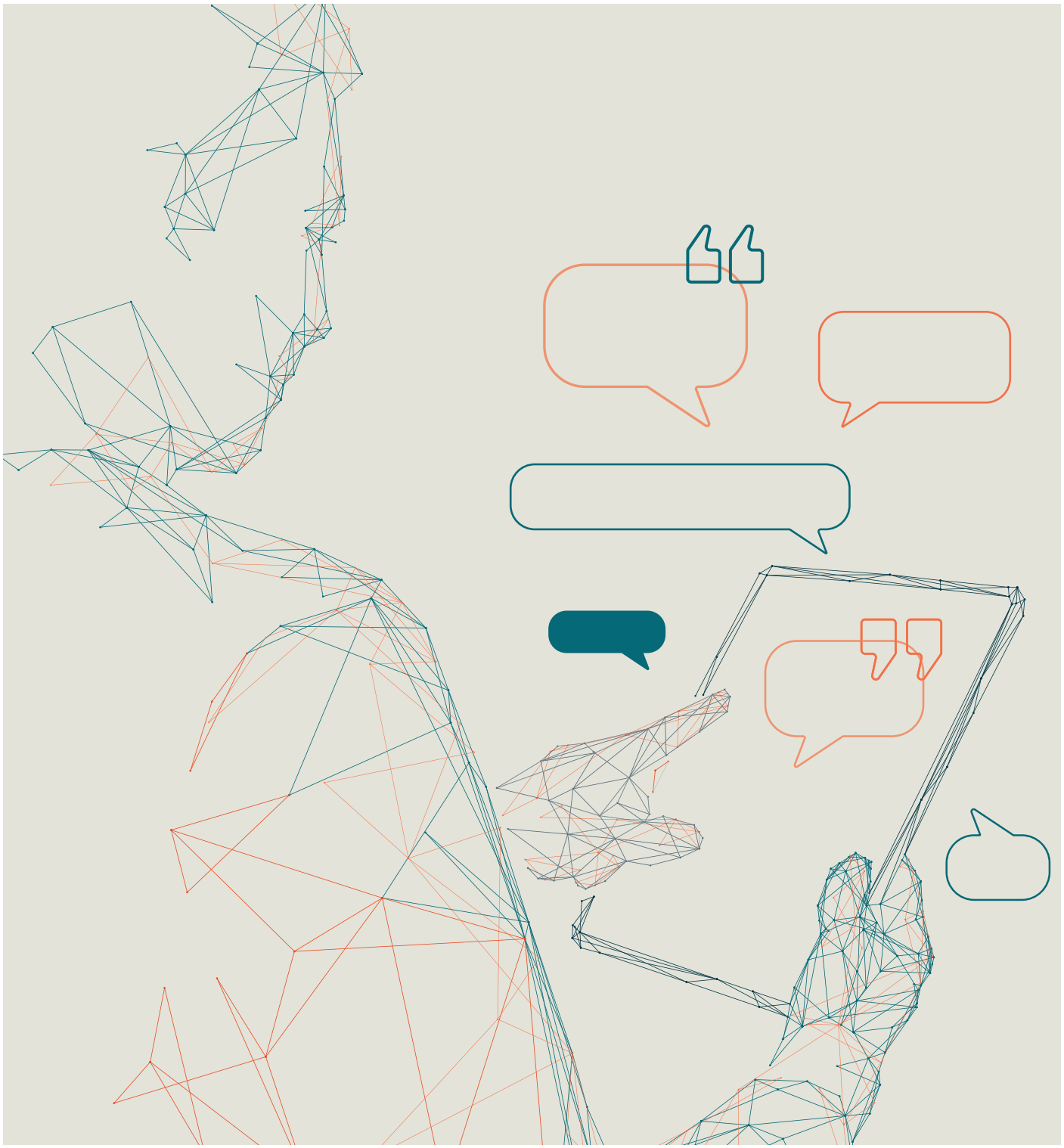
Cybersicherheit für Hochschulen, Universitäten und Forschungseinrichtungen

EVIDEN



Hochschulen und Universitäten sind Keimzellen und Inkubatoren für Generationen von Fachleuten, für Ideen und Fortschritt. Forschungseinrichtungen, oftmals eng mit Universitäten verbunden, eröffnen neue Horizonte in Wissenschaft und Technik mit konkreten Ergebnissen.

