83. DFN-Betriebstagung – 08.10.2025

Cybersicherheit an Hochschulen 2025 – Status quo und Ausblick

Ein Blick von außen auf aktuelle Bedrohungen, reale Angriffe und notwendige Schutzmaßnahmen

Hendrik Walter

avency by Sequotech

avency by Sequotech

Wer ist avency?

Kurz und knapp. Wir sichern ab:

> 500.000
Studierende

> 160.000 t
Gewürze

> 26.000
Betten im Healthcare Bereich

> 18 Mio.
Hektoliter Bier

> 3.800
Einzelhandelsfilialen

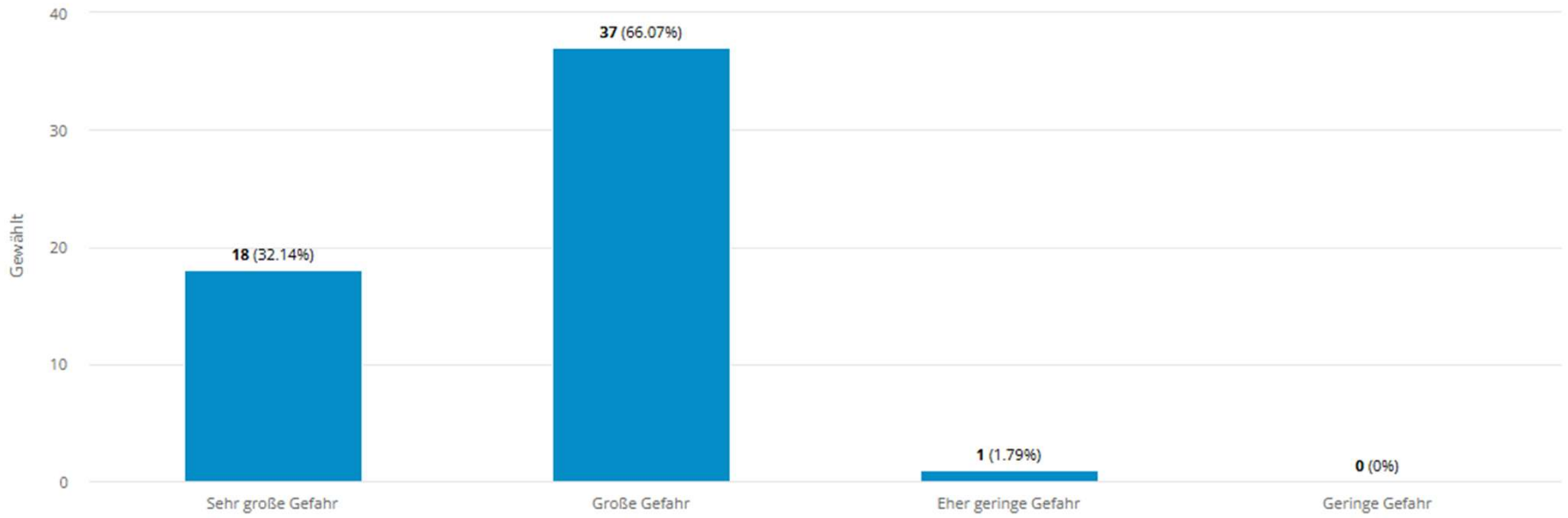
avency
by Sequotech

Anonyme Liveumfrage

Zur Gefahr durch Cyberangriffe

Wie bewerten sie die aktuelle Gefahr durch Cyberangriffe auf Hochschulen in Deutschland?

