HOCHSCHULEN IM VISIER

Cybersicherheit im Spannungsfeld von Forschung & Lehre

18. Oktober 2023

79. DFN-Betriebstagung

Hendrik Walter
Geschäftsführer avency GmbH

avency

MIT SICHERHEIT GUT BERATEN!

Vorwort

Ein Zitat

„[...] Wir müssen die politische und organisatorische Verantwortung für die Sicherheit der von uns angewendeten Informationstechnologien erkennen und entsprechend handeln. Dabei muss der aufscheinende Interessenskonflikt zwischen der von uns allen geforderten Handlungsfreiheit im Bereich Lehre und Forschung und den Belangen der notwendigen Sicherheit erörtert und eine beiden Seiten gerecht werdende, angemessene Lösung erreicht werden.

Die Situation im IT-Bereich der Hochschulen spitzt sich, ohne übertreiben und Ängste hervorrufen zu wollen, deutlich zu. Die Zahl der Zwischenfälle häuft sich, was mit Sicherheit zu internen Auseinandersetzungen führt, darüber hinaus aber dem Ansehen der Hochschulen in der Öffentlichkeit schadet. [...]“

Dr.-Ing. H. Schultz
Ehem. Kanzler der Bauhaus-Universität Weimar
Ehem. Bundessprecher

IT-Sicherheit an Hochschulen
Erarbeitet durch den ZKI-Arbeitskreis IT-Sicherheit
Oktober **2005**

Einstieg in die Thematik

Cybersicherheit im Spannungsfeld von Forschung & Lehre

Welches Risiko besteht für die Rechte der Betroffenen, wenn wir eine KI-basierte Antimalware Lösung einführen und gesicherte Verbindungen entschlüsseln?

Das ist eine sehr wichtige Frage!

Und welches Risiko besteht für die Rechte der Betroffenen, wenn wir es nicht tun?

avency

Interessenkonflikte

Ein typisches Gespräch

Wir müssen effektive IT-Sicherheitsmaßnahmen einführen, um die Hochschule vor Cyberangriffen zu schützen!

Die Interessen des Personals und der Datenschutz müssen oberste Priorität haben!

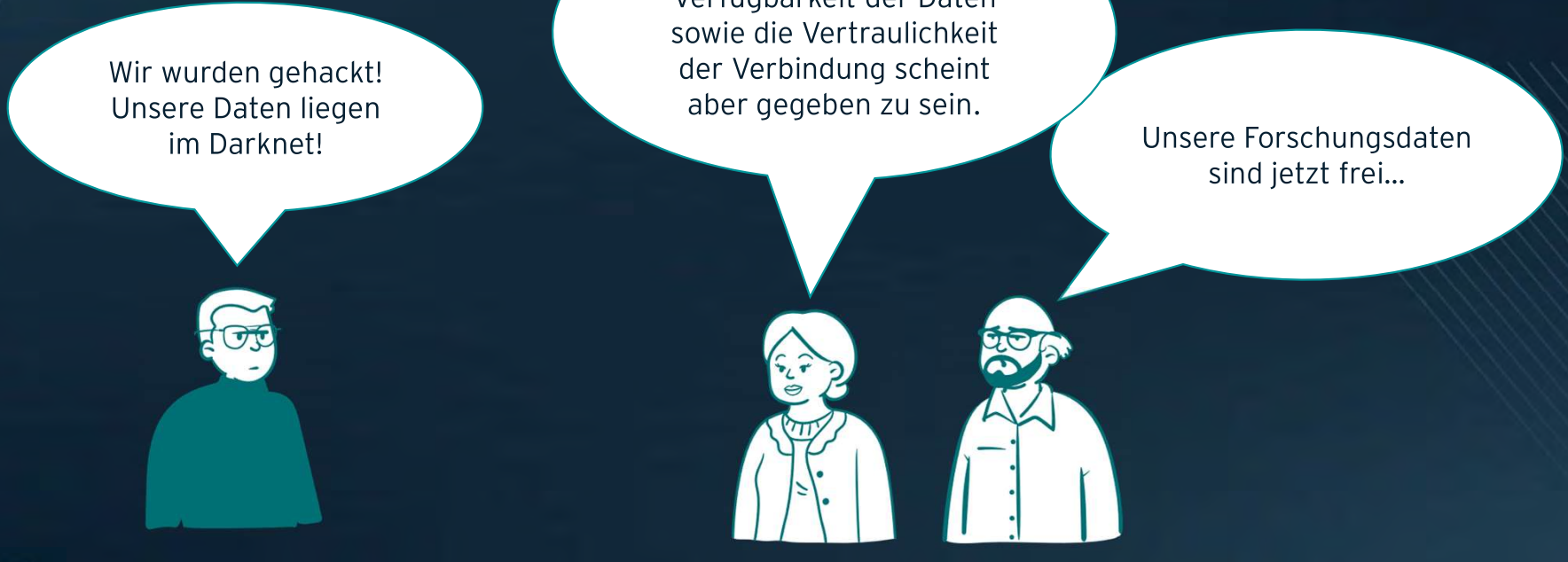
Wir müssen sparen!

Die Freiheit und Integrität von Forschung & Lehre muss jederzeit gewährleistet sein!

avency

Kurze Zeit später...

Post Mortem

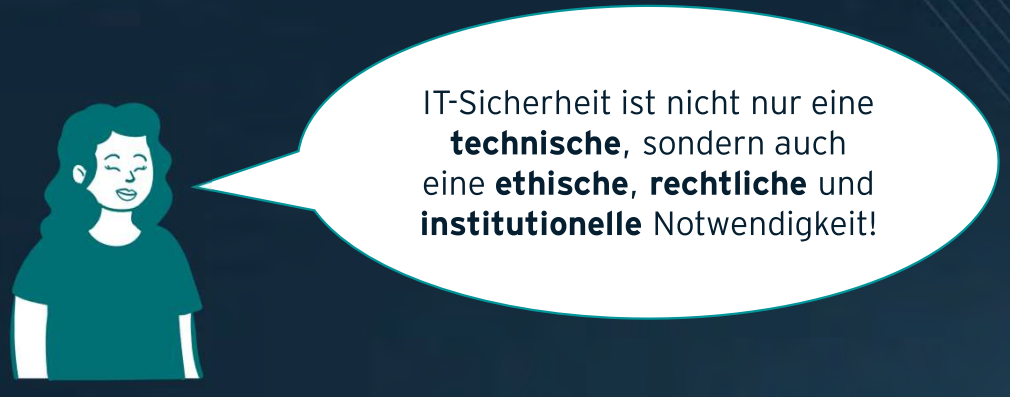


IT-Sicherheit ist nicht optional

Warum IT-Sicherheit an Hochschulen unverzichtbar ist

- Datenschutz: Sicherstellung des Schutzes persönlicher und sensibler Daten
- Rechtliche Compliance: Einhaltung gesetzlicher und regulatorischer Vorgaben (DSGVO, IT-SiG)
- Forschungsschutz: Wahrung der Integrität und Vertraulichkeit wissenschaftlicher Daten.
- Reputation: Schutz des institutionellen Ansehens und Vertrauens.
- Systemintegrität: Gewährleistung eines sicheren und störungsfreien Betriebes.

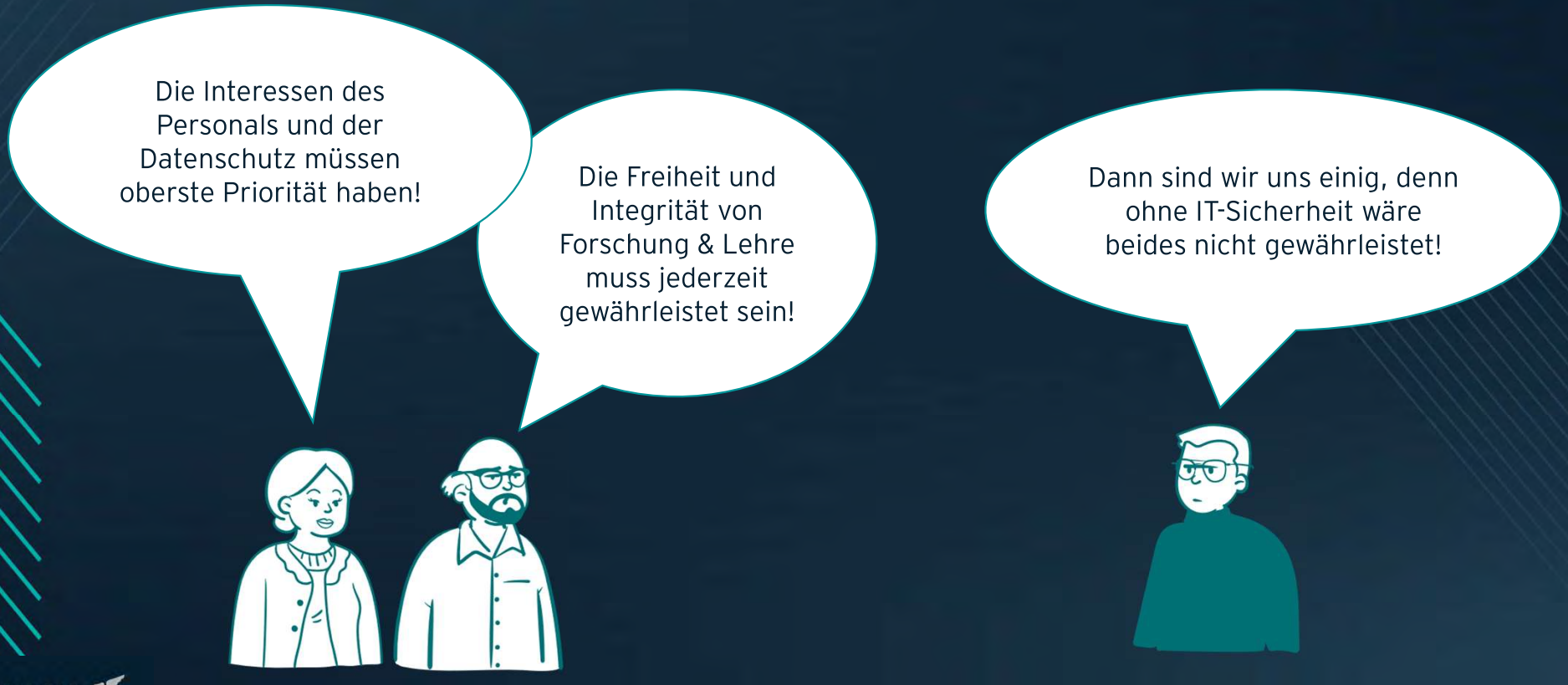
Es muss allen Beteiligten klar sein:



avency

Die Interessenkonflikte auflösen

Ein gemeinsames Ziel



avency

Ein gemeinsamer Weg

Überwindung von Vorbehalten gegenüber IT-Sicherheit an Hochschulen

- Transparenz: Offene Kommunikation der Sicherheitsziele und -methoden.
- Beteiligung: Einbeziehung der Gemeinschaft in Entscheidungsprozesse.
- Bildung: Schulungen zur Vermittlung der Bedeutung der IT-Sicherheit.
- Differenzierung: Angepasste Sicherheitsniveaus für verschiedene Bereiche.
- Datenschutz: Klarheit und Strenge bei Datenschutzpraktiken.

