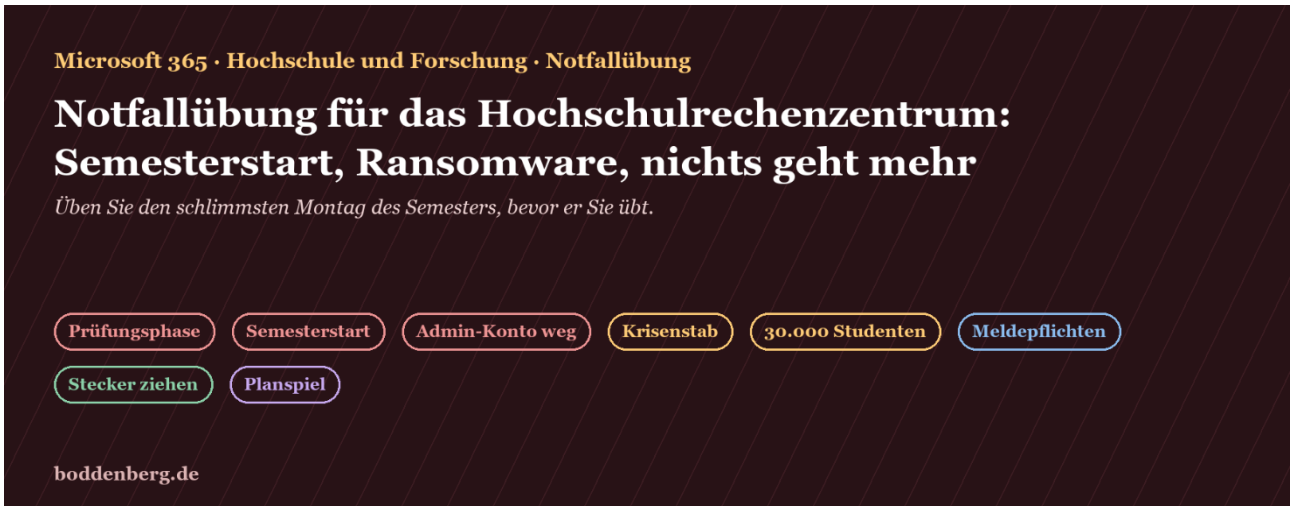
Notfallübung für das Hochschulrechenzentrum: Semesterstart, Ransomware, nichts geht mehr



WISSEN
Alle Beiträge der Serie zu Microsoft 365 in Hochschule und Forschung an einem Ort.
› **Microsoft 365 in Hochschule und Forschung**

BERATUNG
Moderierte Notfall- und Red-Team-Übung für Ihre Hochschule: Drehbuch, Durchführung, Auswertung, Maßnahmenliste.
› **Beratung für Hochschulen und Forschung**

SCHULUNG
Für Rechenzentrum, Krisenstab und Helpdesk: Vorfallsbearbeitung im Tenant, Rollen im Krisenstab, Kommunikation unter Druck.
› **Schulungen für Hochschulen und Forschung**

Montag, 6:40 Uhr, zweite Woche der Prüfungsphase. Beim Helpdesk klingelt das Telefon, dann noch einmal, dann ununterbrochen. Das Prüfungsamt kommt nicht an die Notenlisten, im Dekanat zeigen die Dateien seltsame Endungen, und auf dem Drucker der Kanzlerin liegt ein freundlich formulierter Erpresserbrief mit Kontaktadresse im Darknet. Um 7:30 Uhr erreicht die Rufbereitschaft die Leitung des Hochschulrechenzentrums. Um 7:45 Uhr stellt sich die Frage, die in keinem Handbuch steht: Wer darf jetzt eigentlich entscheiden, das Netz zu trennen, während 1.200 Studenten in den Hörsälen auf ihre Klausur warten?

Wenn Sie diese Frage für Ihre Hochschule heute nicht in einem Satz beantworten können, sind Sie in guter Gesellschaft. Und genau deshalb gibt es Notfallübungen. Nicht, weil Ihr Rechenzentrum sein Handwerk nicht verstünde, sondern weil das Handwerk im Ernstfall nicht das Problem ist. Der Kernsatz dieses Beitrags lautet:

WICHTIG · Der Kernsatz

Große Schäden entstehen selten, weil niemand weiß, wie es geht. Sie entstehen, weil jemand, der es kann, unter Druck den falschen Knopf drückt: das Backup zurückspielt, bevor der Angreifer draußen ist, 40.000 Konten auf einmal zurücksetzt, den infizierten Server neu installiert und damit die Spuren gleich mit, oder um 8 Uhr morgens eine Rundmail verschickt, die um 10 Uhr nicht mehr stimmt.

Dieser Beitrag ist der Abschluss der Serie Microsoft 365 in Hochschule und Forschung. Er beschreibt, wie eine moderierte Notfallübung im Hochschultakt aussieht: drei Planspiel-Szenarien, die zu Semesterkalender und Campus-Realität passen, wer am Tisch sitzen muss, wie Sie 30.000 Studenten erreichen, wenn Mail und Portal tot sind, welche Meldepflichten laufen und welche

Stellen helfen. Er richtet sich an Leitungen von Hochschulrechenzentren, CIOs, Kanzlerinnen und Kanzler, Dezernate, Datenschutzbeauftragte und Personalräte, ausdrücklich auch an außeruniversitäre Forschungseinrichtungen. Universitätsklinika spielen als Teil des Gesundheitswesens in einer eigenen Liga und bleiben hier außen vor.

FAKTEN · Das Wichtigste in Kürze

Ein Planspiel (Tabletop-Übung) übt Entscheidungen, nicht Technik. Drei bis vier Stunden mit den richtigen Personen am Tisch decken mehr Lücken auf als jedes Notfallhandbuch, das seit 2019 im Wiki liegt.

Die drei Hochschul-Szenarien: Verschlüsselung in der Prüfungsphase, Ausfall des Identitätsdienstes zum Semesterstart, kompromittiertes Administratorkonto.

Die wichtigste Maßnahme nach fast jeder Übung ist eine Vorabermächtigung: schriftlich festgelegt, wer was ohne Rückfrage trennen darf und was nie ohne Krisenstab passiert.

Meldepflichten laufen parallel: Gegenüber der Datenschutzaufsicht gilt nach Art. 33 DSGVO grundsätzlich die 72-Stunden-Frist. Ob zusätzlich das BSI-Gesetz greift, hängt von Rechtsform und Sektor ab und ist für die meisten staatlichen Hochschulen nicht der Fall, für manche Forschungseinrichtung aber durchaus.

Warum Hochschulen den Ernstfall üben müssen

Hochschulen sind in den vergangenen Jahren wiederholt Opfer von Ransomware geworden, mit Ausfällen, die nicht in Stunden, sondern in Wochen und Monaten gemessen wurden. Warum der Campus ein so dankbares Ziel ist, beschreibt der Beitrag Microsoft-365-Security an Hochschulen: Offene Netze, private Geräte und Konten als Beute ausführlich: offene Netze, unverwaltete Privatgeräte, hohe Fluktuation und verteilte Administratorrechte. Dieser Beitrag beginnt dort, wo die Prävention aufgehört hat zu wirken, also in dem Moment, in dem es trotzdem passiert ist.