Anzahl Antworten: 56



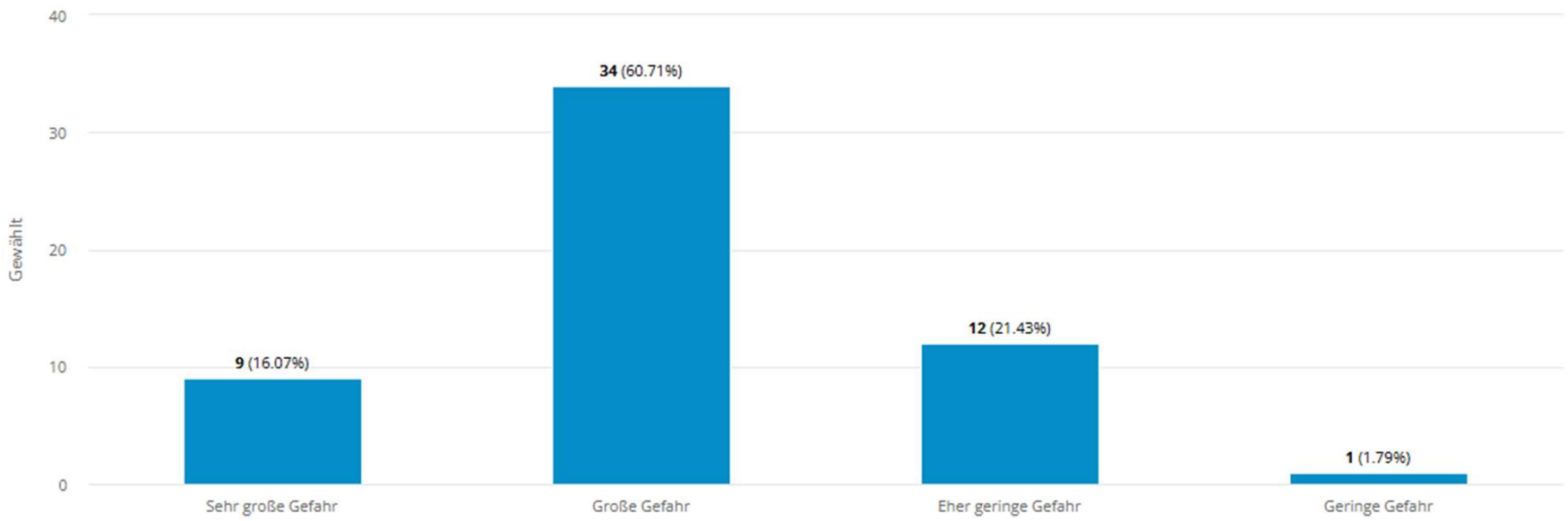
avency
by Sequotech

Anonyme Liveumfrage

Zur Gefahr durch Cyberangriffe

Wie bewerten sie die aktuelle Gefahr durch Cyberangriffe auf Ihre Hochschule ?

Anzahl Antworten: 56



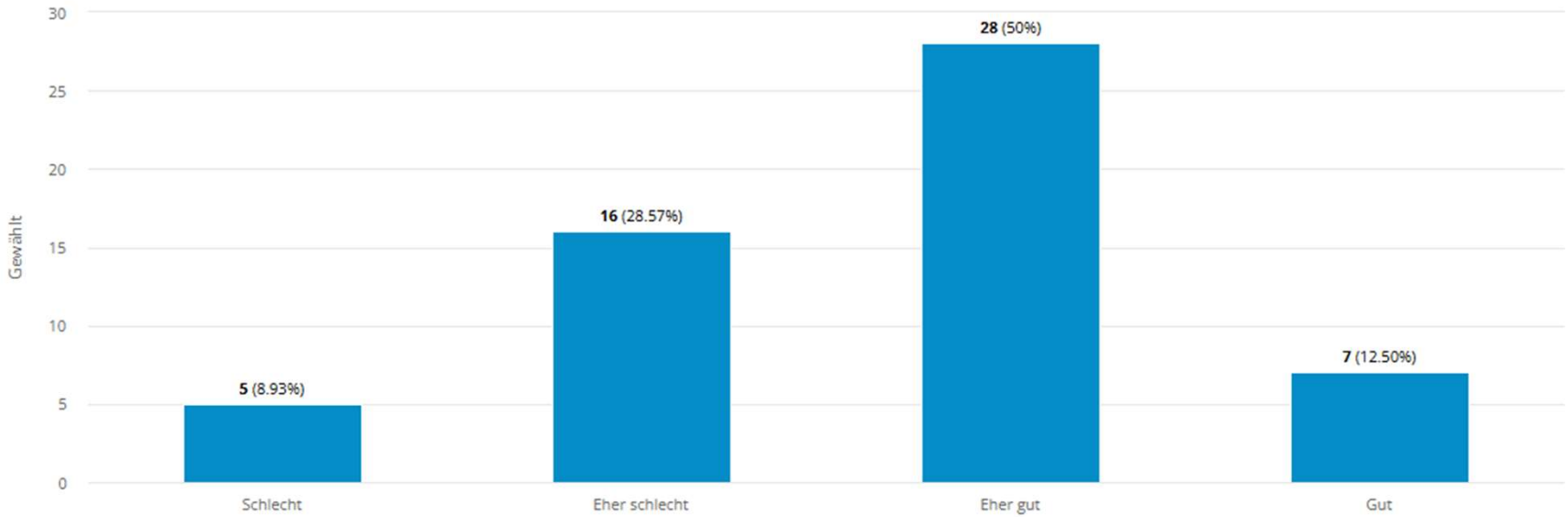
avency
by Sequotech

Anonyme Liveumfrage

Zur Gefahr durch Cyberangriffe

Wie bewerten sie die Sicherheitsvorkehrungen Ihrer Einrichtung?