Das gemeinsame Ziel:

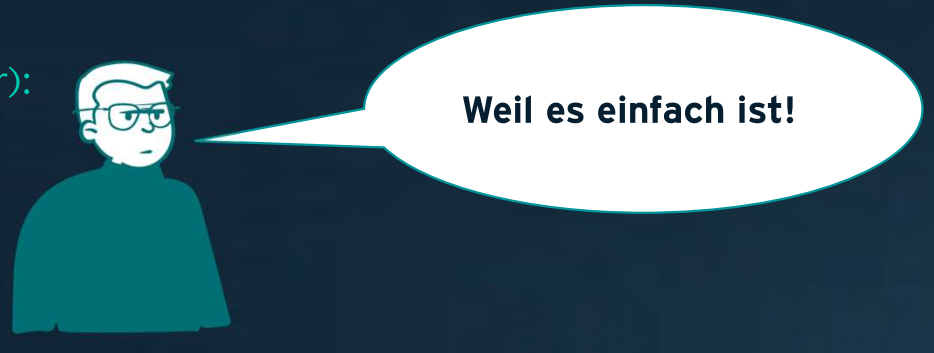
Eine ausgewogene Strategie, die IT-Sicherheit mit Respekt für Autonomie und Privatsphäre verbindet!

Hochschulen im Visier

Warum werden ausgerechnet Hochschulen vermehrt angegriffen?

- Offene (IT-) Strukturen
- Historische Begebenheiten (Wofür gibt es eigentlich diese privaten IP-Adressen?)
- Komplexe Systeme
- Vielfältige Aufgabengebiete in Forschung und Lehre
- Viele unerfahrene und wechselnde Anwender (Phishing)
- Unmengen an wertvollen Daten – von Studierenden, Lehrenden, der Belegschaft und Forschung.

Der Hauptgrund ist aber (leider):



avency

Hochschulen im Visier

Anatomie eines typischen Angriffs (durch aktives Zutun eines Nutzers)

1. Phishing-E-Mail an Hochschul-Nutzer
2. Nutzer trägt seine Nutzerkennung und Passwort auf Phishing Seite ein
3. Angreifer hat Zugriff auf interne Systeme (z.B. via VPN)
4. Privilege-Escalation durch Ausnutzung von Sicherheitslücken
5. Installation von Backdoor. Nachladen von Schadcode
6. Network Scan, Lateral Movement & Infektion weiterer Systeme
7. Windows System mit Domain-Admin Kennung im Cache gefunden (LSASS Dump)
8. Übernahme des AD-Forrest und Infektion der gesamten Umgebung
9. Datendiebstahl, Verschlüsselung und Erpressung

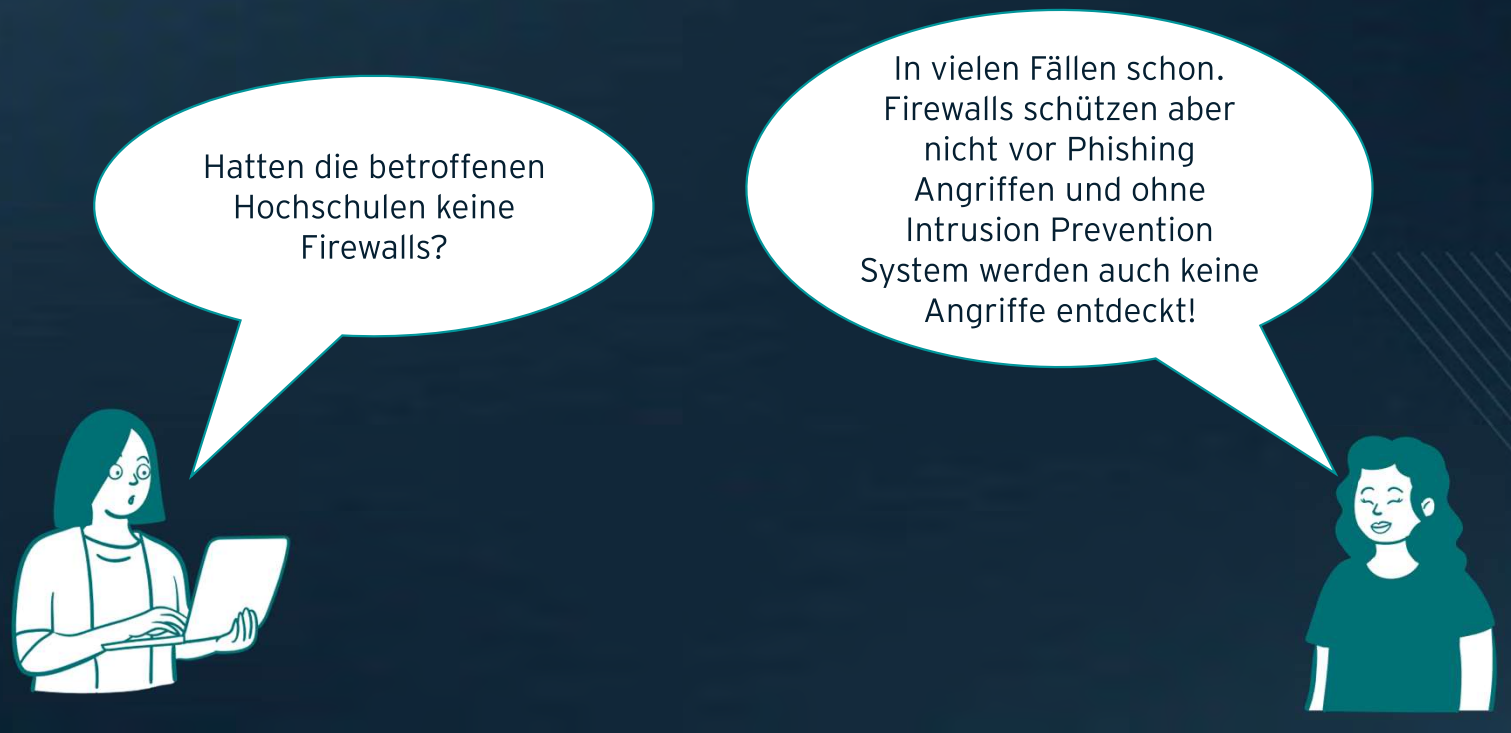
Hochschulen im Visier

Anatomie eines typischen Angriffs (ohne aktives Zutun eines Nutzers)

1. Vulnerability Scan von Online-Diensten der Hochschule
2. Sicherheitslücke (z.B.) in Citrix Netscaler/Exchange Server gefunden und ausgenutzt
3. Rootkit installiert und Schadcode nachgeladen
4. Netzwerkscan, Lateral Movement, Übernahme weiterer Systeme
5. Auffinden von Credentials eines LDAP Service Accounts (mit Domain-Admin Rechten)
6. Übernahme des AD-Forrest
7. Infektion aller Systeme, Datendiebstahl, Ransomware, Erpressung...

Hochschulen im Visier

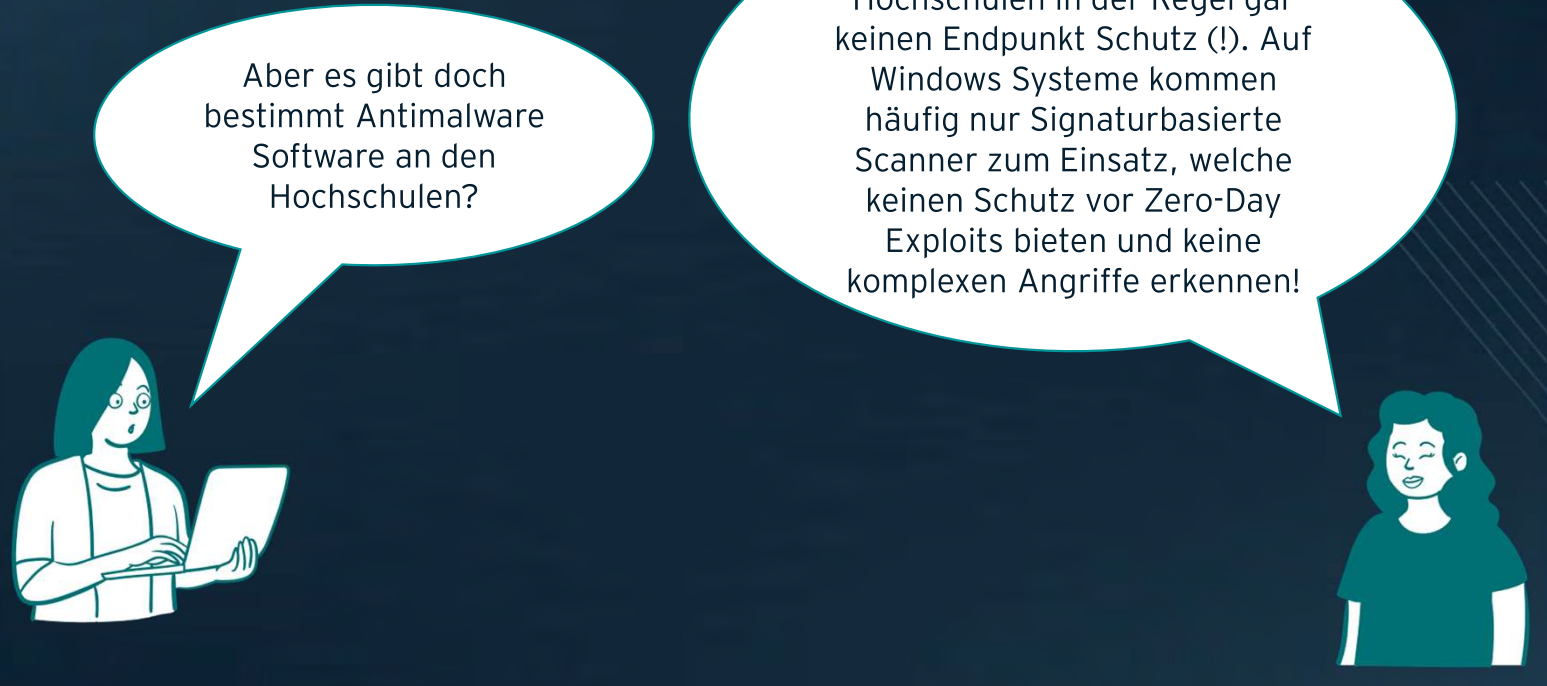
Anatomie eines typischen Angriffs



avency

Hochschulen im Visier

Anatomie eines typischen Angriffs

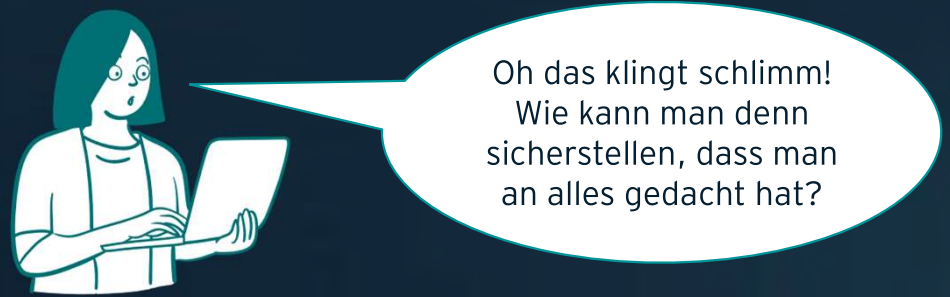


Warum ist es so einfach?