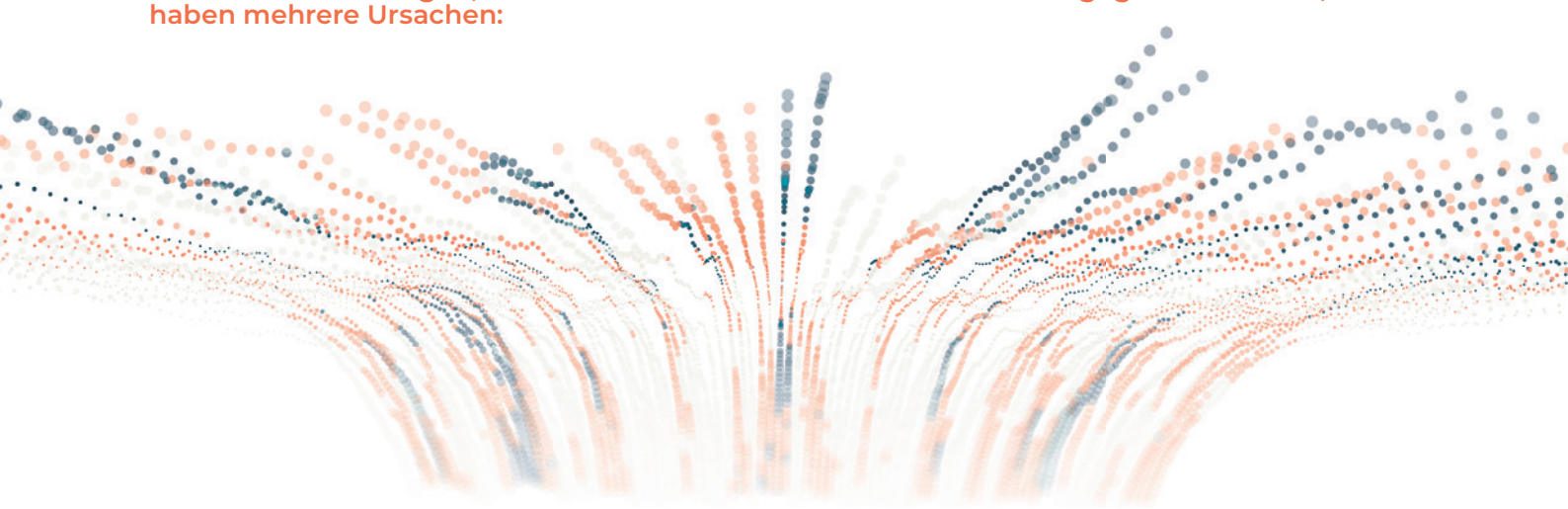
IT-Systeme – lokal und cloudbasiert – sind ein unverzichtbarer Dreh- und Angelpunkt für deren effiziente Arbeit. Die zahlreichen und anspruchsvollen Nutzer arbeiten mit ihnen unter anderem an organisatorischen, fachlichen oder Kommunikationsthemen.

Sensible Daten werden verarbeitet, die Integrität und der ordnungsgemäße Gebrauch sowie die Nutzbarkeit der Systeme muss sichergestellt werden. Cybersicherheit ist im täglichen Geschäftsbetrieb von Hochschulen, Universitäten und Forschungseinrichtungen eine komplexe Herausforderung.