Anzahl Antworten: 56



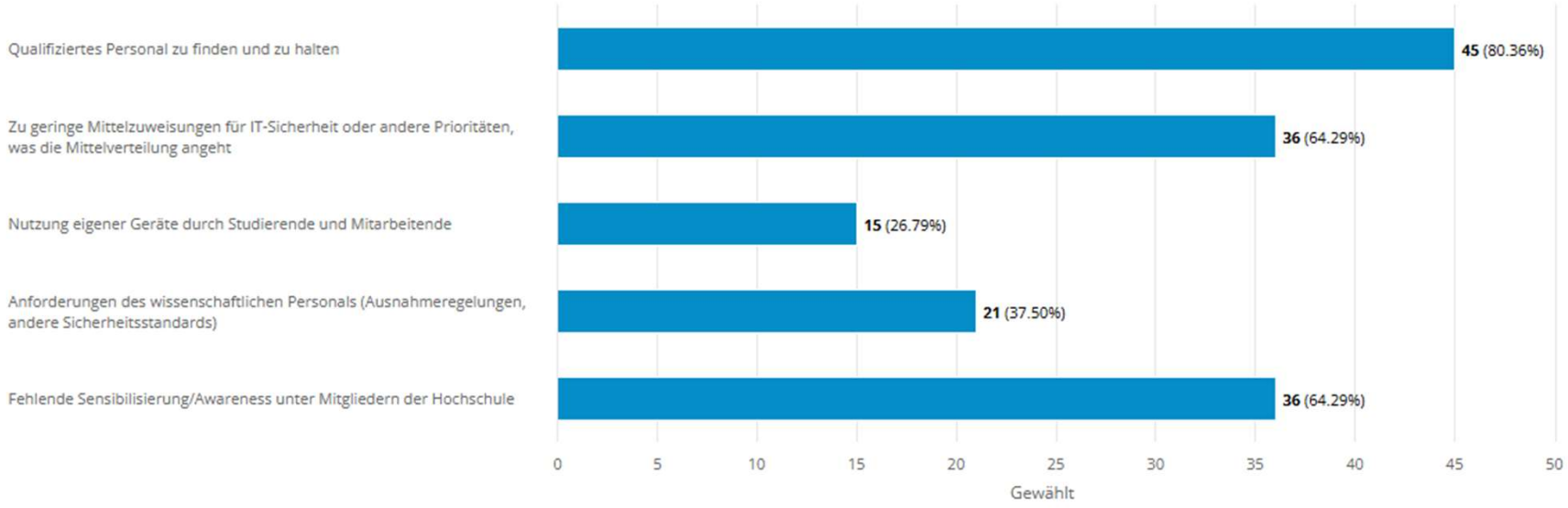
avency
by Sequotech

Anonyme Liveumfrage

Zur Gefahr durch Cyberangriffe

Was sehen sie als die größten Herausforderungen Ihrer Hochschule bei der Abwehr von Cyberangriffen? (Mehrfachauswahl möglich, max. 3 Antworten)

Anzahl Antworten: 56



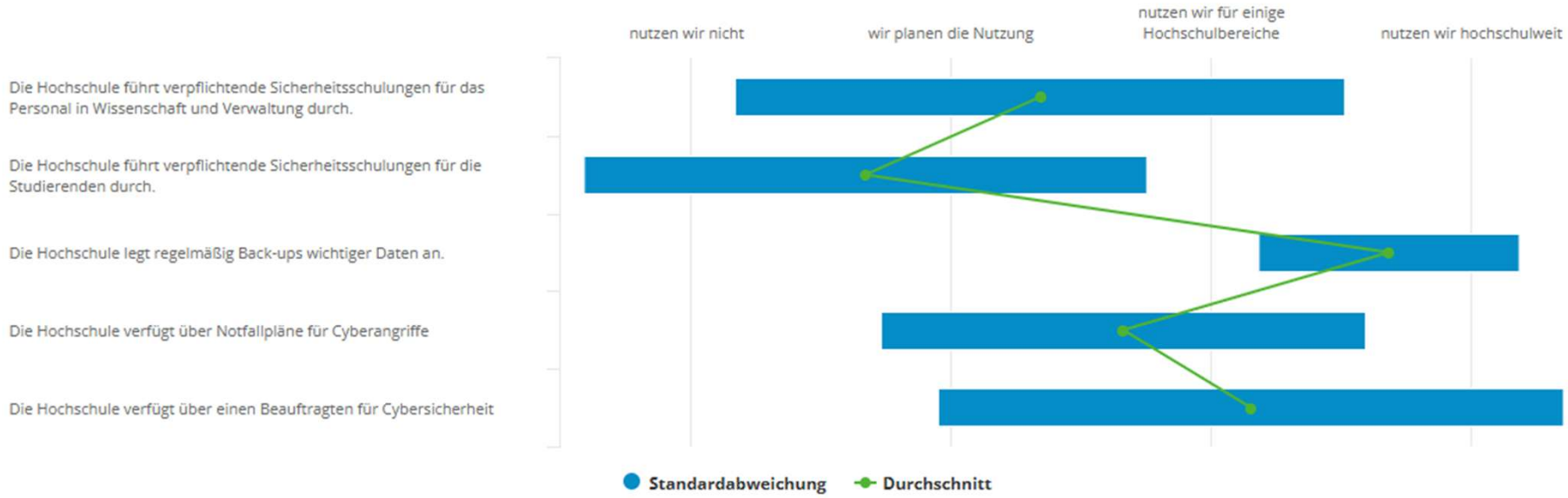
avency
by Sequotech

Anonyme Liveumfrage

Zur Gefahr durch Cyberangriffe

Welche der folgenden Maßnahmen werden an Ihrer Hochschule eingesetzt?