Weil viele Hochschulen hinsichtlich IT-Sicherheit immer noch zu wenig unternehmen!

Die häufigsten Fehler:

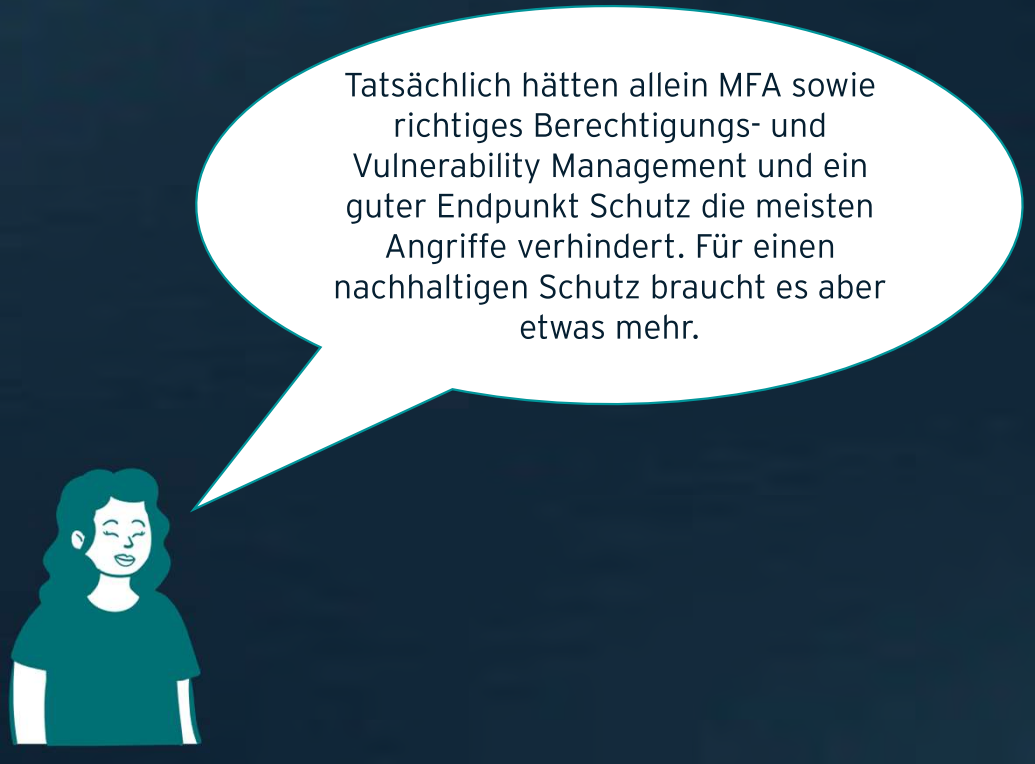
- Kein flächendeckender Einsatz von 2-Faktor-Auth/MFA (Remote-Access/VPN, IT-Management)
- Falscher Umgang mit Administratorberechtigungen (Service Accounts/Domain Admins etc..)
- Schlecht konfigurierte sowie ungepatchte Systeme (Kein einheitliches Endpoint-Mangement / XEM)
- Keine Netzwerksegmentierung per NextGen-Firewall, häufig nur rudimentäre ACL auf Routern
- Kein zeitgemäßer Endpunkt-Schutz (Signaturen schützen nur noch sehr begrenzt)
- Keine DNS-Sicherheit (Damit ist nicht DNSSEC gemeint!)



avency

Warum ist es so einfach?

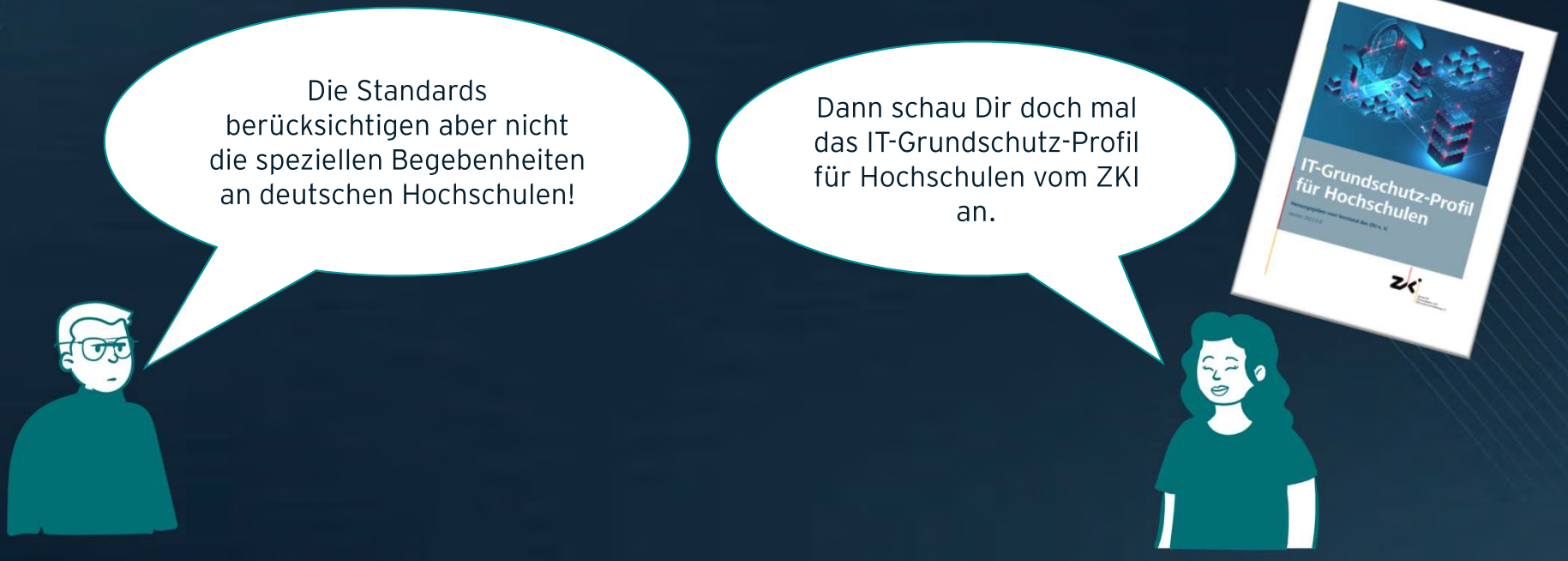
Weil viele Hochschulen hinsichtlich IT-Sicherheit immer noch zu wenig unternehmen!



Lösungsansätze

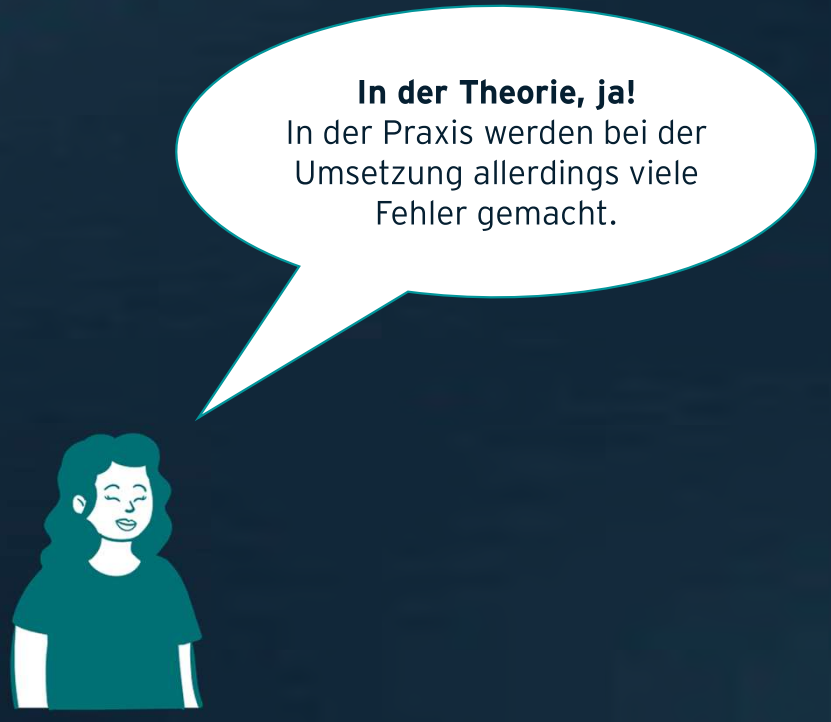
Wie können Hochschulen sich effektiv und nachhaltig schützen?

IT-Sicherheit sollte auf Basis von etablierten Standards (BSI/ISO/NIST/CIS) aufgebaut werden!



So einfach ist das also?

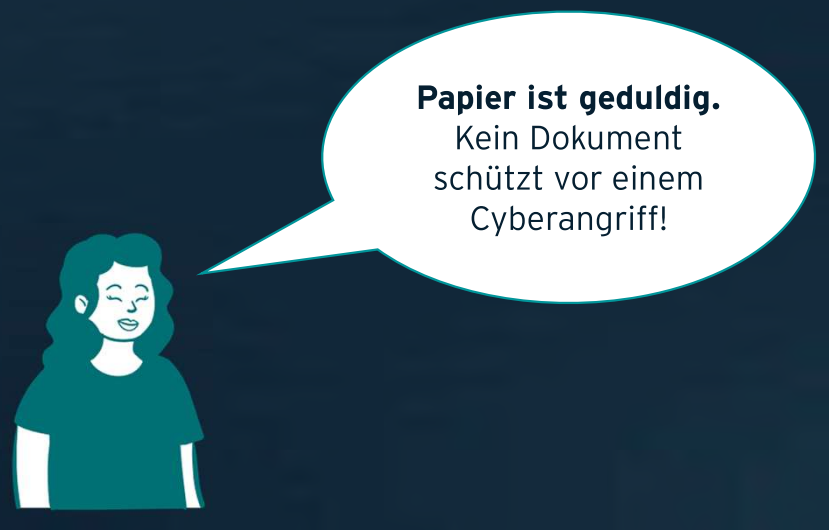
Bausteine fand ich schon als Kind toll!