Insbesondere die deutschen Hochschulen und Universitäten werden seit 2019 massiv angegriffen. Zum einen verfügen sie über sehr wertvolle (Foschungs-)Daten und sind ein reizvolles Ziel, zum anderen weisen sie eine komplexe und schwer zu schützende IT-Infrastruktur auf und sind dadurch mitunter auch ein vergleichsweise leichtes Ziel.

Aktuelle Herausforderungen

Die Herausforderungen, denen sich Hochschulen und Universitäten gegenüber sehen, haben mehrere Ursachen:



1. Heterogenität

Die Benutzerbasis im Umfeld von Hochschulen und Universitäten ist sehr heterogen. Mitarbeiter der Hochschule, externe Mitarbeiter, studentische Hilfskräfte, und nicht zuletzt die naturgemäß **ständig fluktuierenden** Studierenden haben Zugriff auf die Netzwerke. Das Bewusstsein für Cybersicherheit ist in den Nutzergruppen sehr unterschiedlich und insbesondere in den Bereichen mit hoher Fluktuation oft nur rudimentär ausgeprägt, aber genau dort auch sehr schwer aufzubauen. **Phishing und Social Engineering** finden hier oft fruchtbaren Boden.

Und so heterogen wie die Nutzerbasis sind in weiten Teilen auch die Gerätschaften mit denen zugegriffen wird. **Bring Your Own Device** (BYOD) ist für die Studierenden an der Tagesordnung und damit eine **bunte Welt aus allen möglichen Geräten, Betriebssystemen, Versionsständen, Konfigurationen** und somit auch **Sicherheitszuständen.**

2. Fehlende zentrale Kontrolle

Die Grenzen zwischen „interner IT“ und „öffentlichem Bereich“ sind oft fließend. Der Zugang zu Informationen und Systemen soll für alle Beteiligten leicht und ohne großen Aufwand möglich sein. Doch die **Verantwortung für die verschiedenen Systeme liegt oft in unterschiedlichen Händen**. Neben übergreifenden Systemen für die gesamte Hochschule sind in den verschiedenen Fachbereichen, Fakultäten, Instituten, Laboren, Einrichtungen, etc. häufig IT-Systeme etabliert, die nicht einer zentralen Verantwortung bzw. Kontrolle unterliegen, aber dennoch an das „Hochschulnetz“ angebunden sind. Zusätzlich erhöht die übliche Einbindung in einen großen Netzwerk- und Kommunikationsverbund von Hochschulen, Universitäten, Forschungsein-richtigungen, etc. die Komplexität der Cybersicherheitsherausforderungen.

3. Schutzbedarf und Ressourcen

Der Schutzbedarf dieser verschiedenen Netze und Systeme ist sehr unterschiedlich. Oftmals steht die Zugänglichkeit und „einfache Nutzbarkeit“ der Systeme im Vordergrund, nicht nur aus der Perspektive der Systemanwender, sondern auch aus Sicht der Systemverantwortlichen, die nur **wenig Ressourcen** (Fachpersonal und finanzielle Mittel) haben, um komplexe Zugangsmechanismen aufzubauen, zu pflegen und zu überwachen.

Doch auch in der IT einer Hochschule werden **sensible und schützenswerte** Daten verarbeitet. Neben personenbezogenen **Daten** verschiedenster Ausprägung sind dies die **Forschungsergebnisse** und **geistiges Eigentum**, insbesondere bei Kooperationen mit oder Beauftragungen durch Unternehmen und Behörden. Auch die Einhaltung von regulatorischen Vorschriften wird aufgrund der Vielfalt der Daten und Nutzer immer komplizierter.

4. Veraltete Systeme

Auch wenn moderne Hochschulen es nicht gerne zugeben, so sind doch oftmals noch „**Legacy Systems**“ im Einsatz - mit allem, was das aus der Cybersicherheitsperspektive mit sich bringt – von veralteten und damit unsicheren Protokollen bis zum nicht mehr vorhandenem Herstellersupport und der damit entfallenen Versorgung mit Sicherheitsupdates. Auch die Integration solcher Legacy Systeme in eine moderne Cybersicherheitsarchitektur ist oftmals eine Herausforderung.