Das Notfallhandbuch und die Wirklichkeit

Fast jede Hochschule hat irgendwo ein Notfallkonzept. Es wurde für ein Audit geschrieben, liegt auf einem Dateiserver, der im Ernstfall verschlüsselt ist, und nennt als Ansprechpartner einen Kollegen, der vor drei Jahren an eine andere Universität gewechselt ist. Das ist kein Vorwurf, sondern Naturgesetz: Dokumente, die nie benutzt werden, verrotten. Eine Übung ist der einzige Weg, ein Konzept regelmäßig mit der Wirklichkeit zu konfrontieren, ohne dass die Wirklichkeit gleich zurückschlägt.

Hinzu kommt eine hochschultypische Besonderheit: Entscheidungswege sind kollegial organisiert. Das Präsidium entscheidet, aber die Fakultäten haben eigene Zuständigkeiten, das Prüfungsamt hat Fristen aus Prüfungsordnungen, der Senat möchte informiert werden, und ein Lehrstuhl mit eigenem Server betrachtet diesen nicht unbedingt als Teil der zentralen IT. In der Krise ist für diese Abstimmung keine Zeit. Die Zuständigkeiten müssen vorher klar sein, und das klärt man am besten in einer Übung, in der noch niemand Angst hat.

Planspiel, technische Übung, Red Team: was wann passt

Der Begriff Notfallübung deckt sehr unterschiedliche Formate ab. Für den Einstieg empfiehlt sich fast immer das moderierte Planspiel. Die technischen Formate lohnen sich, wenn die Entscheidungswege stehen und man wissen will, ob die Technik hinterherkommt.

Format	Was geübt wird	Aufwand	Wann sinnvoll
Moderiertes Planspiel (Tabletop)	Entscheidungen, Zuständigkeiten,	Vorbereitung zwei bis vier Wochen, Durchführung drei bis	Als Einstieg und danach jährlich

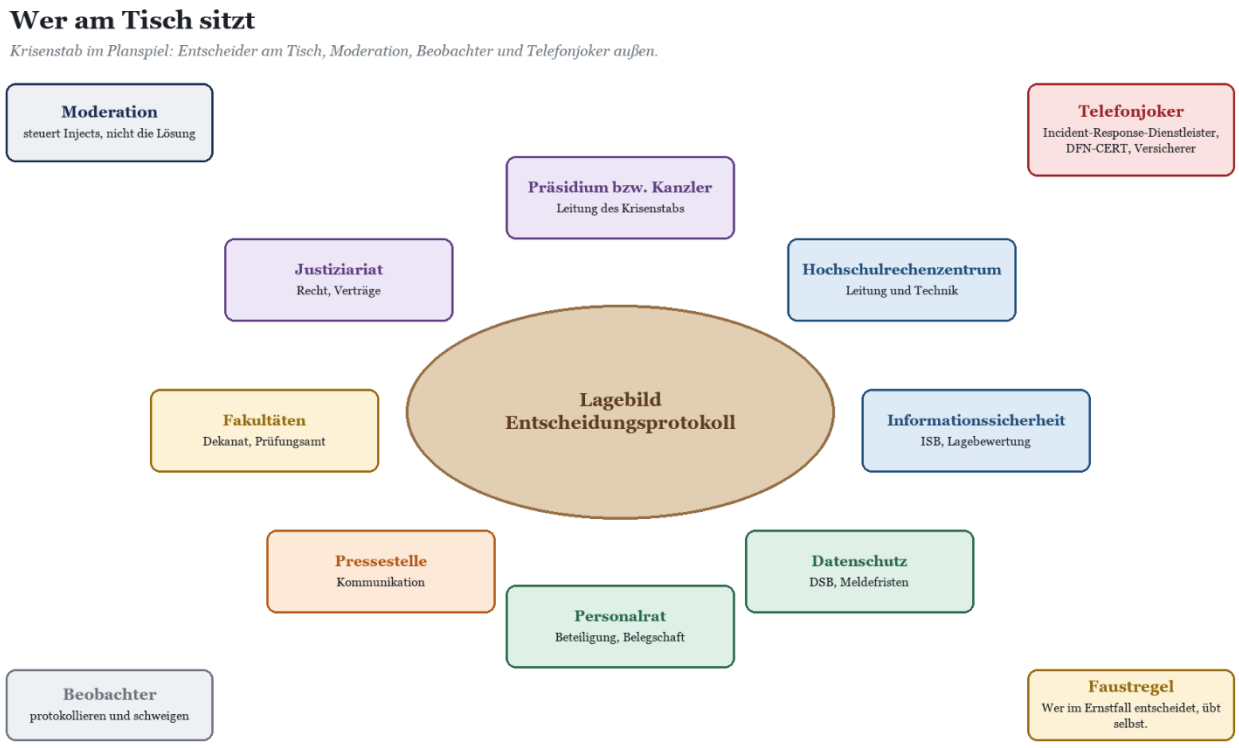
	Kommunikation, Meldewege	vier Stunden	
Technische Wiederanlaufübung	Wiederherstellung aus Backup, Notbetrieb, Reihenfolge des Wiederanlaufs	ein bis mehrere Tage, Testumgebung nötig	Wenn Backup-Konzept und Prioritäten feststehen
Alarmierungsübung	Erreichbarkeit, Telefonketten, Notfallkanäle	gering, unangekündigt möglich	Halbjährlich, gern vor Semesterbeginn
Red-Team-Übung	Erkennung und Reaktion gegen realistische Angreifer	hoch, klare Regeln und Freigaben nötig	Wenn Planspiel und Grundschutz sitzen
Kombinierte Übung	Planspiel, dazu technische Injects aus einem Red-Team-Lauf	hoch	Für Fortgeschrittene, alle zwei bis drei Jahre

TIPP · Klein anfangen, aber ernst

Die erste Übung muss nicht perfekt sein. Ein Szenario, drei Stunden, die richtigen acht Personen und eine Moderation, die nicht zum Rechenzentrum gehört, reichen. Wichtig ist nur, dass das Präsidium die Übung beauftragt und selbst teilnimmt. Eine Übung, zu der die Hochschulleitung ihre Vertretung schickt, übt hauptsächlich das Vertreten.

Wer am Tisch sitzt

Ein Planspiel steht und fällt mit der Besetzung. Die Faustregel ist einfach: Wer im Ernstfall entscheidet, sitzt auch in der Übung am Tisch, persönlich. Die Runde sollte acht bis zehn Personen nicht überschreiten, weil Krisenstäbe mit zwanzig Personen keine Krisenstäbe mehr sind, sondern Informationsveranstaltungen.



Skizze 2: Acht Stühle, ein Protokoll. Mehr Stühle machen den Krisenstab nicht klüger, nur langsamer.