Fehler bei der Umsetzung des IT-Grundschutzes

Worauf man unbedingt achten sollte

- Vollständigkeit: Es müssen alle Basis-Anforderungen (mindestens) umgesetzt werden.
- Genauigkeit der Umsetzung: Die Bausteine müssen sorgfältig in die Praxis umgesetzt werden.
- Priorität: Zuerst die Basis Hausaufgaben machen. XDR, SIEM, SOC & Co. ist (nur) die Kür!



avency

Fehler bei der Umsetzung des IT-Grundschutzes

BSI-zertifizierte Produkte?

Brauchen wir eigentlich eine BSI-zertifizierte Firewall?

Nein!
Einige Hersteller werben zwar gerne mit einer „BSI-Zertifizierung“ aber das BSI ist eine Common Criteria Zertifizierungsstelle und der Standard ist international.
Der IT-Grundschutz empfiehlt eine **Zertifizierung nach Common Criteria** (alt: EAL4+, neu: cPP for Network Devices 2.2).

IT-Grundschutz | NET.3.2 Firewall

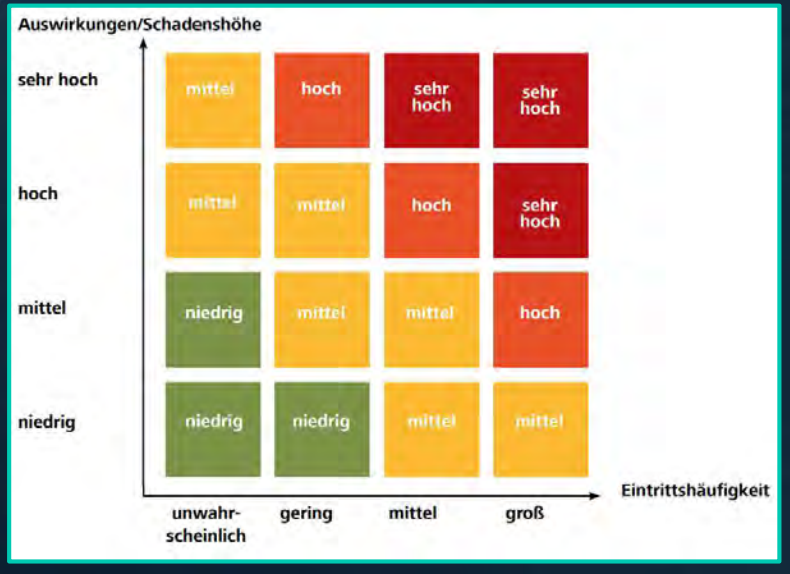
NET.3.2.A31 Einsatz von zertifizierten Produkten (H)

Firewalls mit einer Sicherheitsevaluierung nach Common Criteria SOLLTEN eingesetzt werden, mindestens mit der Stufe EAL4.

Fehler bei der Umsetzung des IT-Grundschutzes

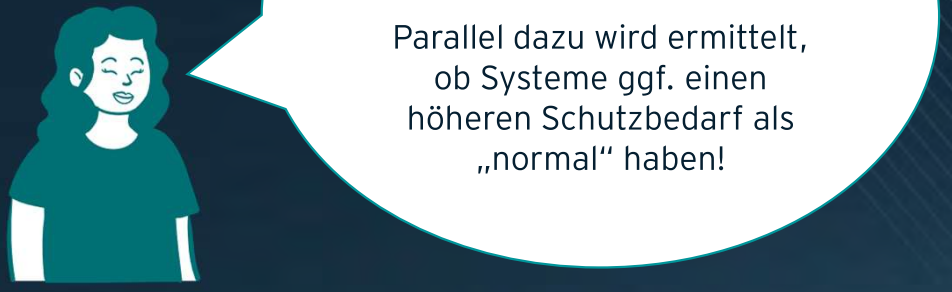
Wie sie uns an Hochschulen häufig begegnen

Schutzbedarfskategorien	Beschreibung
„normal“	Die Schadensauswirkungen sind begrenzt und überschaubar.
„hoch“	Die Schadensauswirkungen können beträchtlich sein.
„sehr hoch“	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.



Bildquelle: ZKI – IT-Grundschutz-Profil für Hochschulen

Müssen wir jetzt erst den Schutzbedarf aller Systeme ermitteln, bevor wir mit der praktischen Umsetzung der Bausteine beginnen können?



avency

Beispiel: ZKI IT-Grundschutz-Profil

Übergeordneten Bausteine

Das sind die wichtigsten übergeordneten Bausteine zur Cyberabwehr und ausgerechnet hier sind viele Hochschulen nicht gut aufgestellt.

Prio	Sicherheits-management	Organisation und Personal	Konzepte und Vorgehensweisen	Betrieb	Detektion und Reaktion
R1	Sicherheits-management **ISMS.1**	Organisation **ORP.1** Personal **ORP.2** Sensibilisierung und Schulung zur Informationssicherheit **ORP.3** Identitäts- und Berechtigungsma-nagement **ORP.4**	Datensicherungs-konzept **CON. 3** Löschen und Vernichten **CON. 6**	Ordnungsgemäße IT Administration **OPS.1.1.2.** Patch- und Änderungsmanagement **OPS.1.1.3.** Schutz vor Schadprogrammen **OPS.1.1.4.** Protokollierung **OPS.1.1.5** Software-Tests und -Freigaben **OPS.1.1.6**	

Gute Sache aber einer klickt immer drauf!

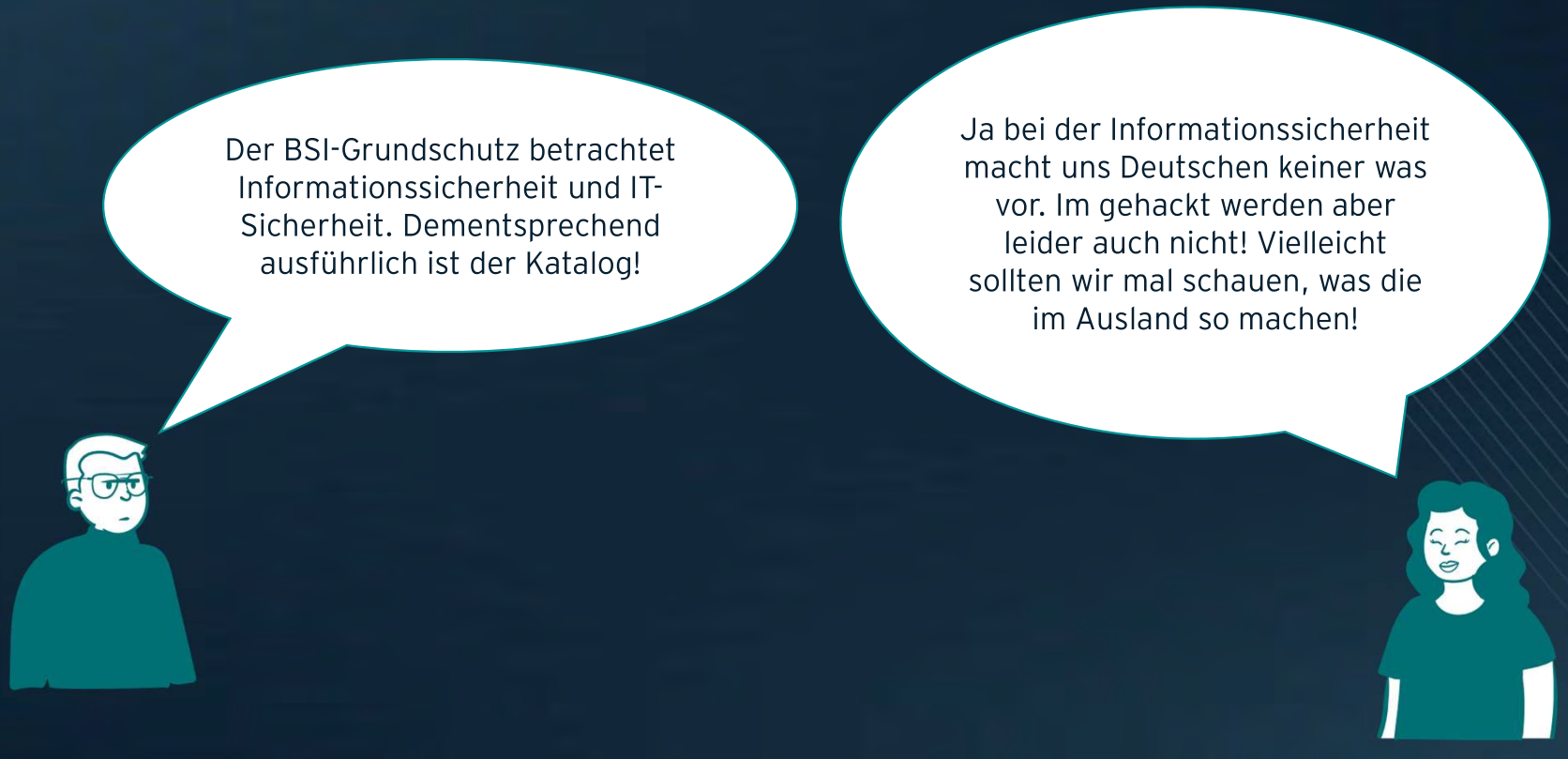
Einige beschäftigen sich intensiv mit Detektion und Reaktion (Prio R2/3), obwohl sie den Betrieb noch gar nicht im Griff haben.

