Sieben erste Schritte zum besseren Schutz

Cybersicherheit an Hochschulen

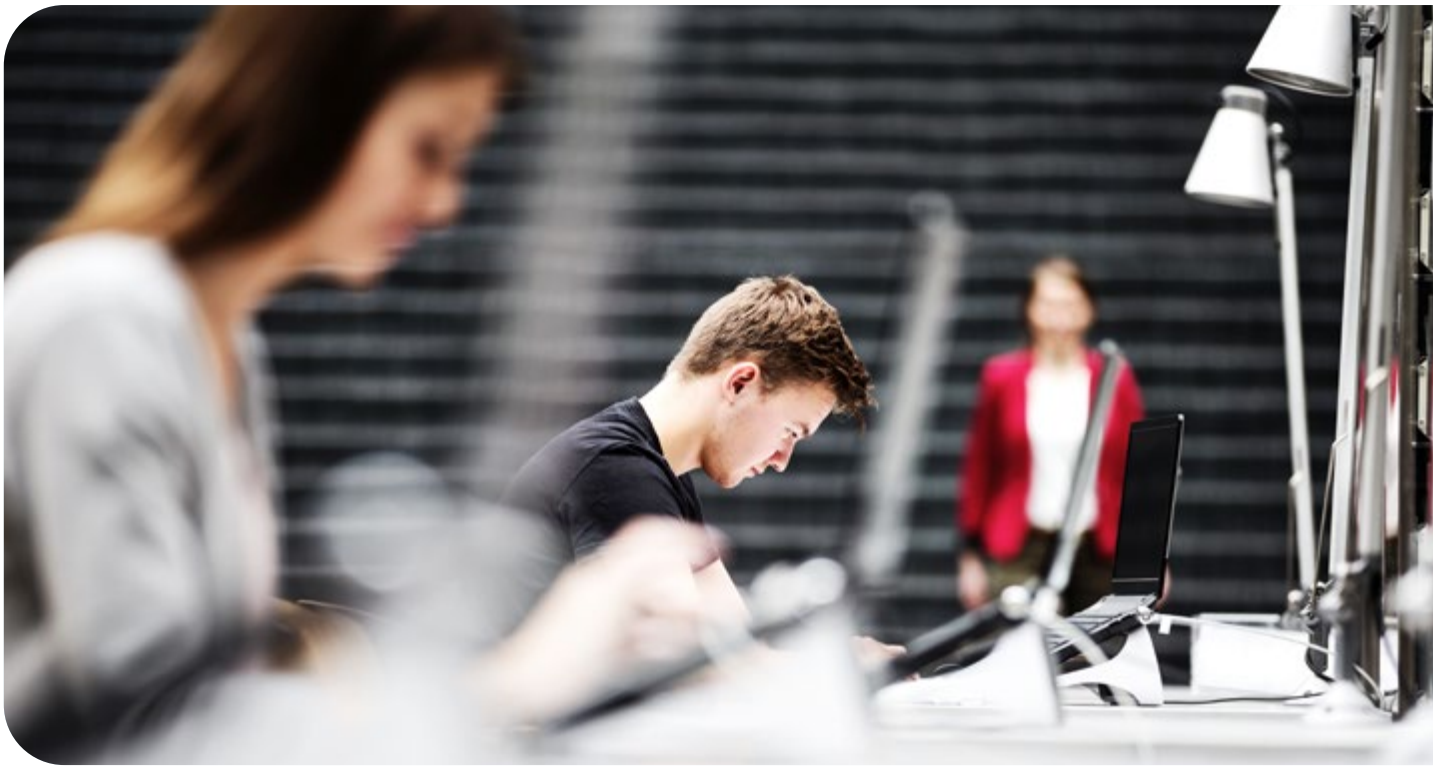
Die Anzahl „erfolgreicher“ Cyberangriffe in Deutschland auf Bildungs-, Verwaltungs- und Gesundheitseinrichtungen hat in den vergangenen zwei Jahren signifikant zugenommen. Dies belegen Zahlen des Analyseunternehmens KonBriefing[1]

Insbesondere der öffentliche Bildungs- und Forschungsbereich rückt dabei zunehmend in den Fokus der Aggressoren. Der Grund ist so simpel wie fatal: Die Cybersecurity von Hochschulen und Universitäten ist aufgrund des freien Zugangs zur Forschung sowie limitierter Ressourcen häufig lückenhaft und somit oft ein Opfer von Zufallstreffern oder eines Kollateralschadens. Dabei können die Auswirkungen nicht nur für die einzelne Hochschule, sondern ganze Bildungsinfrastrukturen verheerend sein.