Rolle	Wer typischerweise	Aufgabe im	Typische Lücke in der

		Krisenstab	Übung
Leitung	Präsident bzw. Rektor oder Kanzler	Entscheidet, priorisiert, vertritt nach außen	Weiß nicht, welche Entscheidungen ihm überhaupt vorgelegt werden
Hochschulrechenzentrum	Leitung und eine technische Fachkraft	Lagebild, technische Optionen, Folgen	Erklärt Technik statt Optionen mit Konsequenzen
Informationssicherheit	Informationssicherheitsbeauftragter	Bewertung, Koordination mit externen Stellen	Rolle existiert nur auf dem Papier
Datenschutz	Datenschutzbeauftragter	Bewertung der Meldepflicht, Dokumentation	Wird erst am dritten Tag informiert
Personalrat	Vorsitz oder benanntes Mitglied	Beteiligung bei Maßnahmen, Vertrauen der Belegschaft	Wird als Bremse gesehen statt als Partner
Pressestelle	Leitung Hochschulkommunikation	Kommunikation nach innen und außen	Hat keinen Zugang zu Kanälen ohne eigene IT
Fakultäten	Ein Dekan oder Studiendekan, dazu Prüfungsamt	Folgen für Lehre und Prüfungen	Fristen aus Prüfungsordnungen sind niemandem präsent
Justiziariat	Leitung Rechtsabteilung	Verträge, Haftung, Strafanzeige	Versicherungsbedingungen liegen nicht vor

Moderation und Beobachtung

Die Moderation steuert das Szenario mit sogenannten Injects, also neuen Informationen, die im Verlauf eingespielt werden: der Anruf einer Journalistin, die Mail des Wissenschaftsministeriums, die Nachricht, dass auch die Backups betroffen sind. Sie gibt keine Lösungen vor und rettet niemanden. Gute Moderation erhöht den Druck so weit, dass Lücken sichtbar werden, aber nicht so weit, dass die Runde in Abwehrhaltung geht. Deshalb sollte die Moderation nicht aus dem eigenen Rechenzentrum kommen: Wer morgen wieder mit dem Kanzler zusammenarbeiten muss, spielt ihm heute keinen Erpresserbrief zu.

Beobachter protokollieren, welche Entscheidungen wann und auf welcher Grundlage fielen, wo es hakte und wer auf wen gewartet hat. Sie greifen nicht ein. Ihr Protokoll ist die Grundlage des Berichts und damit der eigentliche Ertrag der Übung.

Personalrat und Datenschutz gehören an den Tisch, nicht ans Ende

In vielen Hochschulen werden Personalrat und Datenschutzbeauftragte im Ernstfall erst informiert, wenn die wichtigsten Entscheidungen gefallen sind. Das ist aus Sicht des Rechenzentrums verständlich und aus Sicht der Hochschule teuer. Ein Vorfall bringt fast immer Maßnahmen mit sich, die die Belegschaft betreffen: Auswertung von Anmeldeprotokollen, erzwungene Kennwortwechsel, Notarbeitsplätze, Überstunden im Rechenzentrum, möglicherweise die Prüfung, ob ein bestimmtes Konto durch Fehlverhalten kompromittiert wurde. Wer diese Fragen vorher mit dem Personalrat geklärt hat, etwa in einer Dienstvereinbarung, die Notfälle

ausdrücklich regelt, gewinnt im Ernstfall Stunden. Die Grundlagen dazu beschreibt der Beitrag Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle.

HINWEIS · Keine Rechtsberatung

Wie weit die Beteiligungsrechte des Personalrats in Eilfällen reichen und ob vorläufige Maßnahmen ohne vorherige Zustimmung zulässig sind, regeln die Personalvertretungsgesetze der Länder unterschiedlich. Bei außeruniversitären Einrichtungen in privater Rechtsform gilt in der Regel das Betriebsverfassungsgesetz. Klären Sie die Eilfallregelung vorab mit Ihrem Justiziariat und dem Personalrat. Dieser Beitrag ersetzt keine Rechtsberatung.

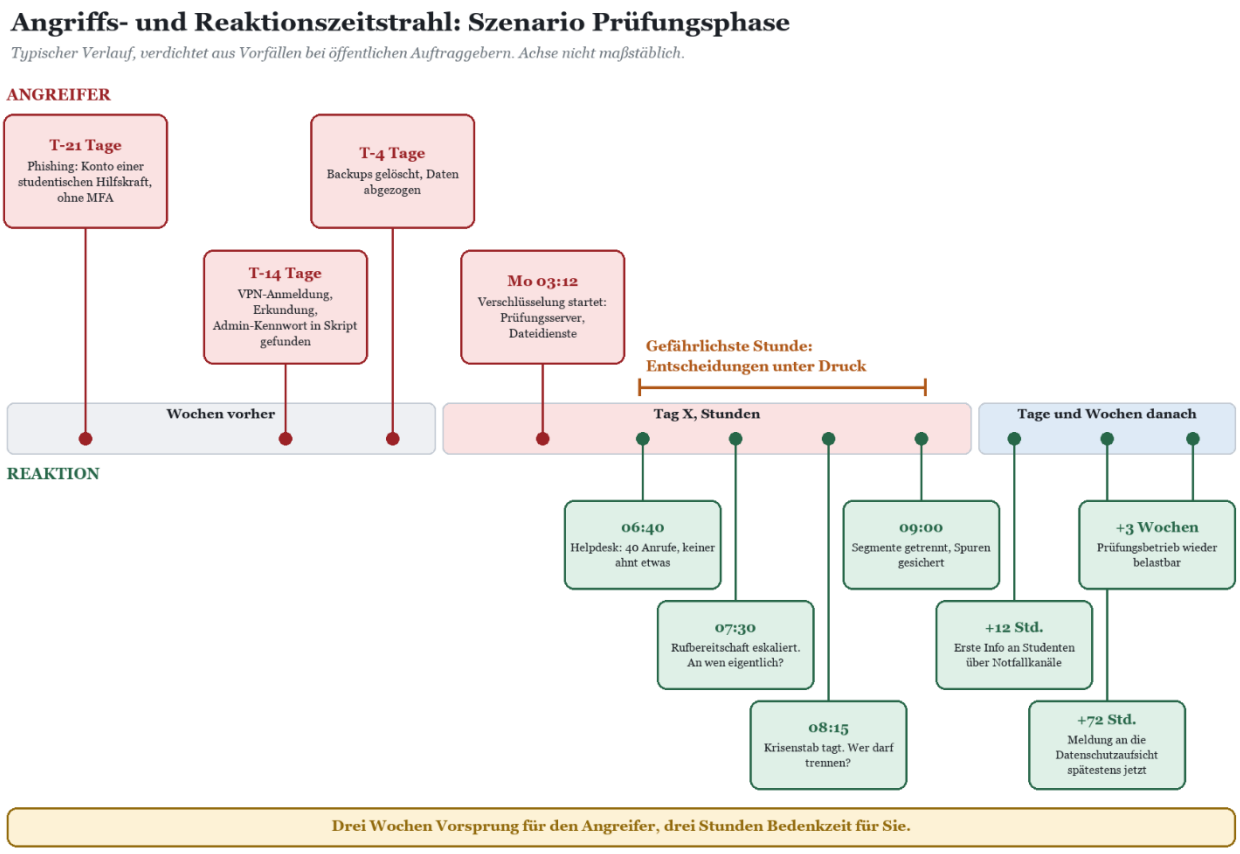
Drei Planspiel-Szenarien im Hochschultakt

Angreifer haben einen Kalender, und er sieht dem akademischen Kalender verdächtig ähnlich. Ein Ausfall in der vorlesungsfreien Zeit im August ist ärgerlich. Derselbe Ausfall in der Prüfungsphase, in der Woche der Rückmeldefrist oder am ersten Vorlesungstag ist eine Krise. Die drei folgenden Szenarien sind deshalb auf Hochschulmomente zugeschnitten, in denen der Druck am größten ist.