Viele sind hier relativ weit. Das ist auch sehr wichtig (daher R1). Es verhindert in der Praxis aber kaum einen Angriff!

avency

Weitere Frameworks / Best Practices

Mit Fokus auf den sicheren Betrieb



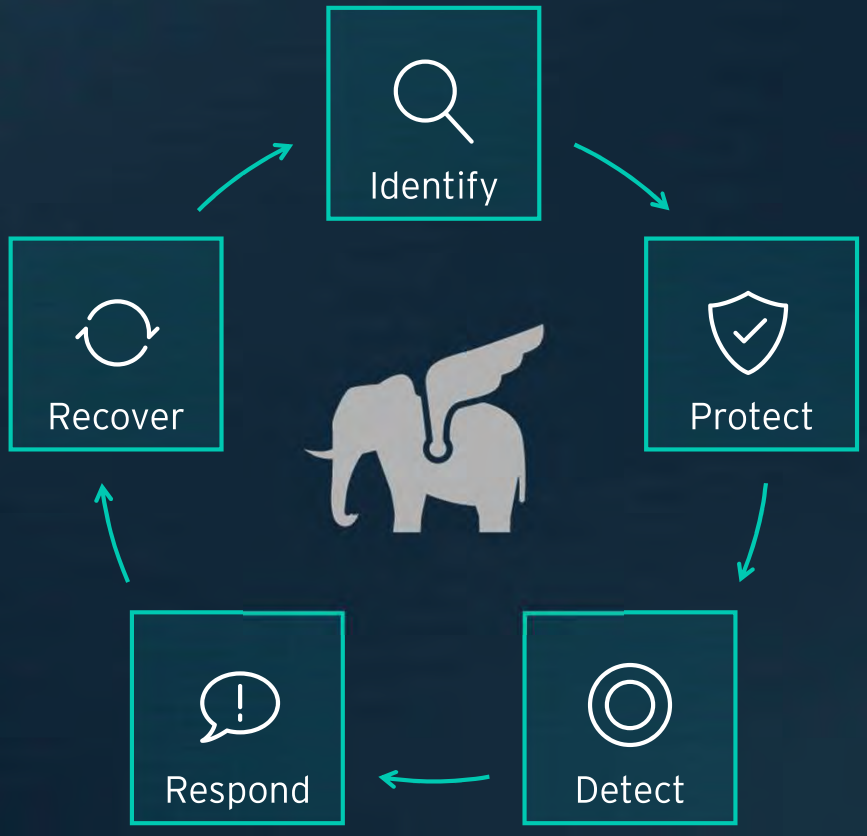
Das NIST Cybersecurity Framework (aus den USA)

Ein Framework nur für Cybersicherheit

- Fokus auf IT-Sicherheit
- Schnelle Umsetzung und Adaption möglich
- Klarer Fokus auf das Wesentliche (5 Hauptbausteine)
- Leicht und verständlich
- Lifecycle Gedanke
- 48 Seiten NIST vs. 858 Seiten BSI

Das avency (NIST)

CYBERSECURITY Framework



avency

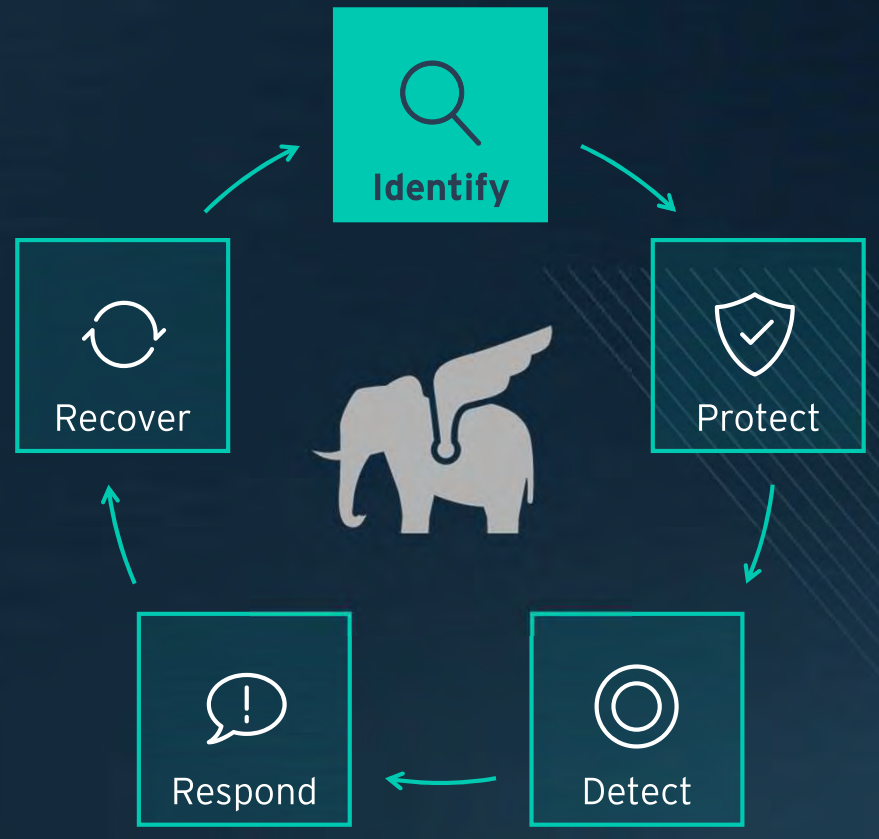
Das avency (NIST)

CYBERSECURITY Framework

Identify

- Assets aufspüren
- Assets inventarisieren
- Assets bewerten

„Kronjuwelen lassen sich nur schützen, wenn man weiß, welche es überhaupt gibt und wo diese sich befinden.“



avency

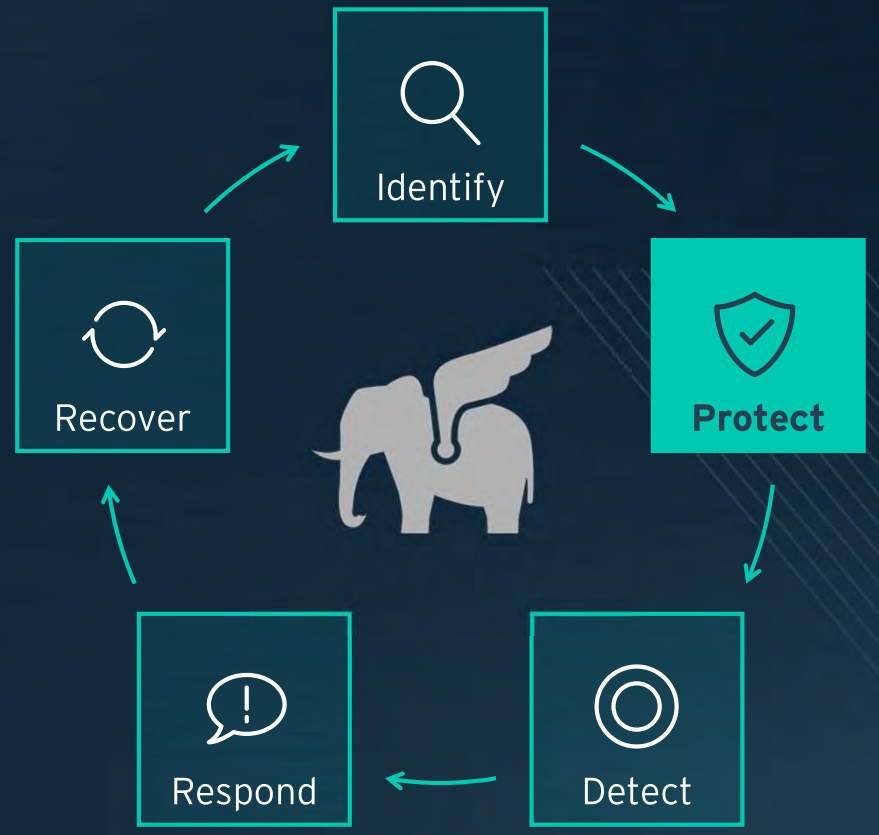
Das avency (NIST)

CYBERSECURITY Framework

Protect

- Assets aktiv schützen
- Umgebung immunisieren
- Angriffe abwehren

„Vorbeugen ist besser als heilen.“



avency

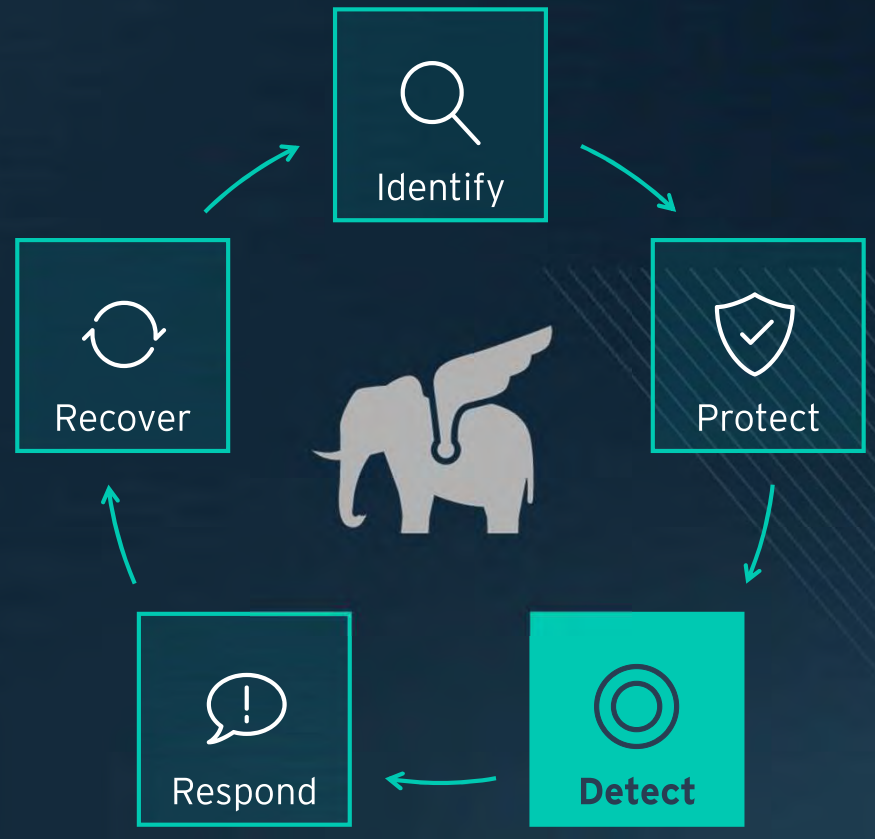
Das avency (NIST)

CYBERSECURITY Framework

Detect

- Schwachstellen aufdecken
- Risiken bewerten
- Angriffe erkennen

"Es gibt 2 Arten von CISOs:
Die, welche angegriffen wurden, und die, welche nicht wissen, dass sie angegriffen wurden."