Besonderheiten bei Forschungseinrichtungen

Aufgrund der anders gelagerten Schwerpunkte sollten bei Forschungseinrichtungen die folgenden Punkte ergänzend berücksichtigt werden:

1. Ruf und Vertrauen

Neben drohendem unberechtigtem Abfluss bzw. dem Verlust von wertvoller Information (z.B. durch Ransomware) spielt der Ruf und das Vertrauen in eine Forschungseinrichtung eine wesentliche Rolle in Bezug auf Finanzmittel, Partnerschaften und Talente.

Im Kern steht dabei die Wahrung der akademischen Integrität durch Schaffen von Nachvollziehbarkeit und durch Verhinderung von Datenmanipulationen bzw. Datenfälschungen, die die Glaubwürdigkeit der Forschungsergebnisse beeinträchtigen können. Viele Forschungseinrichtungen erhalten Fördermittel von Regierungsbehörden und anderen Stellen, die oft mit Anforderungen an die Cybersicherheit und den Datenschutz verbunden sind.

2. Kontinuität von Forschungsaktivitäten

Forschungsaktivitäten sind der Kern des Geschäftsbetriebes von Forschungseinrichtungen. So trivial das klingt, so klar bringt es auf den Punkt, warum es gilt, Behinderung und/oder Unterbrechung der Forschungsaktivitäten durch Cybervorfälle wie Ransomware-Angriffe oder Datenschutzverletzungen zu verhindern bzw. ihre Auswirkungen zu minimieren.

3. Aktive Abwehr zum eigenen Schutz und dem der Partner

Die aktive Reaktionsfähigkeit auf Security Incidents ist für Forschungseinrichtungen besonders wichtig, denn neben den bereits genannten Gründen ist die enge Zusammenarbeit mit anderen Organisationen ein wichtiger Aspekt. Diese baut auf effektive Kommunikation und Zusammenarbeit mit externen Partnern. Doch über diese Wege können auch Sicherheitsvorfälle „überspringen“, was unbedingt vermieden werden muss. Rasches, konsequentes Erkennen und Eindämmen von Sicherheitsvorfällen ist unbedingt erforderlich.

Zentrale Handlungsfelder

Im Bereich Cybersicherheit für Hochschulen, Universitäten und Forschungseinrichtungen ergeben sich drei Handlungsfelder, die abhängig von der Art der Organisation unterschiedlich stark gewichtet werden:

Hochschulen / Universitäten

Übergreifende sichere Identifizierung und **Authentifizierung** der Benutzer und **angemessener Zugriffsschutz**	Kontinuierlicher **fundierter Einblick** in **„was passiert in unserer Umgebung“**	**Vorbereitet sein auf den Fall der Fälle - Reaktionsfähigkeit bei Angriffen und Cyber Security Incidents**

Forschungseinrichtungen

Unerlässlich: die Konzentration auf Fokuspunkte

Der Grundsatz der Cybersicherheit, dass singuläre Maßnahmen zwar nicht per se sinnlos sind, aber nur im wohlstrukturierten, orchestrierten Zusammenspiel zum Erfolg führen, gilt auch im Bereich der Lehre und Forschung. Dennoch macht es Sinn, **Fokuspunkte zu setzen, um sich bei der Betrachtung der eigenen Cybersicherheit nicht zu verzetteln**. Für Hochschulen und Universitäten einerseits und Forschungseinrichtungen andererseits ergeben sich unterschiedliche Schwerpunkte mit gemeinsamen Handlungsfeldern:

Handlungsfeld 1: Gebündelte Kontrolle

Um die Basis für eine **übergreifende sichere Identifizierung und Authentifizierung** der Benutzer und einen **angemessenen Zugriffsschutz** zu legen, bietet sich für Hochschulen, Universitäten und Forschungseinrichtungen die Einführung und konsequente Nutzung von **Single Sign On (SSO)** an.

