNSTER
University of Applied Sciences

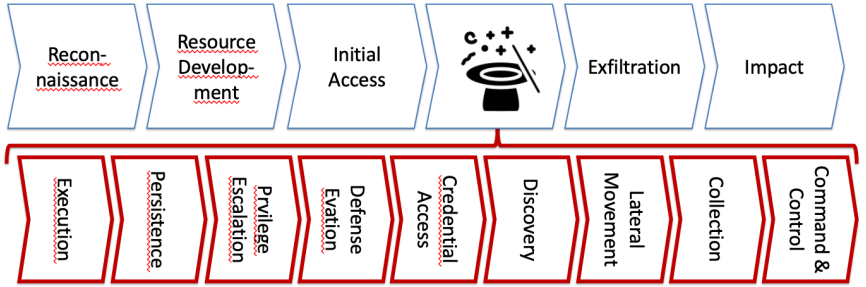
Krisenkommunikation

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-geebnet/28865720.html

FH MÜNSTER
University of Applied Sciences

Zusammenfassung



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

Diskussion! Fragen?

Prof. Dr. Sebastian Schinzel

schinzel@fh-muenster.de
@seecurity@infosec.exchange
https://fh-muenster.de/it-sicherheit