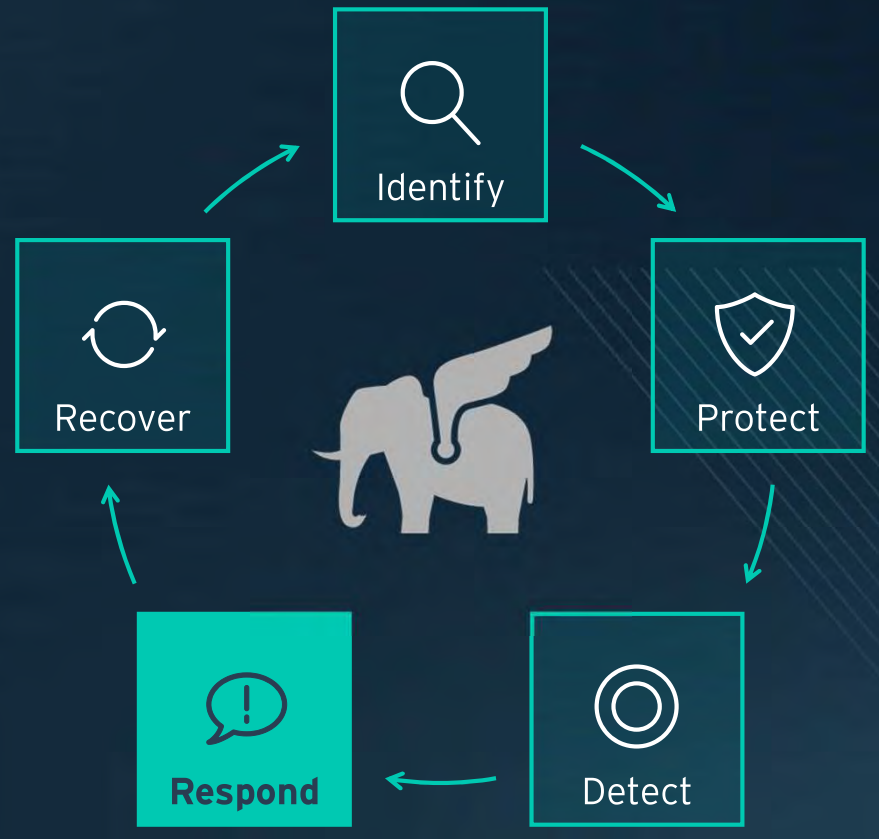
Das avency (NIST)

CYBERSECURITY Framework

Respond

- Auf Angriffe reagieren
- Automatisierte Aktionen
- Alert Workflow

„Bei einem Sicherheitsvorfall zählt jede Minute. Ein hoher Automatisierungsgrad stellt einen entscheidenden Vorteil dar.“



avency

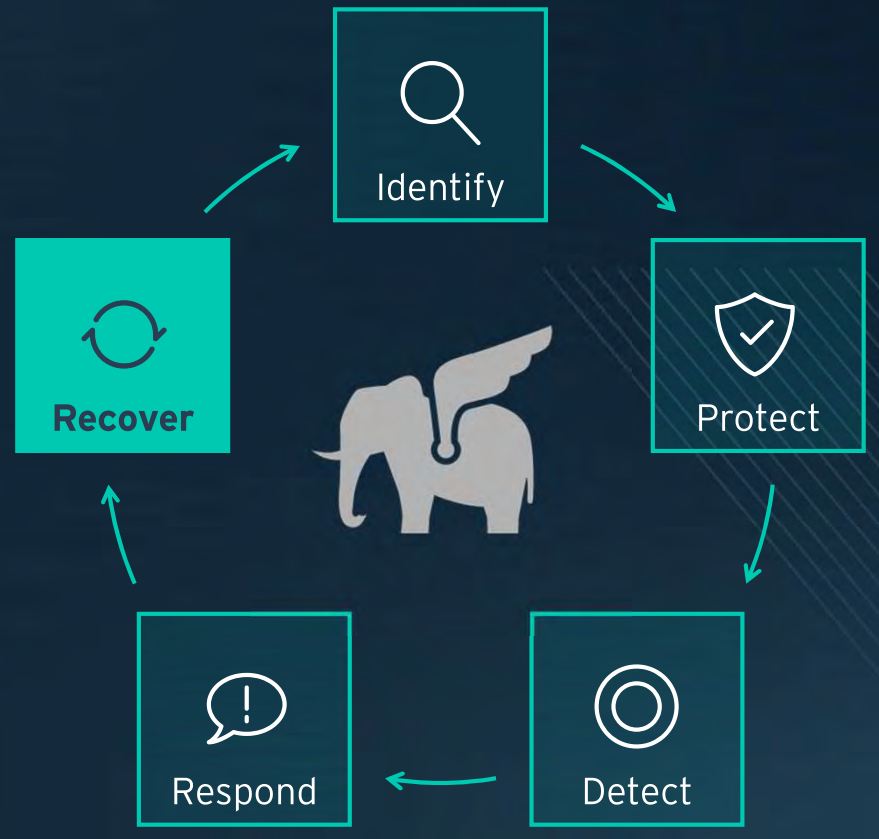
Das avency (NIST)

CYBERSECURITY Framework

Recover

- Business Continuity
- Asset Recovery
- Lernprozess

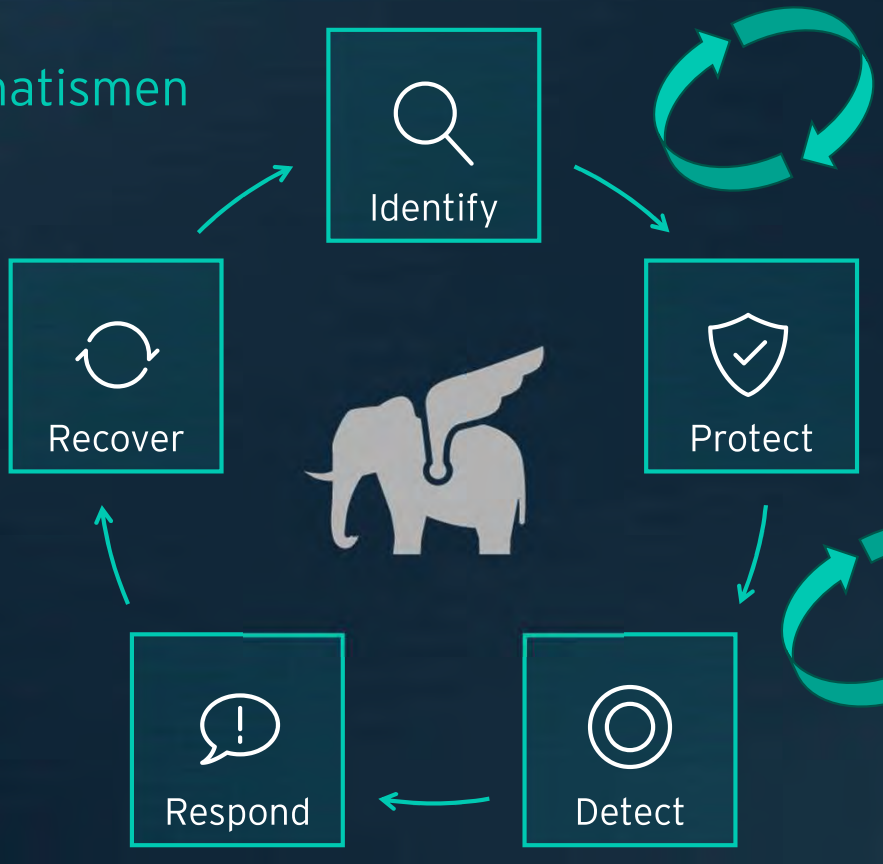
„Es gibt keine 100-prozentige Sicherheit. Ein Unternehmen muss jederzeit auf den Worst-Case vorbereitet sein."



Das avency (NIST)

CYBERSECURITY Framework

Schnittstellen/Automatismen



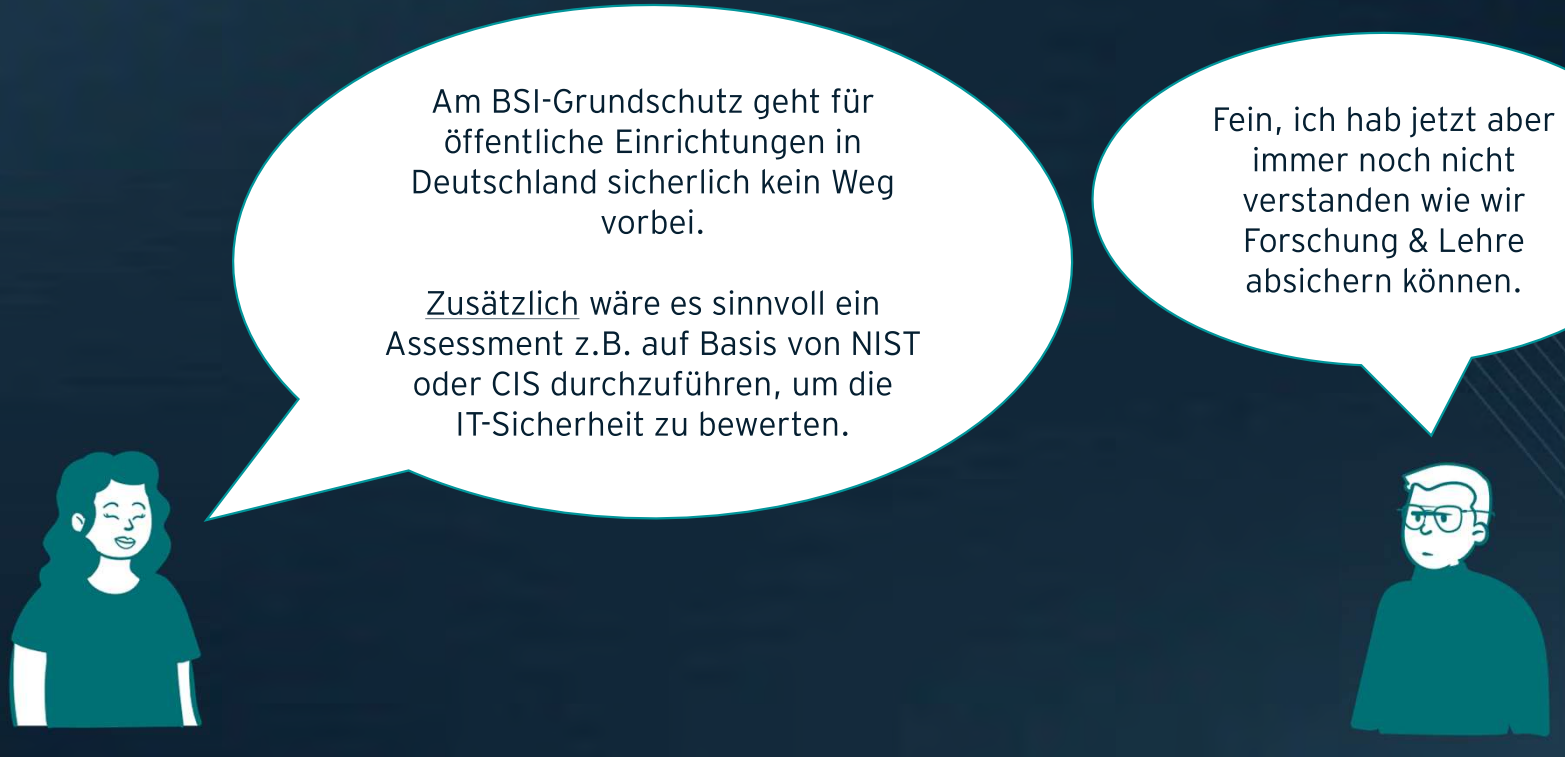
Client ist non-compliant
→ Firewall/Endpoint schränkt Zugriff ein

IPS/DNS Security erkennt Botnet Traffic
→ Endpoints/FWs isolieren Client

avency

Welches Framework sollte man nun nehmen?