Bei SSO authentifiziert sich der Nutzer zentral bei einem „Identity Provider“, der auch die Berechtigungen des Nutzers prüft. Bei erfolgreicher Authentifizierung und passenden Berechtigungen wird dem Nutzer ein Token ausgestellt, das den Zugang zu einem oder mehreren Diensten ermöglicht.

Durch SSO werden Administratoren in die Lage versetzt, zentral Benutzerkonten, wie auch Zugriffe auf verschiedene Ressourcen, bereitzustellen und zu verwalten. So wird nicht nur der Onboarding-Prozess deutlich vereinfacht, auch wenn ein Mitarbeiter oder Student die Einrichtung verlässt, kann sein Zugriff auf alle Systeme mit einer einzigen Aktion sofort widerrufen werden.

Generell reduziert SSO die Risiken im Zusammenhang mit unbefugtem Zugriff, Angriffen mit Zugangsdaten und Datenschutzverletzungen, da sie einen **robusteren und zentralisierten Ansatz für die Zugangsverwaltung** bietet und zudem die Wahrscheinlichkeit verringert, dass schwache Passwörter verwendet werden.

SSO muss nicht als Big Bang eingeführt werden. Zwar können im Endausbau alle Systeme einschließlich Studentenportalen, Anwendungen für Lehrende und Mitarbeiter sowie Verwaltungssysteme durch SSO einheitlich geschützt werden, SSO kann aber schrittweise eingeführt werden, z.B. zunächst für die Mitarbeiter der Hochschule/Universität und erst in weiteren Schritten für die Studierendenschaft.

Grundsätzlich gilt: Gerade im Zusammenspiel mit SSO sollte auch der **Einsatz von Multi-Faktor-Authentisierung (MFA)** in Erwägung gezogen werden.

MFA trägt dazu bei, die **Risiken von auf Anmeldeinformationen basierenden Angriffen** wie Phishing, Brute-Force-Angriffen und Passwort-Spraying zu

mindern, denn selbst wenn das Passwort eines Benutzers kompromittiert ist, ist ein zusätzlicher Authentifizierungsfaktor erforderlich, um Zugang zu erhalten. In der modernen Welt hat faktisch jeder Benutzer ein Smartphone zu Hand, das über entsprechende kostenlose Apps als „Faktor" für die Multifaktorauthentifizierung dienen kann.

Selbst wenn kein SSO zum Tragen kommt, so ist der **Einsatz von MFA für bestimmte Bereiche absolut zu empfehlen**. Für sensible Daten, darunter Forschungsdaten, personenbezogene Daten und Finanzdaten, fügt MFA eine zusätzliche Schutzebene hinzu, um unbefugten Zugriff auf diese Daten zu verhindern.

Eine wesentliche Rolle können im Kontext der MFA auch **digitale Zertifikate** spielen, wenn sie als starker Faktor zur Authentisierung genutzt werden. Das ist nur ein, allerdings sehr wichtiger, Mehrwert einer **Public Key Infrastruktur (PKI)**, die zum Erstellen und Verwalten dieser Zertifikate notwendig ist. Generell ist die Etablierung einer PKI im eigenen Ökosystem zur Cybersicherheit im Kontext **sicherer Identitäten** (für Personen, Maschinen, Services und vieles mehr) sehr zu empfehlen.

Gerade bei **„Nicht-Büro-Umgebungen", wie in Laboren, Messständen, etc. kann auch die Nutzung von Wearables als Authentisierungsfaktor** zielführend sein, da z.B. notwendige Schutzkleidung oder widrige Umgebungsbedingungen die sonst üblichen Methoden (wie beispielsweise eine Authentifizierungs-App auf einem Smartphone) erschwert oder gar unmöglich macht. Mittels „Wearable"-Geräten, wie intelligente Armbänder mit kontaktloser Verbindung, können Benutzer durch Annäherung authentifiziert werden. Durch Einsatz biometrischer Technologie erfolgt die sichere Identifizierung und Authentifizierung der jeweiligen Person.