Anzahl Antworten: 56



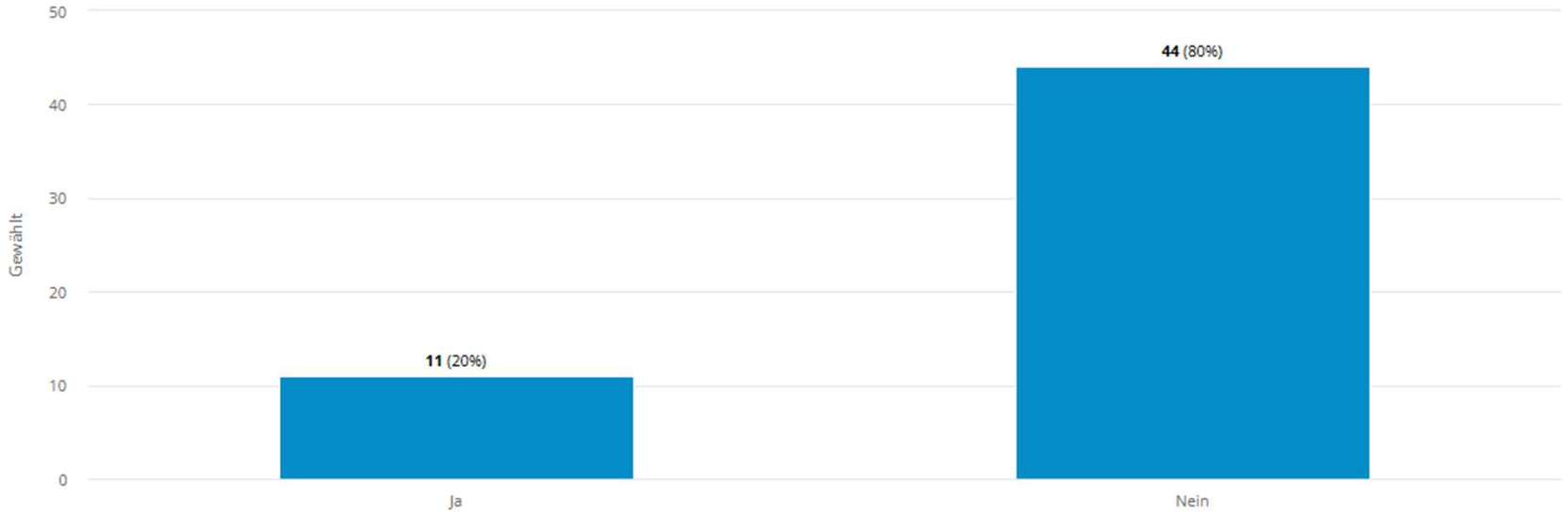
avency
by Sequotech

Anonyme Liveumfrage

Zur Gefahr durch Cyberangriffe

Unsere Hochschule war in den letzten 5 Jahren Opfer eines Cyberangriffs, der zum Diebstahl von Daten oder zu Einschränkungen des Betriebs geführt hat.

Anzahl Antworten: 55

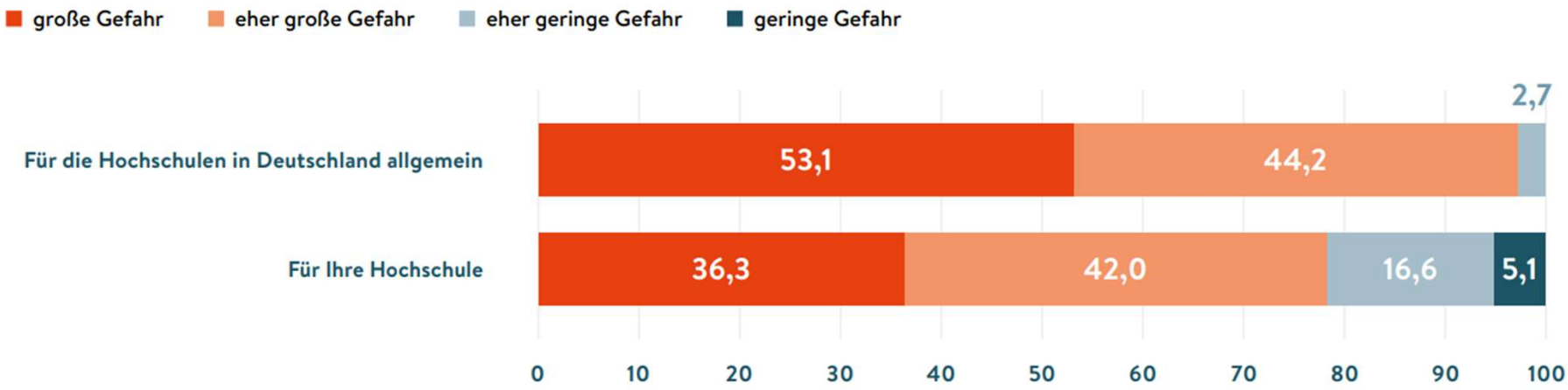


avency
by Sequotech

Selbsteinschätzung Hochschulleitung

Bewertung der Gefahr durch Cyberangriffe

Bewertung der Gefahr durch Cyberangriffe für die Hochschulen durch die Hochschulleitungen; in Prozent