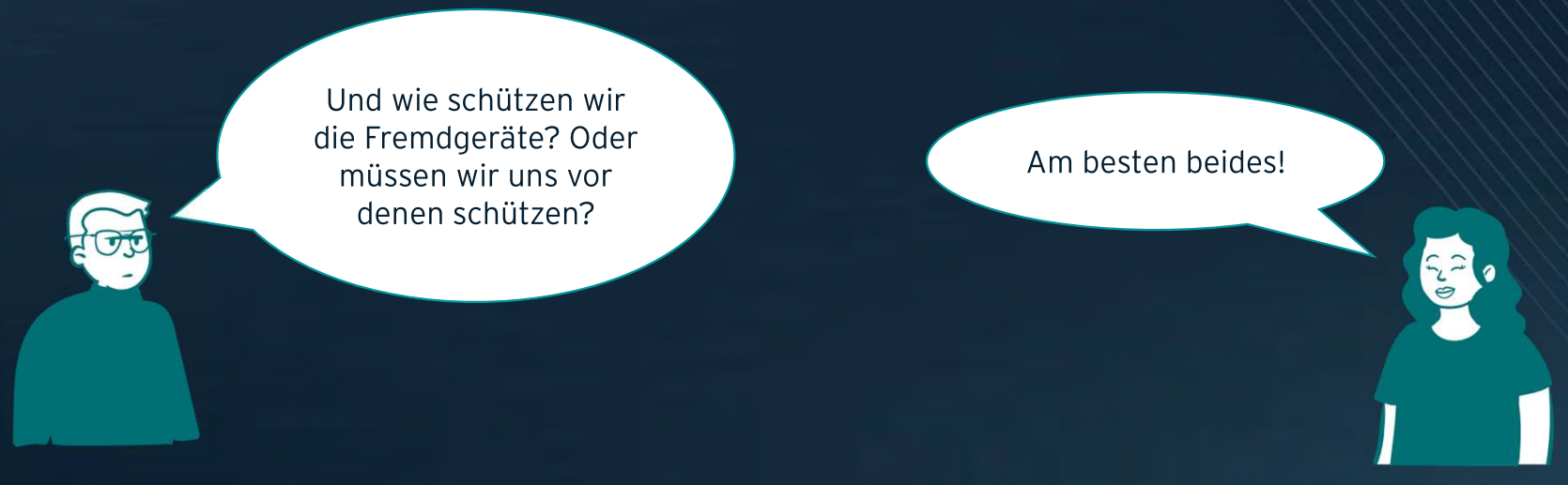
Handlungsempfehlungen aus der Praxis



Die technische Herausforderung in Forschung und Lehre

Handlungsempfehlungen aus der Praxis

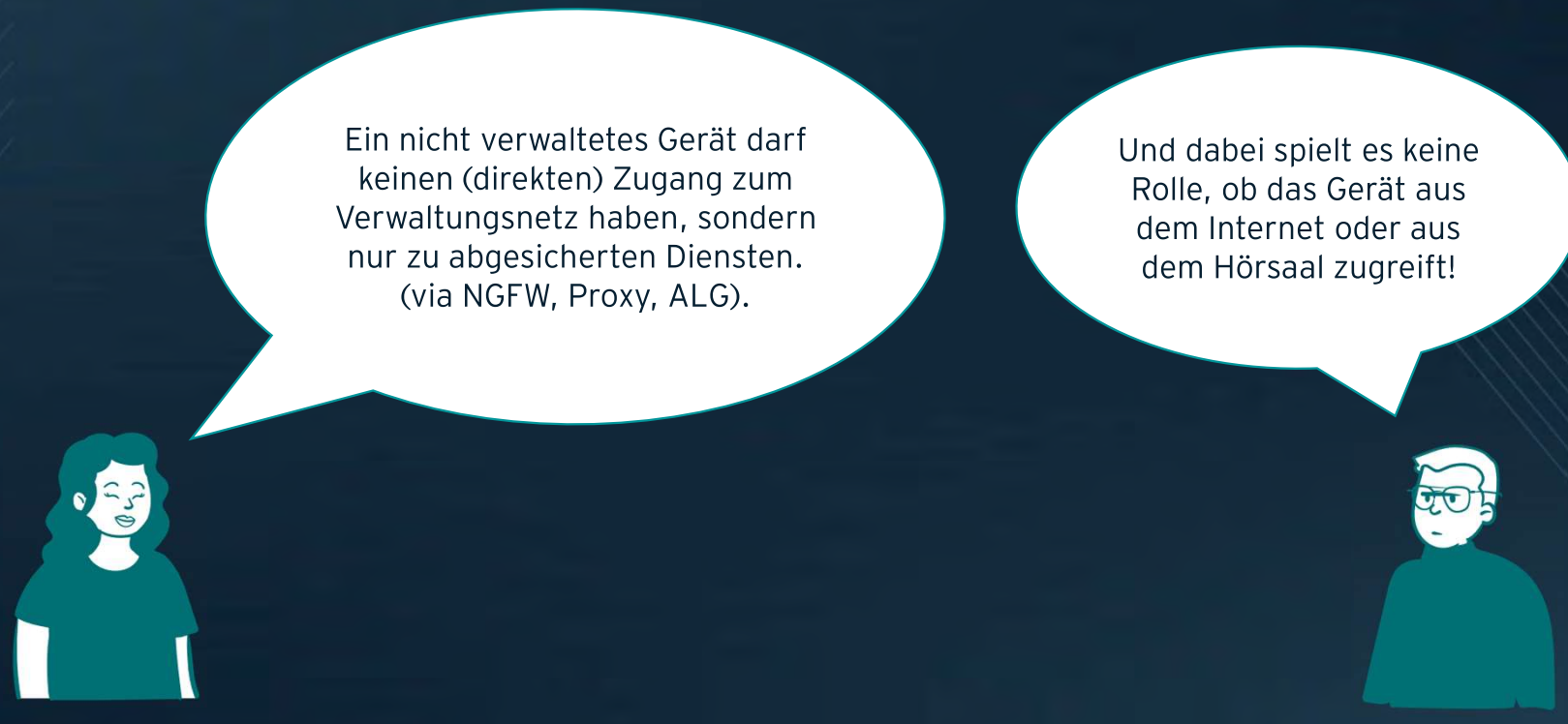
- Für Hochschuleigene Systeme gilt: Absicherung nach Verwaltungsstandard (z.B. Grundschutz)
- Für Fremdgeräte (z.B. von Studierenden und Lehrenden) können verständlicherweise keine Sicherheitsprotokolle und keine Installation von Software erzwungen werden.



avency

Wie sichern wir Forschung und Lehre ab?

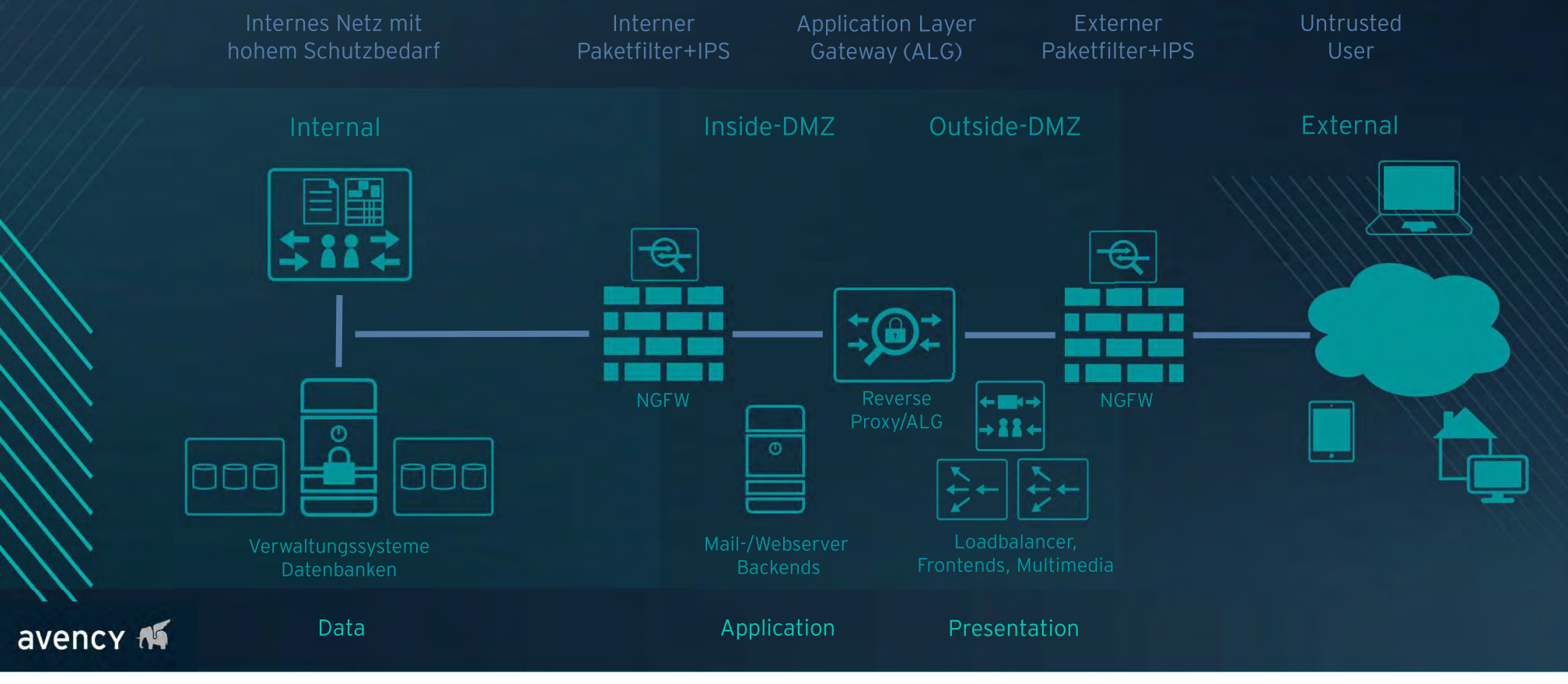
Handlungsempfehlungen aus der Praxis



avency

Absicherung kritischer Dienste

Das 3-Schichten Modell (aus Netzwerk- und Anwendungssicht)



avency

Wie sichern wir Forschung und Lehre ab?