Handlungsfeld 2: Fundierter Einblick und aussagekräftige Erkenntnisse

Aufgrund der Heterogenität der IT-Landschaft von Hochschulen und Universitäten in Struktur, Nutzerschaft, Verantwortlichkeit, Schutzbedarf, etc. ist es unabdingbar, kontinuierlich fundierten Einblick zu haben und cybersicherheitsrelevante Vorgänge zu erkennen. Auch bei Forschungseinrichtungen **darf ein Security-Incident nicht erst durch seine Auswirkungen bemerkt werden**.

Durch den Einsatz eines **Security Information and Event Management (SIEM)** Systems, das Protokoll- und Ereignisdaten von den verschiedenen Systemen und Anwendungen aus der gesamten IT-Landschaft der Hochschule sammelt und kondensiert, wird die Grundlage geschaffen, um aus der Flut von Information potenziell security-relevante Vorgänge, wie z.B. unbefugte Zugriffsversuche, Malware-Infektionen oder ungewöhnlichen Netzwerkverkehr zu erkennen.

Das SIEM liefert dabei eine Informationsbasis, die durch **versierte Auswertung der Informationen** einen Mehrwert bietet. Hier kommt das **Security Operation Center (SOC)** zum Zuge. Sicherheitsanalysten im SOC werten die Informationen aus, identifizieren potenzielle Sicherheitsbedrohungen und stoßen geeignete Gegenmaßnahmen an.

Diese **hochspezialisierten Experten** sind ein rares Gut, der Aufbau einer eigenen SIEM/SOC Umgebung ein aufwändiges und teures Unterfangen. Denn es müssen nicht nur die technischen Aspekte, sondern auch die organisatorische Seite berücksichtigt werden. Damit ein SOC effektiv und effizient arbeiten kann, muss ergänzend zu der SIEM-Umgebung auch der Rest der „SOC Workbench" etabliert werden. Hierzu gehören beispielsweise Security Orchestration, Automation and Response (SOAR) Systeme, sowie Threat Intelligence. Und die kontinuierliche Organisation einer **24x7 Überwachung** durch Security Experten ist ebenso herausfordernd.

Daher ist „Managed SIEM/SOC" ein Baustein, den Hochschulen, Universitäten und Forschungseinrichtungen sinnvollerweise **bei einem Cyber Security Dienstleister als Service einkaufen**.

Handlungsfeld 3: Vorbereitet sein auf den Fall der Fälle

Das Gleiche gilt auch für den Bereich der **Incident Response**. Hier bedarf es in noch stärkerem Maße versierter Fachleute, denn es gilt **bei einem laufenden Cyberangriff das Richtige zu tun**.

Um das klar auf den Punkt zu bringen: Ein **akuter Cyberangriff** bedeutet eine ausgewachsene **Krisensituation**!

Es gilt, einen **kühlen Kopf zu bewahren, das Risiko einzustufen und die richtigen Schritte einzuleiten**. Dieses „operative Krisenmanagement" ist ein wesentlicher Erfolgsfaktor für die Abwehr eines laufenden Cyberangriffs bzw. die Schadensbegrenzung durch gezielte Maßnahmen. Außerdem ist es wichtig, strukturiert Artefakte zu sammeln und Beweise zu sichern. Schließlich muss ein Vorfall analysiert und es müssen Lessons Learned abgeleitet werden, damit man gestärkt aus der Krise hervor gehen kann.

Dafür die **notwendigen Experten** in der benötigen Anzahl und Güte vorzuhalten ist für eine einzelne Organisation nicht abbildbar. Zwar kann und soll man sich technisch und organisatorisch auf den Ernstfall vorbereiten – beispielsweise durch **professionell durchgeführte Krisenplanspiele** – aber wenn es darauf ankommt, **braucht man Profis für die akute Umsetzung**. Hier sollten **vereinbarte Servicelevel** in Erwägung gezogen werden, damit der Dienstleister im Bedarfsfall auch wirklich helfen kann.