Es werden nicht nur die Server verschlüsselt, oft verbunden mit der Drohung, personenbezogene Daten im Darknet zu veröffentlichen, sondern auch noch alle Daten auf den Speicher-Systemen gleichzeitig gelöscht – ohne eine Möglichkeit zur Wiederherstellung. Denn das Backup wird ebenfalls verschlüsselt. Über solch einen Angriff mit Erpressungstrojanern (Ransomware) werden dann die betroffenen Institutionen mit Lösegeldzahlungen erpresst oder bewusst in ihrem Betrieb und ihrer Reputation beschädigt.

IT-EntscheiderInnen an Hochschulen stehen daher aktuell unter enormem Handlungsdruck. Doch aus Zeitmangel fehlt ihnen meist der Überblick über die vielen, komplexen Möglichkeiten. Gleichzeitig mangelt es an Fachkräften und damit auch Know-how und Ressourcen. Zudem sind viele Informationen und Lösungen nur für technisch versierte Personen verständlich: Denn was bedeuten Begriffe wie *Zero Trust, SASE, XDR* oder *Managed Endpoint* konkret in der Praxis?

[1] Vgl. https://konbriefing.com/de-topics/hackerangriff-deutschland.html, Cyberangriffe 2021: 106, 2022:166.



Cybersecurity-Spielregeln

Die verwendeten Lösungen werden oft nicht zielführend eingesetzt. Denn aus völlig nachvollziehbaren Gründen fehlt zumeist ein organisationsübergreifendes Verständnis bezüglich der „Spielregeln“ von Cybersecurity. Erst wenn alle, vom Präsidium über IT-EntscheiderInnen bis zum IT-Admininstrator, die Cybersecurity-Spielregeln kennen sowie artikulieren und kommunizieren können – ohne dabei in technische, produktspezifische oder regulatorische Details zu verfallen – lassen sich Lösungen für fast alle Probleme finden.

Grundsätzlich sollten sich alle Projekte und Aktivitäten an den folgenden **vier übergeordneten Zielen** orientieren und priorisiert werden – denn Cybersecurity ist ein unendliches Spiel.

Unsere übergeordneten Ziele

1. Gelingt es uns, den operativen Betrieb (NetOps, Bereitstellung und kontinuierliche Orchestrierung) zu vereinfachen, indem die Komplexität reduziert und die Automatisierung/Integration erhöht wird?
2. Lässt sich das Security Operations Management (SecOps) verbessern sowie das Cybersecurity-Risiko kontinuierlich reduzieren, indem Schwachstellen und Cybervorfälle frühzeitig und ganzheitlich erkannt, bewertet und beseitigt werden können?
3. Wird die Nutzerakzeptanz und -zufriedenheit erhöht – bei gleichzeitiger Verbesserung der IT-Sicherheit – mit dem Ziel, einer Schatten-IT vorzubeugen?
4. Können wir eine flexible und sichere Umsetzung von neuen Geschäftsanforderungen und Digitalisierungsinitiativen gewährleisten?

Massive Cyberbedrohung – sieben essenzielle Handlungsfelder

Wir leben in einer Zeit der maximalen Cyberbedrohung. Daher ist es entscheidend, jetzt die dringenden und wichtigen Handlungsfelder zu priorisieren. Jeder IT-Verantwortliche sollte die folgenden sieben Handlungsanweisungen für sich bewerten und bei Bedarf schnellstmöglich die entsprechenden Gegenmaßnahmen ergreifen.

1 *Sind meine privilegierten Admin-Accounts durch eine starke Authentifizierung und Autorisierung vor unberechtigter Nutzung geschützt?*

Warum ist dies wichtig?

- Wo auch immer die Angreifer eindringen, sie wollen IMMER die Admin-Rechte von kritischen Systemen erlangen. Ganz besonders kritisch sind Active Directory, Windows Domain Controller und Backup-Systeme.
- Nutzername und Passwort sind kein ausreichender Schutz.

Wie kann ich das umsetzen?