Handlungsempfehlungen aus der Praxis

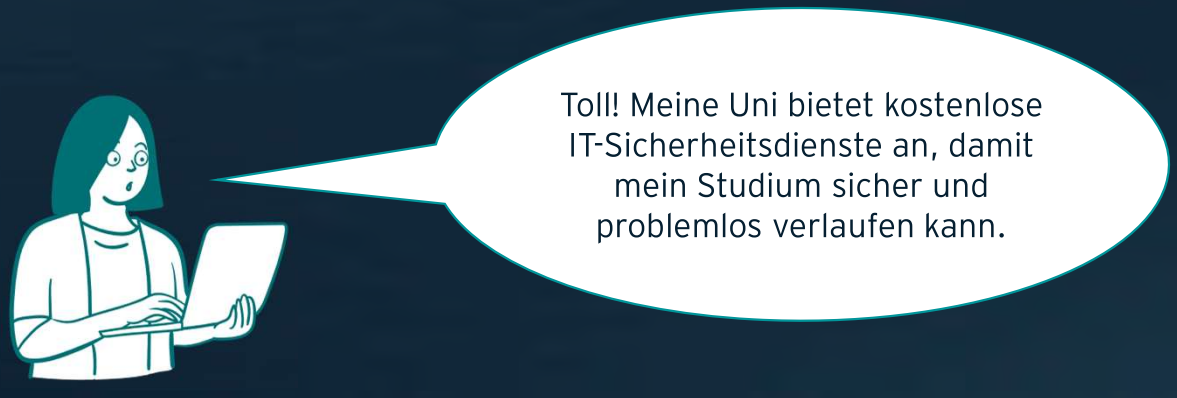
Und was können wir für den Schutz fremder Geräte tun?

Der Internetzugang über die Hochschule wird auch für Drittgeräte geschützt (URL-Filter). Zudem appellieren wir an die Eigenverantwortung und bieten Schulungen sowie die Nutzung von Diensten auf freiwilliger Basis an.

Die Hochschule als IT-Dienstleister

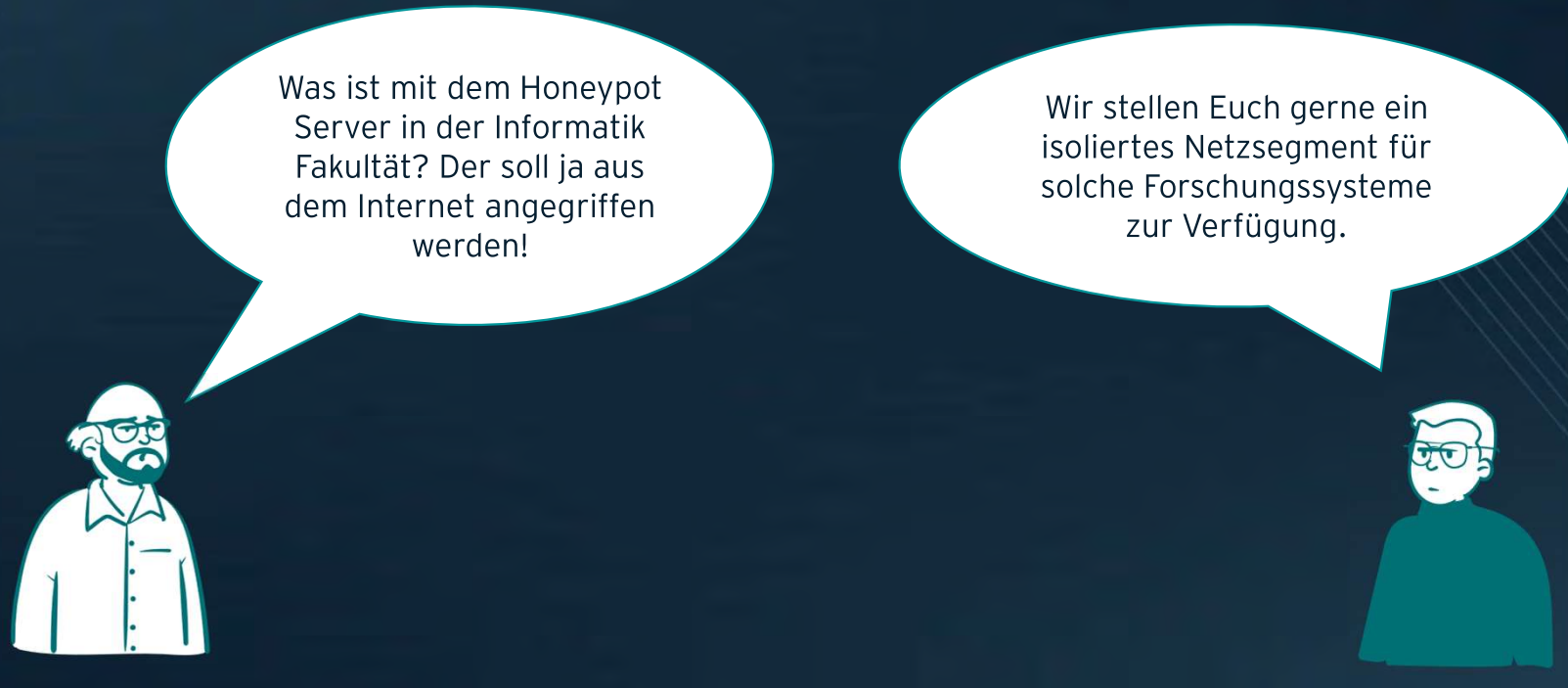
Aus der Not eine Tugend machen

- Die Hochschule sollte sich im Bereich IT-Sicherheit als Dienstleister verstehen
- Kostenfreie Angebote von Schulungen, Beratungsleistungen sowie Sicherheitssoftware/Diensten fördern das Vertrauen der Hochschulgemeinschaft in die Institution und ihre Systeme.
- Viele Hersteller haben günstige Lizenzprogramme speziell für Studierende



Wie sichern wir Forschung und Lehre ab?

Ausnahmen sind notwendig und absolut okay!



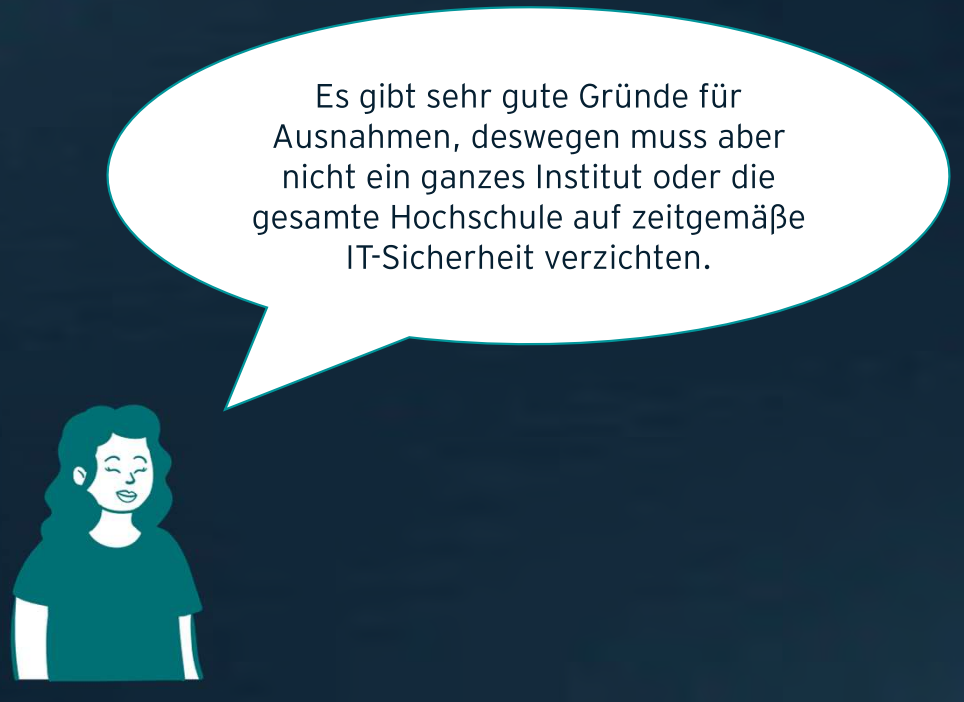
Wie sichern wir Forschung und Lehre ab?

Ausnahmen sind notwendig und absolut okay!

avency

Wie sichern wir Forschung und Lehre ab?

Fazit zu Ausnahmen



Wie sichern wir Forschung und Lehre ab?

Transparenz und Vertrauen schaffen

Ich möchte nicht, dass eine Sicherheitssoftware überwacht, was auf meinem PC geschieht und wo ich im Internet surfe.

Wir überwachen nicht, was du konkret tust oder welche Seiten du aufrufst. Die Software blockiert lediglich bösartige Webseiten, Viren und schadhafte Programme.

Auf unserer Webseite findest du ein ausführliches Aufklärungsvideo dazu.

avency

Und wie sollen wir das alles schaffen und betreiben?

Personalengpässe sind kein Argument keine IT-Sicherheit zu machen!

Es gibt heutzutage sehr gute Lösungen, mit denen man viele Anforderungen weitestgehend automatisieren kann!

Und es gibt erfahrene Dienstleister, die uns sowohl bei der Umsetzung als auch im Betrieb unterstützen können.

avency

Schlusswort

Das Grundgesetz garantiert vorbehaltlos die Freiheit von Wissenschaft, Forschung und Lehre. Das Grundgesetz garantiert aber auch die Funktionsfähigkeit der Forschungseinrichtung selbst, sowie das allgemeine Persönlichkeitsrecht, worunter auch der Schutz von personenbezogenen Daten fällt.

IT-Sicherheit ist daher nicht nur ein technisches Werkzeug oder eine gesetzliche Anforderung, sondern ein grundlegender Pfeiler, um die im Grundgesetz verankerten Rechte und Freiheiten zu wahren. Sie schützt die Integrität und Autonomie der wissenschaftlichen Arbeit, sichert die Vertraulichkeit personenbezogener Daten und bewahrt die Funktionsfähigkeit von Forschungs- und Bildungseinrichtungen.

Es ist essentiell und dringend notwendig, dass IT-Sicherheit in Forschungs- und Bildungseinrichtungen endlich die Priorität und Anerkennung erhält, die sie verdient.

Hendrik Walter, 2023

HOCHSCHULEN IM VISIER

Cybersicherheit im Spannungsfeld von Forschung & Lehre

VIELEN DANK!

hendrik.walter@avency.de

avency

MIT SICHERHEIT GUT BERATEN!