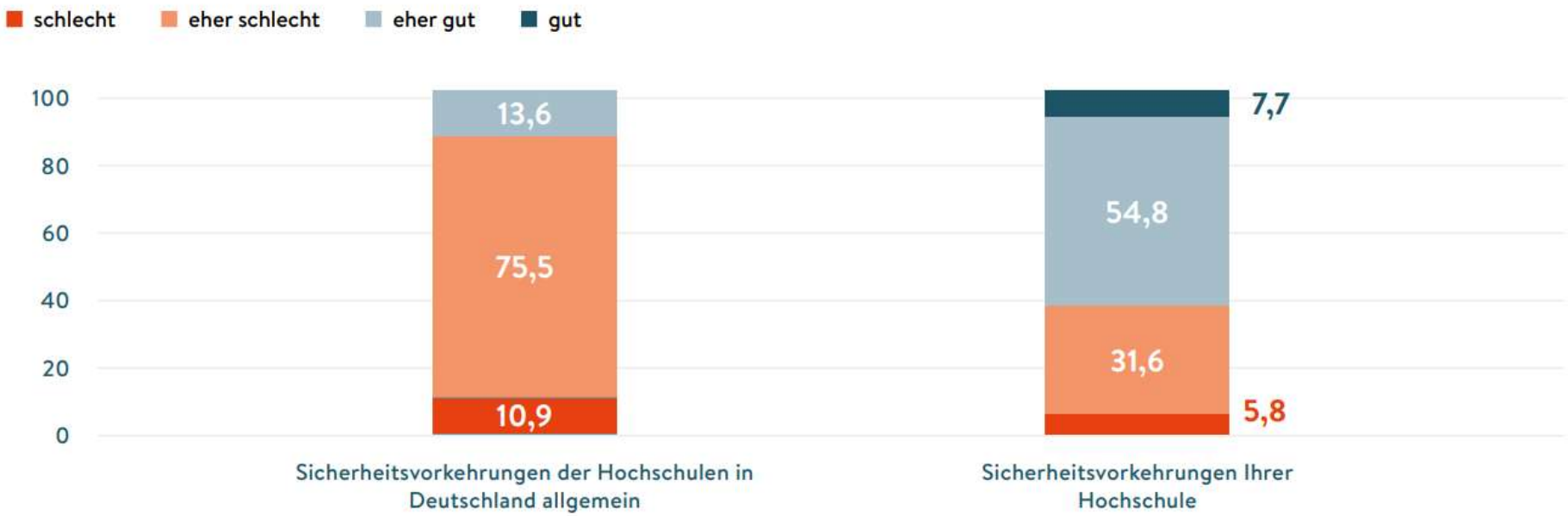
Quelle: Hochschulbarometer 2024

avency by Sequotech

Selbsteinschätzung Hochschulleitung

Bewertung der Sicherheitsvorkehrungen

Bewertung der Sicherheitsvorkehrungen der Hochschulen durch die Hochschulleitungen; in Prozent



Quelle: Hochschulbarometer 2024

avency by Sequotech

Die 4 größten Herausforderungen

Und der Grund warum Hochschulen ein besonders attraktives Ziel sind

1 Mangel an qualifiziertem Personal

Es fehlt an ausreichend IT-Sicherheitsexpert:innen, um komplexe Angriffe abzuwehren und Notfallpläne professionell umzusetzen.

2 Zu geringe Mittel

Viele Hochschulen haben keine ausreichenden Budgets für moderne Sicherheitslösungen, kontinuierliches Monitoring und externe Unterstützung.

3 Bring your own Device

Die private Nutzung von Laptops, Tablets und Smartphones erschwert eine einheitliche Sicherheitskontrolle und eröffnet zusätzliche Angriffsflächen.

4 Nötige Ausnahmen

Forschung und Lehre verlangen offene Systeme und Sonderregelungen, die Sicherheitsrichtlinien oft durchlöchern und schwer konsequent durchsetzbar machen.

avency
by Sequotech

Lagebild Deutschland

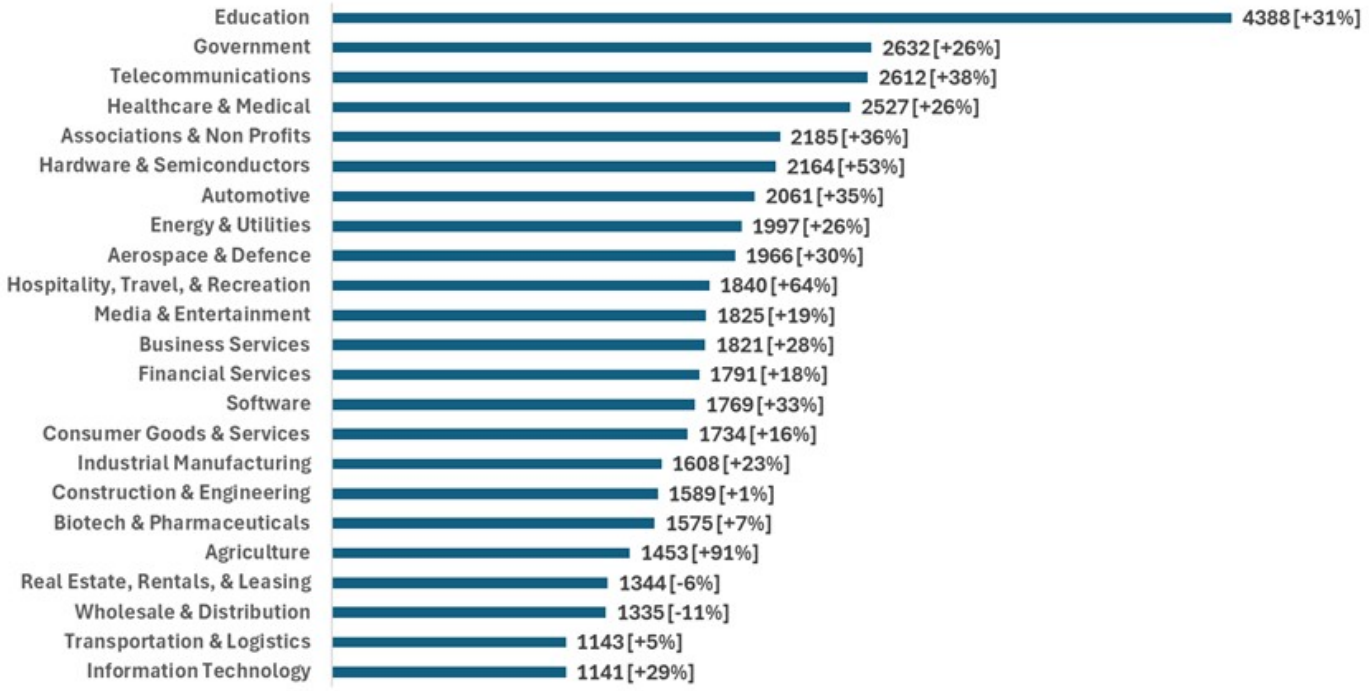
- Zahlen werden auf Bundesebene nicht systematisch erfasst. Angriffe sind auch nicht automatisch meldepflichtig (außer bei meldepflichtigem Datenschutzvorfall).