Schlussfolgerungen

Das **wohlstrukturierte, orchestrierte Zusammenspiel von Cybersicherheitsmaßnahmen ist der Schlüssel zum Erfolg**. Da es keine hundertprozentige Sicherheit geben kann, bleibt es immer eine Risikobetrachtung und eine Abwägung zwischen Aufwand und potenziellem Schaden.

Es gilt die Bereiche der Cybersicherheit in Angriff zu nehmen, die für die eigene Situation den besten Effekt erzielen und dann von dieser Basis ausgehend **das Gesamtbild auf- und auszubauen - entsprechend dem eigenen Bedarf bzw. der eigenen Risikoaffinität**.

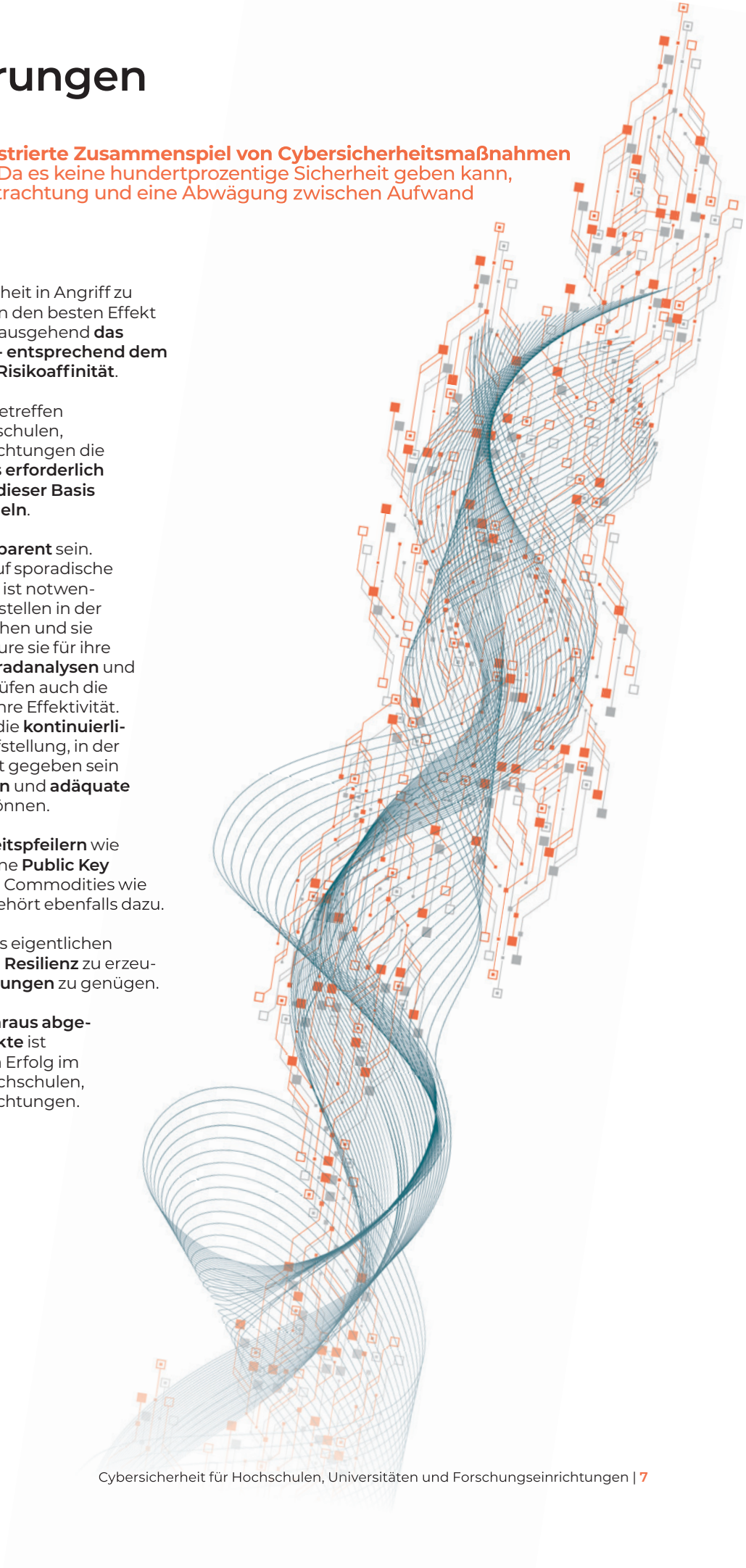
Die hier genannten Fokuspunkte betreffen wesentliche Bereiche, die für Hochschulen, Universitäten und Forschungseinrichtungen die Basis bilden sollten. **Dennoch ist es erforderlich in Bezug auf Cybersicherheit von dieser Basis aus weiter zu denken und zu handeln**.