Szenario	Übungsziel	Beteiligte	Dauer
Verschlüsselung in der Prüfungsphase	Vorabermächtigung zum Trennen erproben, Prioritäten im Wiederanlauf festlegen, Umgang mit Prüfungsfristen und Lösegeldfrage	Präsidium bzw. Kanzler, Rechenzentrum, ISB, Datenschutz, Personalrat, Pressestelle, Dekanat und Prüfungsamt, Justiziariat	vier Stunden
Ausfall des Identitätsdienstes zum Semesterstart	Notbetrieb ohne zentrale Anmeldung, Kommunikation an Erstsemester ohne Mail und Portal, Notfallzugang für Administratoren	Rechenzentrum, Identitätsmanagement, Pressestelle, Studienberatung, Immatrikulationsamt, Präsidium	drei Stunden
Kompromittiertes Administratorkonto	Erkennung, Eindämmung im Tenant ohne Kollateralschaden, Beweissicherung, Meldepflicht bewerten	Rechenzentrum, ISB, Datenschutz, Personalrat, Fakultäts-IT, Kanzler	drei Stunden

Szenario 1: Verschlüsselung in der Prüfungsphase

Das Ausgangsbild kennen Sie aus der Einleitung. Der Angreifer kam drei Wochen vorher über das Konto einer studentischen Hilfskraft ohne MFA, fand auf einem Dateiserver ein Skript mit einem fest eingetragenen Administratorkennwort, löschte vier Tage vor dem Angriff die erreichbaren Sicherungen und zog Daten ab. Am Montagmorgen startet die Verschlüsselung. Der Zeitstrahl zeigt, wie ungleich die Zeit verteilt ist.



Skizze 1: Der Angriff dauert Wochen, die Entscheidung Minuten. Geübt wird die zweite Hälfte.

Bewährte Injects für dieses Szenario:

- **7:50 Uhr:** Das Prüfungsamt fragt, ob die Klausur um 9 Uhr stattfindet. Die Sitzpläne liegen auf dem verschlüsselten Laufwerk.
- **8:30 Uhr:** Ein Lehrstuhl meldet, sein eigener Server laufe noch. Soll er vom Netz, obwohl dort die Messdaten eines Verbundprojekts liegen?
- **9:15 Uhr:** Ein Kollege aus dem Rechenzentrum schlägt vor, die Dateiserver aus dem Backup von Freitag wiederherzustellen. Es sei doch alles da.
- **10:00 Uhr:** Die Lokalzeitung hat einen Hinweis bekommen und bittet um Stellungnahme bis 11 Uhr.
- **11:30 Uhr:** Auf einer Leak-Seite tauchen erste Dateien aus der Personalabteilung auf, darunter Unterlagen aus einem laufenden Berufungsverfahren.
- **13:00 Uhr:** Das Wissenschaftsministerium bittet um einen Sachstandsbericht und fragt, ob gezahlt werden soll.

Der Inject um 9:15 Uhr ist der Knopf aus dem Kernsatz. Das Backup von Freitag enthält mit hoher Wahrscheinlichkeit den Angreifer, denn der war seit drei Wochen im Netz. Wer jetzt zurückspielt, stellt nicht den Betrieb wieder her, sondern die Ausgangslage des Angreifers, und überschreibt möglicherweise Spuren, die für die Aufklärung nötig sind. Die richtige Antwort ist nicht nein, sondern: noch nicht, erst nach Klärung des Einstiegswegs und in eine saubere Umgebung. Die Übung zeigt, ob jemand am Tisch diese Antwort geben kann und ob die Leitung sie gegen den Druck des Prüfungsamts durchhält. Welche Daten im Tenant besonders schützenswert sind und deshalb beim Leak die schwersten Folgen haben, beschreibt der Beitrag Prüfungsdaten, Berufungsakten, Personalvorgänge: Besonders schützenswerte Daten im Hochschul-Tenant.

WARNUNG · Prüfungsfristen sind kein technisches Problem

Ob eine Klausur verschoben, eine Abgabefrist verlängert oder eine Prüfung ersatzweise mündlich abgenommen werden kann, regeln Prüfungsordnungen und Prüfungsausschüsse, nicht das Rechenzentrum. Klären Sie in der Übung, wer diese Entscheidung trifft und wie sie den Studenten mitgeteilt wird. Sonst entscheidet am Montagmorgen der Hörsaalwart.

Szenario 2: Ausfall des Identitätsdienstes zum Semesterstart

Erster Vorlesungstag, 8.000 Erstsemester haben gerade ihre Zugangsdaten bekommen, die Rückmeldefrist läuft. Um 7 Uhr fällt der zentrale Identitätsdienst aus: Der Verzeichnisdienst vor Ort ist nach einem fehlgeschlagenen Update nicht mehr erreichbar, die Synchronisation nach Entra ID steht, der Shibboleth-Identity-Provider der Hochschule kann niemanden mehr anmelden. Damit sind nicht nur Mail und Teams betroffen, sondern auch das Campus-Management, die Lernplattform, die Bibliothek, das VPN, eduroam und alle Dienste, die über die DFN-AAI angebunden sind.

Dieses Szenario ist kein Angriff, und genau das macht es lehrreich. Es übt die Frage, welche Dienste ohne zentrale Anmeldung weiterlaufen, wer in den Tenant kommt, wenn die Föderation steht, und wie man Erstsemester erreicht, die die Hochschule noch gar nicht kennen. Wie die Anbindung an die DFN-AAI aufgebaut ist und wo die Abhängigkeiten liegen, beschreibt der Beitrag Entra ID und Shibboleth: Microsoft 365 an die DFN-AAI-Welt anbinden.

FAKTEN · Notfallzugang nach Microsoft-Empfehlung

Microsoft empfiehlt in der Entra-Dokumentation zwei oder mehr Notfallzugriffskonten (Emergency Access, Break Glass): reine Cloud-Konten mit der Domäne onmicrosoft.com, weder föderiert noch synchronisiert, keiner einzelnen Person zugeordnet, mit dauerhaft aktiver Rolle des globalen Administrators statt einer nur berechtigten Zuweisung über Privileged Identity Management. Als Anmeldemethode werden phishingresistente Verfahren empfohlen, bevorzugt Passkeys (FIDO2).

Die Konten sind aus Richtlinien für bedingten Zugriff auszunehmen, die die Anmeldung blockieren könnten, und jede Anmeldung mit ihnen soll eine Alarmierung auslösen.

Für das Szenario heißt das: Wenn Ihre Notfallkonten über Shibboleth oder den lokalen Verzeichnisdienst laufen, haben Sie keine Notfallkonten. Sie haben normale Konten mit dramatischem Namen.

Typische Erkenntnis aus diesem Szenario: Die Notfallkonten existieren, aber niemand weiß, wo der FIDO2-Schlüssel liegt, der Tresor steht im verschlossenen Büro einer Kollegin in Elternzeit, und die letzte Testanmeldung war bei der Einrichtung. Prüfen Sie die Konten regelmäßig, und üben Sie die Anmeldung. Wie man solche Altlasten systematisch findet, beschreibt der Beitrag Entra-ID-Überprüfung für Hochschul-Tenants: Was sich nach zehn Jahren Wildwuchs findet.

Szenario 3: Kompromittiertes Administratorkonto

Freitag, 16:20 Uhr. Eine Warnung meldet eine Anmeldung eines Kontos mit Exchange-Administratorrechten aus einem Land, in dem die Hochschule keine Partner hat. Das Konto gehört einem Mitarbeiter der Fakultäts-IT, der für die Postfächer seines Fachbereichs zuständig ist und, wie sich herausstellt, auch globale Rechte hat, weil das 2018 schneller ging. In den letzten zwei Stunden wurden eine neue App-Registrierung mit weitreichenden Berechtigungen angelegt, eine Weiterleitungsregel für das Postfach der Kanzlerin eingerichtet und zwei neue Konten mit Administratorrollen erstellt.