- Von 2022-2024 wurden dem BKA 42 erfolgreiche Hackerangriffe auf deutsche Hochschulen und Wissenschaftseinrichtungen gemeldet. Teils mit dramatischen Folgen/Kosten.

- Ein neuer Trend ist in Deutschland nicht zu beobachten. Die Gefahrenlage bleibt auf hohem Niveau (ca. 20 gemeldete Vorfälle an Hochschulen pro Jahr).

Lagebild International

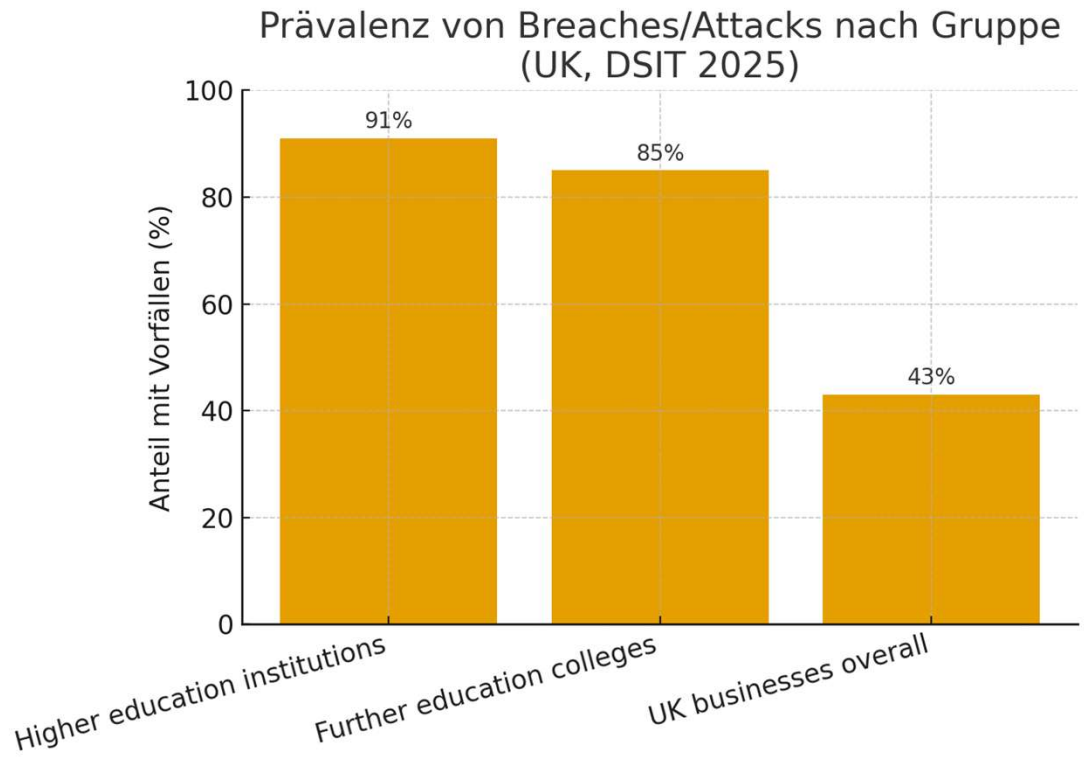
Durchschnittliche wöchentliche Cyberangriffe je Branche/Industriezweig
Q2/2025 vs Q2/2024



Quelle: Checkpoint Research 2025

avency
by Sequotech

Lagebild International



avency
by Sequotech

Aktuelle Bedrohungen

#1 Ransomware & Daten-Erpressung

Bedrohung

Ransomware (Datenabzug + Erpressung) immer noch #1 der Bedrohungen.

Tätergruppen wie Vice Society spezialisieren sich auf Bildungssektor.

Leak-Erpressung immer öfter ohne Verschlüsselung (Backups helfen nicht).

Trend: Unverändert hoch.

Folgen für Hochschulen

Systeme tagelang offline (ggf. Wochenlang), Neustart von IT-Infrastrukturen nötig, Datenleaks mit Studierenden- und Forschungsdaten.

Wichtigste Maßnahmen

- Prävention (IT-Hygiene + Endpoint & Netzwerkschutz).
- Regelmäßige, offline gespeicherte Backups und funktionierende Notfallpläne.

avency
by Sequotech

Aktuelle Bedrohungen

#2 Identitätsangriffe

Bedrohung

Missbrauch von Accounts (gestohlene Passwörter, MFA-Umgehung, OAuth-App-Missbrauch).

Gestohlene Zugangsdaten sind weiter der häufigste Einstiegspunkt für Angreifer!

Trend: Stark steigend.

Folgen

Unbefugter Zugriff auf Mail, Forschungsdaten, Prüfungsportale.

Stille Datenabflüsse, kaum sofort bemerkt. Häufig in Kombination mit Ransomware.