Der **eigene Status Quo** sollte **transparent** sein. Diese Transparenz darf sich nicht auf sporadische Momentaufnahmen begrenzen. Es ist notwendig, **regelmäßig proaktiv** Schwachstellen in der Cybersicherheitsaufstellung zu suchen und sie zu erkennen, bevor böswillige Akteure sie für ihre Zwecke ausnutzen können. **Reifegradanalysen** und insbesondere **Penetration Tests** prüfen auch die etablierten "Security Controls" auf ihre Effektivität. So leisten sie wertvolle Dienste für die **kontinuierliche Verbesserung** der eigenen Aufstellung, in der auch die systematische Möglichkeit gegeben sein muss, **Cyber-Incidents zu erkennen** und **adäquate Gegenmaßnahmen** ergreifen zu können.

Der Einsatz von **zentralen Sicherheitspfeilern** wie I**dentity & Access Management**, eine **Public Key Infrastructure** oder vermeintlichen Commodities wie **Netzwerk-** oder **Cloudsicherheit** gehört ebenfalls dazu.

Zur nachhaltigen Sicherstellung des eigentlichen Geschäftsbetriebs gilt es, **faktische Resilienz** zu erzeugen und **regulatorischen Anforderungen** zu genügen.

Die **Gesamtarchitektur und das daraus abgeleitete Design der einzelnen Aspekte** ist entscheidend für den nachhaltigen Erfolg im Ringen um Cybersicherheit der Hochschulen, Universitäten und Forschungseinrichtungen.



Autoren

Henning Kettner
ist Vertriebsleiter bei Eviden und verantwortet die Betreuung und Entwicklung der Bereiche Bundesländer und Kommunen, Lehre und Forschung, Justiz, Kirchen und Wohlfahrt. Er verfügt über fundierte Erfahrung in der Zusammenarbeit mit öffentlichen Institutionen und Non-Profit-Organisationen. Seine Rolle umfasst strategische Vertriebsansätze und die Förderung innovativer Lösungen für den öffentlichen Sektor und die Wohlfahrtspflege.

Paul Frère
ist Cyber Security Consultant bei Eviden und unterstützt Organisationen dabei, ihre Sicherheitsstrategien zu stärken und Risiken zu minimieren. In seiner Rolle berät er zu innovativen Lösungen, die den komplexen Anforderungen moderner IT-Sicherheit gerecht werden und hilft Kunden, ihre Daten und Systeme effektiv gegen Bedrohungen zu schützen.

Sie möchten die bestehenden technischen und betrieblichen Herausforderungen angehen und die Sicherheit Ihrer Organisation erhöhen?

Kontaktieren Sie uns, um einen Gesprächstermin zu vereinbaren!
henning.kettner@eviden.com

Erfahren Sie mehr über unsere Cyber Security Lösungen:
https://eviden.com/de-de/loesungen/digital-security

Connect with us

/in/eviden
@EvidenLive
@evidenlive
/EvidenLive

eviden.com