- Multifaktor-Authentifizierung und Autorisierung von privilegierten Admin-Accounts vor dem Zugriff auf die Systeme als absolute Pflicht einführen.
- Idealerweise wird dabei der Kontext des Zugriffs (von welchem Ort wird der Zugriff angefragt) – und die Vertrauenswürdigkeit vom genutzten Endgerät beim Request geprüft.
- Das Einrichten dieser Fähigkeiten sollte für alle Arten von Systemen sehr einfach und schnell möglich sein.
- Dabei sollte der User selbst entscheiden können, welchen zweiten Faktor er nutzen möchte (Nutzerzufriedenheit ist essenziell).

2 *Sind alle VPN-Zugänge in das eigene Netzwerk durch eine starke Authentifizierung und Autorisierung geschützt?*

Warum ist dies wichtig?

- Die Nutzung von VPN-Zugängen ist einer der Hauptangriffsvektoren, nachdem persönliche Anmeldedaten in die Hände der Angreifer gelangt sind.
- Die VPN-Anmeldung über Nutzername und Passwort ist kein ausreichender Schutz, da die Identität des Users nicht überprüft werden kann.
- Befindet sich der Angreifer per VPN im Netzwerk, verfügt er über alle Möglichkeiten, sich unbemerkt auszubreiten.

Wie kann ich das umsetzen?

- Zusätzlich zu den unter Frage 1 genannten Umsetzungspunkten:
- Multifaktor-Authentifizierung und Autorisierung bei ***allen*** VPN-Zugängen.

3 *Haben wir eine Übersicht über aktuelle Schwachstellen in unserer IT-Landschaft sowie eine Einschätzung, wie groß die Eintrittswahrscheinlichkeit für uns ist?*

Warum ist dies wichtig?

- Neben dem Faktor Mensch als größtes Cyberrisiko ist die Ausnutzung von Schwachstellen eine leichte Übung für Angreifer.
- Allerdings bilden nicht alle Schwachstellen ein Cyberrisiko. Es gilt, sich auf die kritischsten zu fokussieren, um diese zeitnah zu schließen.
- Sollten außerhalb der eigenen IT (z. B. im Darknet oder in einschlägigen Datenbanken) bereits auffällige Informationen wie E-Mail-Adressen, Nutzernamen und Passwörter oder Hinweise auf eigene Domains existieren, kann dies ein Anzeichen dafür sein, dass man sich bereits im Fadenkreuz der Angreifer befindet.

Wie kann ich das umsetzen?

- Interne und externe Schwachstellen (auch in Domains, die nicht unter meiner Kontrolle sind) kontinuierlich scannen, bewerten und bei großer Eintrittswahrscheinlichkeit (bekannter und beliebter Angriffsvektor) schnellstmöglich schließen.
- Externe Quellen wie das Darknet oder externe Organisationen auf Auffälligkeiten kontinuierlich überprüfen, bewerten und schnellstmöglich reagieren.
- Durchführung von Penetration Tests, um die eigene Angreifbarkeit zu überprüfen.

4 *Haben wir einen DNS-Schutzschirm zum Internet etabliert, um Anomalien und Angriffsversuche frühzeitig zu erkennen und zu blockieren?*

Warum ist dies wichtig?

- Eine Firewall ist ein guter, aber kein ausreichender Schutz vom und zum Internet.
- Höchste Gefahr besteht, wenn Angreifer gestohlene Daten wie eine Kopie des Active Directory in Form von kleinen Datenpaketen abgreifen.
- Ein DNS-Schutzschirm kann dies erkennen und blockieren, gerade wenn die Firewall keinen ausreichenden Schutz bietet.

Wie kann ich das umsetzen?

- Anstatt einen x-beliebigen externen DNS-Resolver zu nutzen, sollte ein DNS-Security-Resolver eingesetzt werden.
- Ohne großen Eingriff in die eigene IT kann die Umstellung auf den externen DNS-Schutzschirm innerhalb weniger Minuten erfolgen (optional nur im Monitoring-Modus, um Sichtbarkeit zu erlangen).
- Es ist ratsam, den DNS-Schutzschirm auf allen Endgeräten zu etablieren, um ortsunabhängig auffällige Verbindungen zum oder aus dem Internet zu blockieren, zu reglementieren oder zu überwachen.

5 *Haben wir im eigenen Netzwerk eine Netzwerk-Anomalie-Erkennung anhand der Netflow-Daten etabliert?*

Warum ist dies wichtig?

- Oft können sich Angreifer nach einem ersten Eindringen völlig unbemerkt über Wochen und Monate hinweg im internen Netzwerk bewegen, um weitere Schwachstellen auszuloten.
- Je früher auffällige Querbewegungen im internen Netzwerk erkannt werden, umso schneller lassen sich Gegenmaßnahmen durchführen, um größere Schäden zu vermeiden.
- Eine Netzwerk-Anomalie-Erkennung liefert ähnlich wie eine Black-Box im Flugzeug auch in der Retrospektive nützliche Hinweise. Das vereinfacht die Reaktion im Falle eines Angriffs erheblich.