Hier liegt der falsche Knopf besonders nah. Die naheliegende Reaktion, das Konto zu sperren und das Kennwort zurückzusetzen, reicht nicht, denn der Angreifer hat sich längst weitere Zugänge

geschaffen. Die zweite naheliegende Reaktion, alle Administratorkonten auf einmal zu sperren, sperrt im schlimmsten Fall das eigene Team aus und lässt die neuen Zugänge des Angreifers unberührt. Geübt wird die Reihenfolge: Sitzungen widerrufen, das Konto sperren, die neu angelegten Konten, App-Registrierungen, Zustimmungen und Postfachregeln identifizieren und gezielt entfernen, Protokolle sichern, bevor sie altern, und erst dann die Ursache klären. Und alles mit Notfallkonten, die nicht selbst betroffen sind.

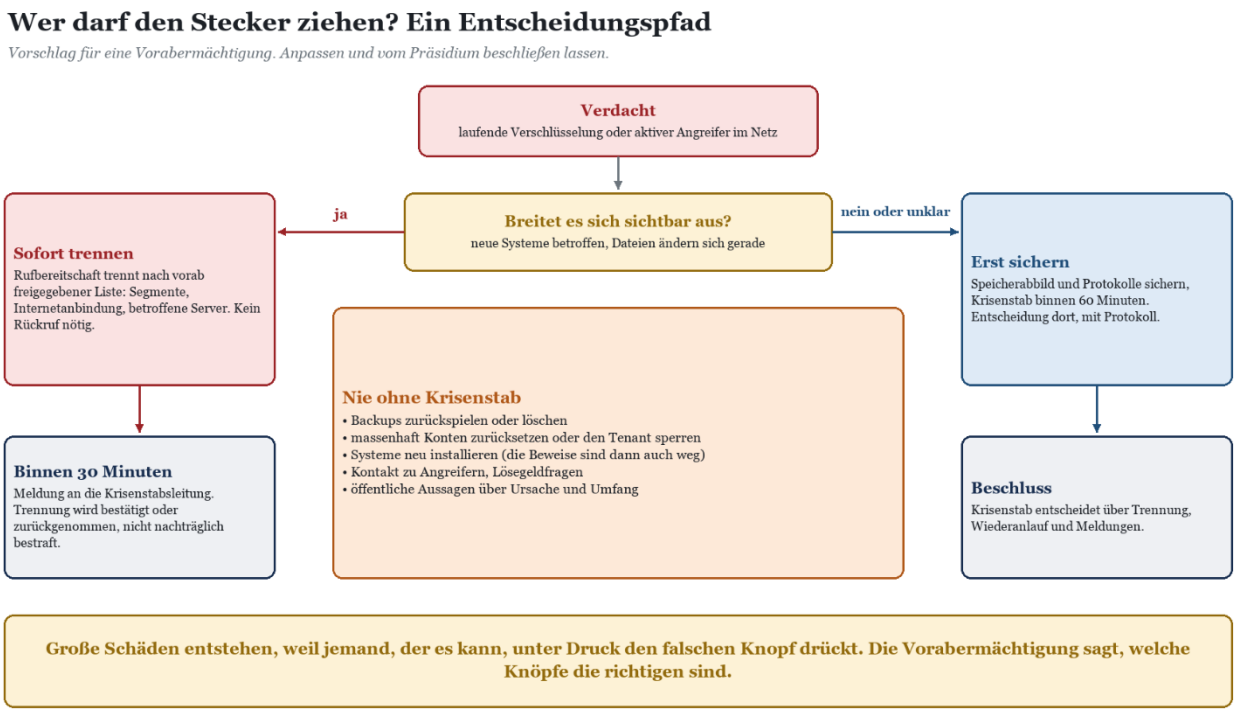
Dieses Szenario ist auch ein Test für die Organisation dezentraler Administration. Wenn Fakultäts-IT und Lehrstuhl-Admins mit zu weitreichenden Rollen arbeiten, ist jedes ihrer Konten ein potenzielles Generalschlüsselkonto. Wie man Rollen auf Verwaltungseinheiten begrenzt, ohne der Fakultäts-IT die Arbeit wegzunehmen, beschreibt der Beitrag Dezentrale IT an der Hochschule: Lehrstuhl-Admins, Fakultäts-IT und ein Tenant für alle; wie phishingresistente MFA für privilegierte Konten durchgesetzt wird, der Beitrag MFA für 30.000 Studenten: Conditional Access an der Hochschule ohne Helpdesk-Kollaps.

TYPISCHE SITUATION · Wer darf den Stecker ziehen?

Aus forensischer Arbeit bei einem Krankenhausverbund, anonymisiert: In der Nacht eines Angriffs war der Administrator in der Rufbereitschaft technisch völlig im Bild. Er sah, wie sich die Verschlüsselung von Server zu Server fortsetzte, und er wusste genau, welche Verbindungen er hätte trennen müssen. Er tat es nicht. Nicht aus Unfähigkeit, sondern weil er nicht wusste, ob er das durfte: Die Trennung hätte auch Systeme getroffen, an denen im laufenden Betrieb gearbeitet wurde, und niemand hatte je festgelegt, wer diese Entscheidung trifft. Er versuchte, die IT-Leitung zu erreichen, dann die Geschäftsführung, dann die Vertretung. Bis eine Freigabe kam, war ein erheblicher Teil der Umgebung zusätzlich verschlüsselt.

Die Lehre daraus war nicht technischer Natur. Es fehlte ein einziges Blatt Papier: die Vorabermächtigung, die der Rufbereitschaft erlaubt, bei sichtbarer Ausbreitung sofort zu trennen, und die festhält, dass dafür niemand nachträglich zur Rechenschaft gezogen wird.

Übertragen auf die Hochschule: Wer darf um drei Uhr nachts das Rechenzentrum vom DFN trennen, mit allen Folgen für Wohnheime, Forschungsrechner und Gastwissenschaftler in anderen Zeitzonen? Wenn die Antwort lautet, das müsste man den Kanzler fragen, dann haben Sie das Problem aus diesem Praxisfall.



Skizze 3: Trennen darf schnell gehen. Alles, was sich nicht zurückdrehen lässt, braucht einen Beschluss.