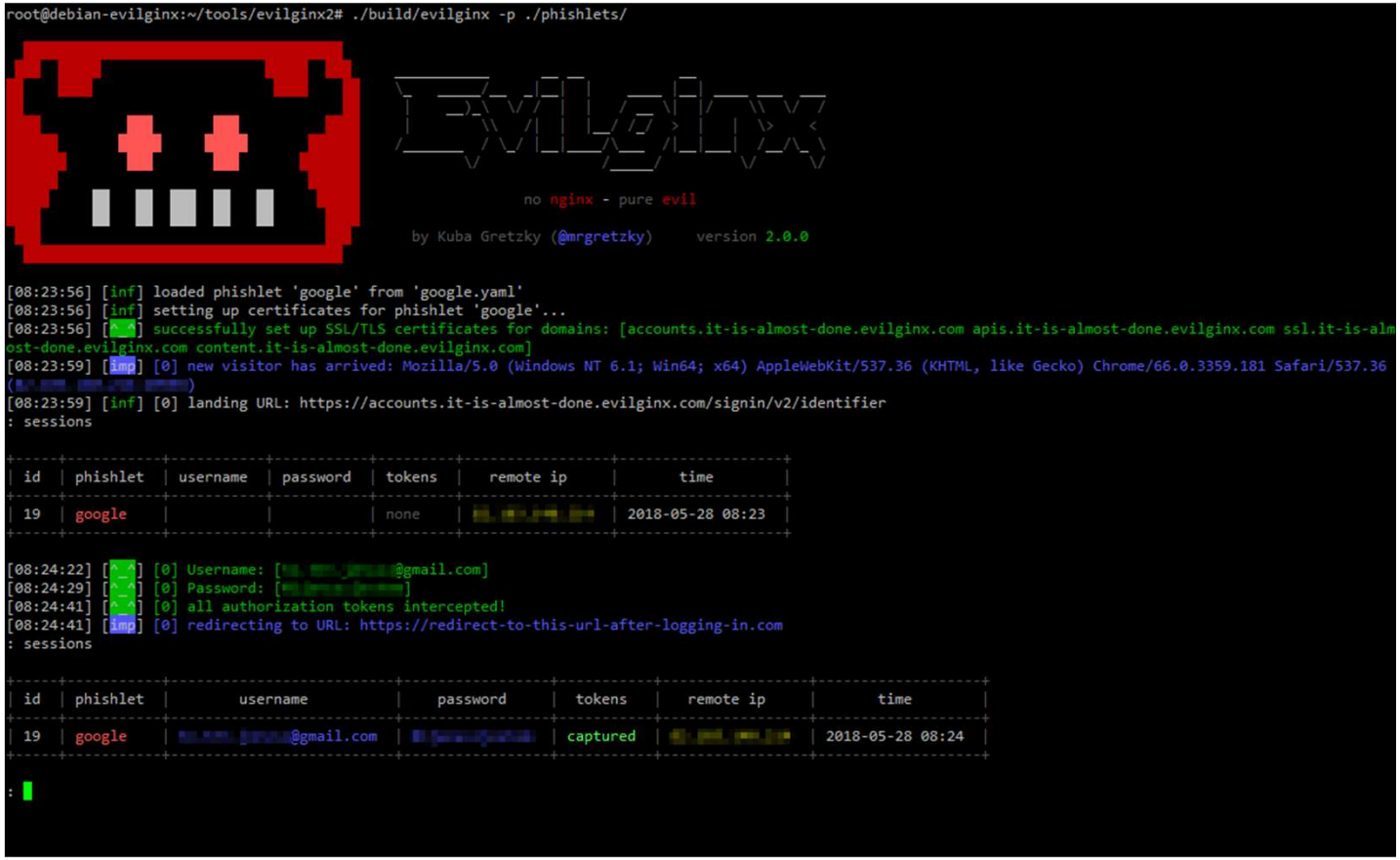
Wichtigste Maßnahmen

- Legacy-Auth vollständig blocken. Admin Rollen zusätzlich sichern (PIM).
- Phishing-resistente MFA (WebAuthn z. B. FIDO2/Passkeys) konsequent einführen (Origin-Bindung).
- Klassische OTP (SMS-/App-Codes) allein reichen nicht mehr.

avency
by Sequotech

Aktuelle Bedrohungen

#2 Identitätsangriffe – Warum klassische MFA nicht mehr reicht!



Moderne Phishing Tools stehlen nicht nur Benutzernamen und Passwort sondern die gesamte MFA-Session (Tokens)!

Wer seine MFA auf Phishing Resistenz testen möchte: Evilginx ist Opensource (BSD-3) und liegt bei Github.

avency
by Sequotech

Aktuelle Bedrohungen

#3 Phishing & Social Engineering (mit KI)

Bedrohung

Täuschung per Mail/Telefon, um Zugangsdaten zu erhalten, Klicks zu erzwingen, oder andere Aktionen auszulösen (z.B. Überweisung).

Neu: KI generierte Deepfakes in Sprache oder sogar Bild (Teams Call) sowie KI generierte Phishing Mails (Rechtschreibfehler etc… ade, Erkennung wird erheblich schwieriger).

QR-Code Phishing auf öffentlichen Plätzen!

Trend: Stark ansteigend.

Folgen

Hohe Erfolgsrate bei Studierenden & Mitarbeitenden. Türöffner für Ransomware oder Datenexfiltration.

Wichtigste Maßnahme

- Verbindliche Awareness-Trainings für Mitarbeitende und Studierende.

avency
by Sequotech

Aktuelle Bedr

#3 Phishin

KI-Betrug explodiert: Deepfakes verursachen Milliardenschäden

Eine Welle hochentwickelter KI-Betrügereien mit Deepfake-Videos und Stimmklonen führt zu beispiellosen finanziellen Verlusten. Regierungen und Cybersicherheitse

01.10.2025, 22:51 Uhr

BE Börse Express

KI-Betrug, Finanzbranche

KI-Betrug bedroht Finanzbranche mit Deepfakes

30.09.2025 - 09:31:02

Künstliche Intelligenz revolutioniert Finanzbetrug durch täuschend echte Deepfakes und Stimmklone, die biometrische Sicherheitssysteme umgehen. Finanzinstitute setzen eigene KI zur Abwehr ein.