Wie kann ich das umsetzen?

- Die vorhandenen Netflow-Daten von Switches und Routern sind durch eine Netzwerk-Anomalie-Erkennung kontinuierlich auszuwerten, idealerweise angereichert durch weitere Datenquellen wie Webproxy etc.
- In einer „Einschwingphase“ von ca. vier Wochen kann das Netzwerk im Monitormodus Visibilität schaffen.
- Bekannte Cyberangriffe werden sofort geblockt, nach der Einschwingphase auch jegliche Auffälligkeiten.

6 *Sind für den Eintritt eines Vorfalls Spezialisten im Incident & Response Management verfügbar, im Sinne eines Notdienstes, den ich jederzeit anrufen kann?*

Warum ist dies wichtig?

- Die Frage ist nicht mehr, ob man angegriffen wird, sondern nur wann. Dafür wird es niemals einen hundertprozentigen Schutz geben.
- Nachdem ein Vorfall erkannt wurde, ist Zeit der entscheidende Faktor, um den Schaden so gering wie möglich zu halten.
- Angesichts der stark zunehmenden Anzahl von Cyberangriffen ist die Verfügbarkeit von Spezialisten im Incident & Response Management extrem wichtig.

Wie kann ich das umsetzen?

- BSI-verifizierten Incident & Response Service nutzen.
- Der Incident & Response Service sollte Teil eines größeren Notfallplans sein.
- Ein guter Incident & Response Service zeichnet sich aus durch
  - einen Rund-um-die-Uhr-Service (24x7x365) und einer großen Anzahl von Spezialisten, die alle Fachrichtungen abdecken.
  - Verfügbarkeit einer Global Threat Intelligence-Fähigkeit
  - Pro-aktive Unterstützungsleistungen

7 *Ist unser Backup ausreichend geschützt und aktualisiert?*

Warum ist dies wichtig?

- Angreifer versuchen fast immer, einen Admin-Zugriff auf das Backup zu erhalten, um es zu verschlüsseln.
- Bei einem verschlüsselten Backup ist die Wiederherstellung ohne den Schlüssel unmöglich, wenn es keine weitere Datensicherung gibt.

Wie kann ich das umsetzen?

- Das Backup sollte sich in einem eigenen Netzwerksegment befinden, welches durch eine Firewall geschützt ist und nur berechtigten Datenverkehr zulässt.
- Der Admin-Zugang zum Backup-System ist durch MFA zusätzlich zu schützen (siehe Frage 1).
- Das Backup selbst sollte gegen Cyberangriffe geschützt sein (z. B. durch nichtveränderbare Backups ohne Zugriff von außen).
- Es empfiehlt sich die Umsetzung einer 3-2-1 Backup-Strategie: drei Kopien oder Versionen, auf mindestens zwei verschiedenen Speichermedien und eine Kopie an einem entfernten Standort.

Zusammenfassung

1. Angesichts der massiven Bedrohungslage sind die essenziellen sieben Handlungsfelder zu prüfen und bei Bedarf Schutzmaßnahmen schnellstmöglich umzusetzen. Wird diese Aufgabe nicht ausreichend erfüllt oder nicht als dringend erachtet, muss sich die Einrichtung der Tatsache bewusst sein, dass die Wahrscheinlichkeit für einen Cyberangriff deutlich erhöht ist.

2. Sind die Sofortmaßnahmen implementiert, ist eine organisationsübergreifende Klarheit und Orientierung zu schaffen, idealerweise verbunden mit einer Fortbildung, damit alle das entsprechende Basiswissen besitzen, artikulieren und auch kommunizieren können.

3. Ein programmatischer Ansatz hilft, erste gemeinsame Schritte zu definieren und zu priorisieren, um entsprechend der eigenen Risikobereitschaft in geeignete operative und technische Fähigkeiten zu investieren.

Impressum
Cisco Systems GmbH
Parkring 20
D-85748 Garching
Tel.: 0800 - 187 36 52
www.cisco.de

Konzept, Text
Fink & Fuchs AG

Gestaltung
Fink & Fuchs AG

Bildnachweise
Seite 1, 2, 3, 6 Cisco
Seite 5 GettyImages