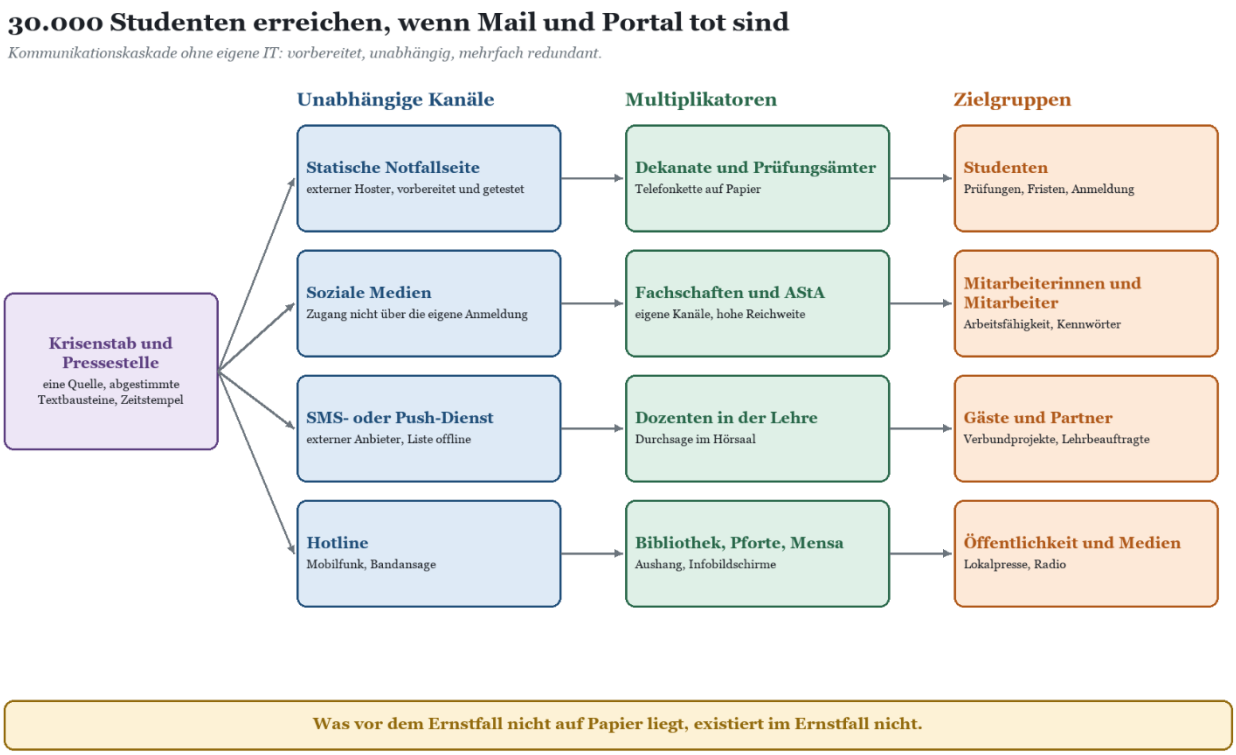
TIPP · Die Vorabermächtigung als wichtigstes Übungsergebnis

Formulieren Sie die Vorabermächtigung als kurzen Präsidiumsbeschluss: welche Maßnahmen die Rufbereitschaft ohne Rückfrage ergreifen darf, unter welchen Bedingungen, bis wann die Leitung zu informieren ist, und welche Maßnahmen ausdrücklich dem Krisenstab vorbehalten sind. Dazu ein Satz, dass gutgläubiges Handeln im Rahmen dieser Ermächtigung nicht nachträglich sanktioniert wird. Ein Blatt, das wochenlange Diskussionen erspart und in der Krise Stunden bringt.

Kommunikation und Meldepflichten, wenn nichts mehr geht

30.000 Studenten erreichen ohne Mail und Portal

Der Reflex in der Krise ist die Rundmail. Sie ist leider genau der Kanal, der bei einem schweren Vorfall als Erstes ausfällt oder abgeschaltet werden muss. Dasselbe gilt für das Hochschulportal, die Lernplattform und die Teams-Kanäle. Wer 30.000 Studenten, 5.000 Mitarbeiterinnen und Mitarbeiter, Lehrbeauftragte und Gäste erreichen will, braucht Kanäle, die unabhängig von der eigenen IT funktionieren, und die müssen vorher eingerichtet und getestet sein.



Skizze 4: Die Mail an alle ist genau der Kanal, der ausfällt. Planen Sie die anderen.

Kanal	Reichweite	Vorbereitung	Stolperstein
Statische Notfallseite bei externem Hoster	hoch, wenn bekannt	Seite und Zugang vorab einrichten, Verweis von der Hauptseite umschaltbar	Liegt der DNS-Dienst der Hochschule selbst im Rechenzentrum, hilft das nur mit vorbereiteter Ausweichlösung
Soziale Medien der Hochschule	hoch bei Studenten	Zugänge unabhängig von der zentralen Anmeldung sichern, Zweitgerät	Konten hängen oft an dienstlichen Mailadressen
SMS- oder Push-Dienst eines externen Anbieters	sehr hoch, wenn Nummern vorliegen	Rechtsgrundlage und Einwilligung klären, Nummernliste offline	Datenschutz und Aktualität der Nummern
Fachschaften und AStA	hoch, schnell	Ansprechpartner vorab benennen, Textbausteine liefern	Gerüchte verbreiten sich über dieselben Kanäle
Dozenten und Aushänge	mittel, aber sicher	Telefonkette der Dekanate auf Papier	Erreicht nur, wer auf dem Campus ist
Lokale Medien	Öffentlichkeit, Eltern, Erstsemester	Presseverteiler offline	Die Medien fragen ohnehin, besser selbst informieren

Ein unterschätzter Teil der Kommunikation sind die Textbausteine. In der Krise formuliert niemand gern unter Zeitdruck einen Satz, der juristisch, technisch und kommunikativ zugleich trägt. Bereiten Sie vor: die erste Nachricht ohne Angaben zur Ursache, die Aufforderung, keine Kennwörter auf Anfrage herauszugeben (die ersten Phishing-Mails im Namen des Rechenzentrums kommen zuverlässig), Hinweise zu Prüfungen und Fristen sowie eine Nachricht für Verbundpartner und Drittmittelgeber. Und legen Sie fest, wer freigibt. Zwei Personen, nicht ein Gremium.

WARNUNG · Gefährliche Hilfsbereitschaft

Sobald ein Ausfall bekannt wird, richten engagierte Fachschaften, Lehrstühle oder einzelne Dozenten eigene Ersatzkanäle ein: eine Messenger-Gruppe hier, ein privates Cloud-Postfach für Abgaben dort. Das ist gut gemeint und erzeugt neue Datenflüsse, die niemand kontrolliert. Nennen Sie in der ersten Nachricht die offiziellen Ausweichwege, bevor sich inoffizielle etablieren.

Meldepflichten: Was parallel läuft

Während das Rechenzentrum mit der Eindämmung beschäftigt ist, laufen Fristen. Die folgende Übersicht nennt die typischen Meldewege. Welche davon für Ihre Einrichtung tatsächlich gelten, hängt von Bundesland, Rechtsform und Trägerschaft ab. Genau das sollte vor der Übung geklärt und in der Übung durchgespielt werden.

Stelle	Anlass	Frist	Hinweis
Datenschutzaufsicht des Landes	Verletzung des Schutzes personenbezogener Daten, außer wenn voraussichtlich kein Risiko besteht	unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden (Art. 33 DSGVO)	Meldung kann schrittweise ergänzt werden. Zuständigkeit je nach Träger und Land, bei kirchlichen Hochschulen die kirchliche Aufsicht
Betroffene Personen	voraussichtlich hohes Risiko für deren Rechte und Freiheiten	unverzüglich (Art. 34 DSGVO)	Bei Leak von Prüfungs- oder Personaldaten naheliegend
BSI	erheblicher Sicherheitsvorfall bei Einrichtungen, die unter das BSI-Gesetz fallen	frühe Erstmeldung binnen 24 Stunden, Meldung binnen 72 Stunden, Abschlussmeldung nach 30 Tagen	Für die meisten staatlichen Hochschulen nicht einschlägig, für manche Forschungseinrichtung in privater Rechtsform zu prüfen
Land (Ministerium, CERT der Landesverwaltung)	nach Landesregelung oder Erlass	je nach Land	Ob Hochschulen einbezogen sind, regelt jedes Land selbst
Polizei, Zentrale Ansprechstelle Cybercrime	Straftat, Erpressung	keine gesetzliche Frist	Anzeige empfehlenswert, auch für Versicherung und Beweissicherung
Cyberversicherung	Versicherungsfall	laut Vertrag, oft sehr kurz	Obliegenheiten vorher kennen, Dienstleisterwahl kann vorgegeben sein
Drittmittelgeber und Verbundpartner	vertragliche Melde- und Geheimhaltungspflichten	laut Vertrag	Bei exportkontrollierten Projekten zusätzlich interne Exportkontrolle einbeziehen

Zur Einordnung des BSI-Gesetzes: Das NIS-2-Umsetzungsgesetz ist am 6. Dezember 2025 in Kraft getreten. Der IT-Planungsrat hat entschieden, die Option der NIS-2-Richtlinie, Bildungseinrichtungen einzubeziehen, nicht zu nutzen; für die kritischen Teile ihrer Landesverwaltungen setzen die Länder die Richtlinie in eigener Verantwortung um. Für eine staatliche Hochschule ergeben sich Pflichten daher eher aus Landesrecht als aus dem BSI-Gesetz. Außeruniversitäre Einrichtungen in privater Rechtsform sollten ihre Betroffenheit dagegen anhand von Sektor und Schwellenwerten prüfen; das BSI stellt dafür eine Betroffenheitsprüfung bereit. Wie die Datenschutzaufsichten der Länder Microsoft 365 an Hochschulen bewerten, beschreibt der

Beitrag Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität.