(arns Call) sowie

(schwieriger)

Q

Tre ark ansteigend.

Folgen

Hohe Erfolgsrate bei Studier

Wichtigste Maßnahme

- Verbindliche Awareness-Trainings für Mitarbeitende und Studierende.

avency by Sequotech

Aktuelle Bedrohungen

#4 Angriffe auf Edge-Systeme

Bedrohung

Ausnutzung von Schwachstellen in VPNs, Firewalls, Remote-Zugängen. Jüngste Beispiele:

PAN-OS CVE-2024-3400 (CVSS: 10.0), FortiOS CVE-2024-21762 (CVSS: 9.6), Ivanti 2025 Exploit-Ketten

Trend: Edge-Exploits als Initialzugang inzwischen bei 20 % (Verdopplung gegenüber Vorjahr!).

Folgen

Angreifer haben direkten Netzwerkzugang. Monate lange Persistenz möglich.

Von Datendiebstahl-/Ransomware Erpressung über Sabotage alle Folgen denkbar.

Wichtigste Maßnahmen

- Schnelles, risikobasiertes Patch-Management für VPNs/Firewalls.
- Kritische Updates müssen binnen Stunden/Tagen, nicht Wochen eingespielt werden.
- Pläne für Notfall Abschaltung (ggf. 2 Vendor Strategie).

avency
by Sequotech

Aktuelle Bedrohungen

#5 Supply-Chain & Drittanbieter

Bedrohung

Angriff über Software-Updates oder externe Dienstleister.

Beispiel: MOVEit-Leak (2023): Daten von ~900 US-Hochschulen über Student Clearinghouse kompromittiert.

Trend: Supply-Chain-Angriffe nehmen zu.

Folgen

Auch bei solider eigener IT werden Forschungs-/Studierendendaten über externe Systeme kompromittiert.

Wichtigste Maßnahme

- Vollständiges Inventar und Risiko-/Sicherheitsbewertung aller Dienstleister & Softwarelieferanten.

Aktuelle Bedrohungen

#6 DDoS gegen Lern- & Prüfungsportale

Bedrohung

Überlastungsangriffe auf Websites, Learning Management Systeme (LMS) und Prüfungsplattformen.

Rekord-DDoS 2024/25: bis 22,2 Tbps!

Folgen

Prüfungen nicht durchführbar, Forschung & Lehre massiv gestört, Reputationsverlust.

Wichtigste Maßnahme

- DDoS-Mitigation durch Provider (Basis DoS Schutz vom DFN + globale Abwehr via Cloudflare/Link11).
- Hochschulen alleine können Spitzenlasten nicht abwehren!

avency
by Sequotech

Aktuelle Bedrohungen

#7 Fehlerhafte Appkonfiguration & Schatten-IT

Bedrohung

Unsichere Cloud/SaaS-Einstellungen (Microsoft 365, Atlassian, Google Workspace) sowie unkontrollierte Nutzung von KI/Cloud-Diensten. Häufig zu viele Global Admins, schwache Sharing Policies.
Angriffe über bösartige OAuth-Apps.

Folgen

Datenabfluss ohne „Hack“ durch Zustimmung oder Schatten-IT (Dropbox, ChatGPT).

Wichtigste Maßnahmen

- Sichere, datenschutzkonforme Tools für File-Sharing und KI-Nutzung bereitstellen.
- Bei Cloud Nutzung Security-Baselines durchsetzen.

avency
by Sequotech

Ausblick

Neue Angriffsvektoren in den nächsten 12–24 Monaten

- KI-skaliertes Social Engineering/Deepfakes
- OAuth-/Consent-Phishing & bösartige Cloud-Apps
- RAG/Prompt-Injection über Campus-Dokumente

avency
by Sequotech

Was sollte man jetzt tun?

IT-Security Best Practices an Hochschulen

Keine grundsätzliche Änderung der bekannten Maßnahmen (BSI-Grundschutz).

Fokus auf:

- Resilienz → Funktionierende(!) Sicherungs- und Notfallkonzepte
- Awareness (Phishing/Deepfakes)
- Phishing-Resistente MFA
- IT-Hygiene → Härtung, Vulnerability und Patch Management
- Verhinderung von Schatten IT (freie KI Chatbots, unsichere Clouddienste)

avency
by Sequotech

Rückblick Tagung 10/2023

ZKI-Grundschutz-Profil – Übergeordnete Bausteine

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

Sehr wichtig, aber einer klickt immer drauf!

Viele beschäftigen sich bereits intensiv mit Detektion und Reaktion (Prio R2/3), obwohl sie R1 noch gar nicht im Griff haben.

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 Äderungsmanagement **OPS.1.1.3.** Schutz vor Schadprogrammen **OPS.1.1.4.** Protokollierung **OPS.1.1.5** Software-Tests und -Freigaben **OPS.1.1.6**	

Viele sind hier relativ weit. Das ist auch sehr wichtig (daher R1). Es verhindert technisch aber keine Angriffe (Prävention).

avency by Sequotech

Sicherheit gewinnt man nicht mit Hype, sondern mit Hausaufgaben!

Hendrik Walter
avency GmbH

avency
by Sequotech