HINWEIS · Hinweis zu Meldepflichten

Ob eine Meldung erforderlich ist, wer sie abgibt und mit welchem Inhalt, ist im Einzelfall rechtlich zu bewerten. Landesdatenschutzgesetze, Hochschulgesetze und Erlasse der Wissenschaftsministerien unterscheiden sich von Land zu Land, ebenso die Frage, ob und wie die Hochschule ein CERT des Landes einbinden muss oder kann. Dieser Beitrag ersetzt keine Rechtsberatung. Legen Sie die Meldewege mit Justiziariat und Datenschutzbeauftragtem vorab fest.

Wer hilft: DFN-CERT, Landesstellen, Dienstleister

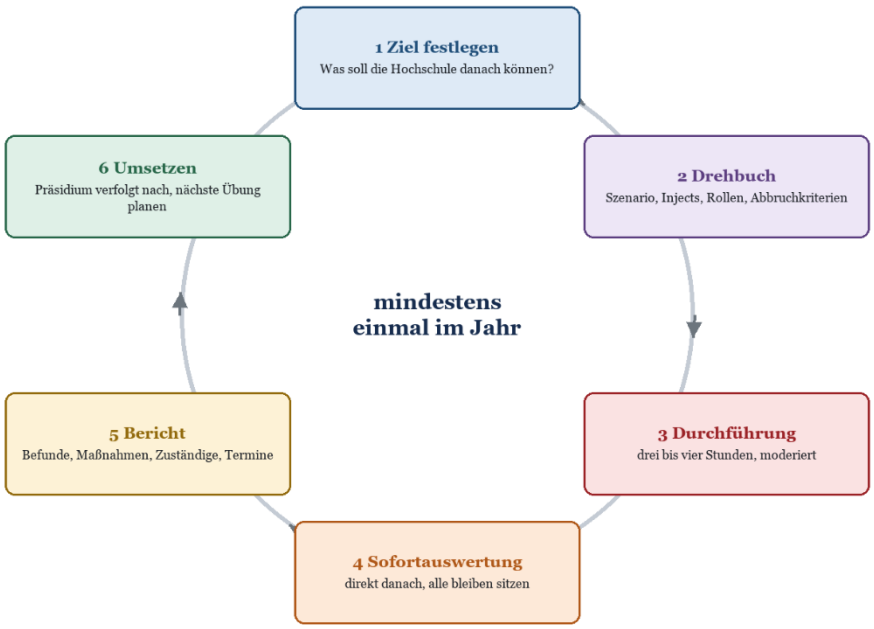
Hochschulen und Forschungseinrichtungen haben einen Vorteil, den viele Unternehmen nicht haben: das DFN-CERT, das Sicherheitsteam im Deutschen Forschungsnetz. Es unterstützt Teilnehmer beim Umgang mit Sicherheitsvorfällen, von kurzfristigen Maßnahmen über die Analyse und die Vermittlung von Kontakten bis zu Hinweisen für den sicheren Wiederanlauf. Prüfen Sie vorab, welche Leistungen Ihre Einrichtung im Rahmen ihrer DFN-Teilnahme nutzen kann, und legen Sie die Notfallnummer dort ab, wo sie im Ernstfall auffindbar ist, also nicht nur im Mailprogramm.

Daneben betreiben die Länder eigene Strukturen, etwa CERTs für die Landesverwaltung und bei den Landeskriminalämtern Zentrale Ansprechstellen Cybercrime. Welche davon für Ihre Hochschule zuständig sind und welche Leistungen sie anbieten, unterscheidet sich erheblich. Für die forensische Analyse und den Wiederaufbau großer Umgebungen braucht es in aller Regel zusätzlich einen spezialisierten Incident-Response-Dienstleister. Den sucht man nicht am Montag um acht. Ein Rahmenvertrag oder zumindest ein vorab geklärter Abruf, gegebenenfalls abgestimmt mit der Versicherung, gehört zu den häufigsten Maßnahmen nach der ersten Übung.

Übung vorbereiten, durchführen, auswerten

Der Übungszyklus: von der Idee bis zur erledigten Maßnahme

Eine Übung ohne Maßnahmenliste ist Theater. Eine Maßnahmenliste ohne Nachverfolgung auch.



Skizze 5: Der Kreis schließt sich erst, wenn die Maßnahmen aus der letzten Übung erledigt sind.

Vorbereitung: Ziel vor Drehbuch

Am Anfang steht nicht das Szenario, sondern das Ziel. Was soll die Hochschule nach der Übung können oder wissen? Etwa: Wir wissen, wer das Netz trennen darf. Wir haben einen getesteten Kanal zu den Studenten. Wir kennen unsere Meldewege. Aus dem Ziel ergibt sich das Szenario, aus dem Szenario die Injects und die Besetzung. Legen Sie außerdem Abbruchkriterien fest: Eine Übung ist kein Prüfungsgespräch, und wenn einzelne Personen bloßgestellt werden, ist das Ziel verfehlt.

- **Auftrag:** schriftlich durch das Präsidium, mit Termin und Teilnehmerkreis.
- **Vertraulichkeit:** Szenario vorab nur Moderation und einer Ansprechperson im Rechenzentrum bekannt, damit niemand die Antworten vorbereitet.
- **Unterlagen:** Notfallhandbuch, Kontaktlisten, Backup-Konzept, Versicherungsbedingungen, Prüfungsordnungen liegen auf dem Tisch, und zwar ausgedruckt. Der Dateiserver ist schließlich verschlüsselt.
- **Personalrat:** über Ziel und Format informieren, klarstellen, dass keine Leistungsbewertung einzelner Personen stattfindet.
- **Termin:** nicht in der Prüfungsphase. Das wäre zwar realistisch, aber es kommt niemand.

Durchführung: Druck dosieren

Ein Planspiel von drei bis vier Stunden folgt meist einem Muster: kurze Einführung in Regeln und Ausgangslage, dann zwei bis drei Phasen mit jeweils mehreren Injects, zwischendurch Zeitsprünge (Es ist jetzt Dienstagmorgen. Die Lage ist folgende.). Die Moderation beobachtet, ob Entscheidungen fallen, wer sie trifft und ob sie protokolliert werden. Hilfreich ist ein sichtbares Lagebild an der Wand, ganz analog auf Flipchart. Spätestens hier merkt jede Runde, dass ein Krisenstab ohne Protokollführer nach zwei Stunden nicht mehr weiß, was er um neun Uhr beschlossen hat.

Auswertung: Die Maßnahmenliste ist das Produkt

Direkt nach der Übung bleiben alle sitzen: Was lief gut, was hat gefehlt, was überraschte? Diese Sofortauswertung liefert die ehrlichsten Antworten, weil der Adrenalinspiegel noch hoch ist. Innerhalb von zwei Wochen folgt ein schriftlicher Bericht mit konkreten Maßnahmen, Verantwortlichen und Terminen. Das Präsidium verfolgt die Umsetzung nach, und die nächste Übung beginnt mit der Frage, was aus der letzten Liste geworden ist.

Häufiger Befund	Typische Maßnahme
Niemand weiß, wer trennen darf	Vorabermächtigung als Präsidiumsbeschluss
Kontaktlisten nur digital	Notfallmappe auf Papier, halbjährlich aktualisiert, an mehreren Orten
Notfallkonten ungetestet oder föderiert	Notfallkonten nach Microsoft-Empfehlung neu aufsetzen, Anmeldung regelmäßig testen
Backups erreichbar für Domänenadministratoren	Unveränderliche oder getrennte Sicherungen, Wiederherstellung üben
Kein Kanal zu Studenten ohne eigene IT	Notfallseite extern, Social-Media-Zugänge unabhängig sichern, Textbausteine
Meldewege unklar	Meldematrix mit Datenschutz und Justiziariat, Vorlagen für Erstmeldung
Kein Dienstleister für Forensik	Rahmenvertrag oder vorab geklärter Abruf
Personalrat erst spät beteiligt	Notfallregelung in der Dienstvereinbarung

FAKTEN · Notfall- und Red-Team-Übung mit externer Moderation

Wir konzipieren und moderieren Planspiele für Hochschulen und Forschungseinrichtungen: Zieldefinition mit dem Präsidium, Drehbuch mit hochschultypischen Injects, Durchführung vor Ort, Sofortauswertung und Bericht mit Maßnahmenliste. Auf Wunsch ergänzt um eine Red-Team-Übung gegen Ihren Microsoft-365-Tenant, deren Ergebnisse als realistische Injects in das nächste Planspiel einfließen. Die Erfahrung dafür stammt aus forensischer Arbeit und Notfallübungen bei öffentlichen Auftraggebern und kirchlichen Trägern.

Mehr dazu auf der Seite Microsoft-365-Beratung für Hochschulen und Forschung. Für Rechenzentrum, Helpdesk und Krisenstab bieten wir passende Trainings an: Microsoft-365-Schulung für Hochschulen und Forschung.

Häufige Fragen zur Notfallübung an der Hochschule

Wie oft sollte eine Hochschule eine Notfallübung durchführen?

Ein moderiertes Planspiel einmal im Jahr ist ein guter Rhythmus, ergänzt um eine kurze Alarmierungsübung vor jedem Semesterbeginn. Wichtiger als die Frequenz ist, dass die Maßnahmen aus der letzten Übung umgesetzt wurden, bevor die nächste beginnt.

Muss das Präsidium wirklich selbst teilnehmen?

Ja. Die Übung trainiert vor allem Entscheidungen, und die trifft im Ernstfall die Hochschulleitung. Eine Übung ohne Präsidium übt, wie man auf eine Entscheidung wartet. Das kann man auch ohne Moderation.

Ist eine Notfallübung mitbestimmungspflichtig?

Das hängt vom Landespersonalvertretungsgesetz und von der Ausgestaltung ab. Ein Planspiel, das Abläufe und keine Personen bewertet, ist in der Regel unkritisch. Informieren Sie den Personalrat trotzdem frühzeitig und laden Sie ihn an den Tisch. Die Frage, ob eine Beteiligung erforderlich ist, klären Sie mit dem Justiziariat.

Sollten wir im Ernstfall Lösegeld zahlen?

Das ist eine Entscheidung der Hochschulleitung unter Beteiligung von Justiziariat, Ministerium und gegebenenfalls Versicherung, und sie sollte in der Übung ausdrücklich durchgespielt werden. Staatliche Stellen raten regelmäßig davon ab. Eine Zahlung garantiert weder die Entschlüsselung noch, dass abgezogene Daten nicht veröffentlicht werden.

Was ist der Unterschied zwischen Planspiel und Red-Team-Übung?

Das Planspiel übt Entscheidungen am Tisch anhand eines fiktiven Szenarios. Die Red-Team-Übung prüft mit realen, abgestimmten Angriffstechniken, ob ein Angriff erkannt und gestoppt wird. Beide ergänzen sich. Für den Einstieg ist das Planspiel fast immer die bessere Wahl.

Brauchen wir ein eigenes Szenario für Microsoft 365?

Szenario 3 mit dem kompromittierten Administratorkonto ist im Kern ein Tenant-Szenario. Daneben lohnt es, im Ransomware-Szenario mitzudenken, welche Dienste in der Cloud weiterlaufen und welche Abhängigkeiten über den lokalen Verzeichnisdienst und die Föderation bestehen. Gerade an Hochschulen mit Shibboleth-Anbindung ist das oft die Überraschung des Tages.

Gilt das auch für außeruniversitäre Forschungseinrichtungen?

Ja, mit zwei Unterschieden: Statt eines Personalrats ist je nach Rechtsform ein Betriebsrat zu beteiligen, und Einrichtungen in privater Rechtsform sollten prüfen, ob sie unter das BSI-Gesetz

fallen. Institute großer Forschungsgesellschaften sollten zudem klären, wie die Zentrale im Ernstfall eingebunden wird.

Fazit: Üben, solange es noch lustig ist

Der schlimmste Montag des Semesters kommt nicht mit Vorankündigung. Wenn er kommt, entscheidet nicht die Qualität der Firewall-Regeln über das Ausmaß des Schadens, sondern die Frage, ob die richtigen Menschen in den ersten Stunden die richtigen Entscheidungen treffen, in der richtigen Reihenfolge und ohne auf jemanden zu warten, der gerade auf einer Tagung in Lissabon sitzt. Große Schäden entstehen, weil jemand, der es kann, unter Druck den falschen Knopf drückt. Eine Übung sorgt dafür, dass die Knöpfe beschriftet sind.

Drei Szenarien, ein Tisch mit acht Stühlen, eine externe Moderation und ein halber Tag Zeit des Präsidiums: Mehr braucht es für den Anfang nicht. Was dabei herauskommt, ist meist unspektakulär und unbezahlbar: eine Vorabermächtigung, eine Notfallmappe auf Papier, ein getesteter Kanal zu den Studenten und das gute Gefühl, dass der Kanzler weiß, was er im Ernstfall gefragt wird. Wenn Sie Ihre erste oder nächste Übung extern moderieren lassen wollen, sprechen Sie uns über die Microsoft-365-Beratung für Hochschulen und Forschung an.

WEITERLESEN · Weiterlesen

Für diesen Beitrag besonders passend aus der Serie:

› Microsoft-365-Security an Hochschulen: Offene Netze, private Geräte und Konten als Beute

› MFA für 30.000 Studenten: Conditional Access an der Hochschule ohne Helpdesk-Kollaps

› Entra-ID-Überprüfung für Hochschul-Tenants: Was sich nach zehn Jahren Wildwuchs findet

› Entra ID und Shibboleth: Microsoft 365 an die DFN-AAI-Welt anbinden

› Dezentrale IT an der Hochschule: Lehrstuhl-Admins, Fakultäts-IT und ein Tenant für alle

› Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle

› Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität

› Prüfungsdaten, Berufungsakten, Personalvorgänge: Besonders schützenswerte Daten im Hochschul-Tenant