

Notfall- und Red-Team-Übung für kirchliche Träger: Wenn die Diakonie-Verwaltung verschlüsselt ist und das Pflegeheim weitermachen muss

Es gibt einen Satz, den du in der Nacht eines Ransomware-Vorfalls nicht hören willst. Er lautet: „Wer darf denn jetzt eigentlich entscheiden, dass wir alles ausmachen?“ Der Satz fällt selten in der IT. Er fällt in einer Telefonkonferenz um kurz nach vier, in der sieben Personen sitzen, von denen drei nicht wissen, warum sie dabei sind, und zwei gerade begreifen, dass sie die Einzigen sind, die es entscheiden dürften.

Kirchliche Träger sind für Erpressergruppen attraktiv, und das hat wenig mit Frömmigkeit zu tun. Sie haben viele Standorte, dünne IT-Mannschaften, gewachsene Verzeichnisdienste, Spendengelder auf Konten und — das ist der eigentliche Hebel — Daten, deren Veröffentlichung Menschen beschädigt: Beratungsakten, Pflegedokumentation, Jugendhilfeberichte, Personalakten nach kirchlichem Arbeitsrecht. Ein Angreifer, der eine Kommune verschlüsselt, erpresst eine Verwaltung. Ein Angreifer, der ein diakonisches Werk verschlüsselt, erpresst eine Verwaltung und hält gleichzeitig die Akten von Menschen in der Hand, die sich in der schlechtesten Phase ihres Lebens an dich gewandt haben.

Dieser Beitrag beschreibt, wie ein Angriff auf einen kirchlichen Träger typischerweise verläuft, was Microsoft 365 davon wirklich abfängt und was nicht, warum Pflege, Kita und Krankenhaus ohne IT weiterlaufen müssen — und wie du das Ganze übst, bevor es passiert. Die Einordnung, was in Kirche, Diakonie und Caritas überhaupt anders ist als in Kommune und Mittelstand, findest du im Überblicksbeitrag [Microsoft 365 in Kirche, Diakonie und Caritas](#). Hier geht es um den Tag, an dem die Theorie aufhört.

FAKTEN · Worum es geht — in vier Sätzen

Ransomware ist bei kirchlichen Trägern kein IT-Problem, sondern ein Betriebsführungsproblem mit IT-Ursache.

Microsoft 365 fängt einen erheblichen Teil des Angriffswegs ab, aber genau den Teil nicht, der bei den meisten Trägern wehtut: den lokalen Dateiserver, die Fachverfahren und den Verzeichnisdienst im eigenen Haus.

Pflege, Kita und Krankenhaus dürfen nicht warten, bis die IT wieder da ist. Der Notfallplan muss auf Papier funktionieren.

Die einzige Vorbereitung, die im Ernstfall nachweislich Zeit spart, ist eine Übung, in der Leitung, IT, Datenschutz, Mitarbeitervertretung und Kommunikation gemeinsam am Tisch sitzen.

Warum kirchliche Träger auf der Zielliste stehen

Erpressergruppen suchen nicht nach Gesinnung, sondern nach Zahlungsbereitschaft und Angriffsfläche. Kirchliche Träger liefern beides in einer Kombination, die selten geworden ist: Sie sind groß genug, um relevant zu sein, und dezentral genug, um an vielen Stellen verwundbar zu sein.

Viele Standorte, ein gemeinsames Verzeichnis

Ein Kirchenkreis mit dreißig Gemeinden, vier Kitas, einer Beratungsstelle und einem angeschlossenen diakonischen Werk hat typischerweise: dreißig Pfarrbüros mit teils privaten Endgeräten, ein historisch gewachsenes Active Directory, zwei bis drei Systemhäuser mit Fernwartungszugängen, einen Dateiserver, auf dem seit 2009 nichts gelöscht wurde, und eine halbe Stelle IT. Für einen Angreifer ist das keine Burg, das ist ein Dorf ohne Mauer.

Die Besonderheit gegenüber der Kommune liegt weniger in der Technik als in der Verfassung: Kirchengemeinden sind rechtlich eigenständig, der Kirchenkreis oder das Dekanat betreibt die Technik oft nur im Auftrag, und die Entscheidung über einen Betriebsstopp liegt im Zweifel bei einem Gremium, das monatlich tagt. Presbyterium, Kirchenvorstand, Pfarrgemeinderat, Kirchenverwaltung, Verbandsversammlung, Aufsichtsrat des Trägers: Das sind fünf unterschiedliche Wege zu einer Entscheidung, und keiner davon ist auf drei Uhr nachts ausgelegt.

Was die Daten für einen Erpresser wert sind

Bei Erpressungsangriffen ist die Verschlüsselung inzwischen der zweite Schritt. Der erste ist der Datenabfluss. Das BSI hat im Jahresbericht 2025 für den Zeitraum Juli 2024 bis Juni 2025 festgestellt, dass professionell organisierte Erpressergruppen trotz eines leichten Rückgangs finanziell motivierter Angriffe die größte Bedrohung bleiben und dass die Zahl neu bekannt gewordener Schwachstellen um rund ein Viertel gestiegen ist. Kleine und mittlere Organisationen sowie Kommunen nennt das BSI ausdrücklich als Gruppen, denen Ressourcen und Bewusstsein fehlen. Kirchliche Träger fallen strukturell in genau diese Kategorie — nur mit sensibleren Daten.

Denn was in einem diakonischen Werk liegt, ist nicht „Verwaltungsdaten“. Es sind Sozialdaten, Gesundheitsdaten, Angaben zu Schwangerschaftskonflikten, Schuldnerberatung, Suchthilfe, Jugendhilfe. Dazu kommen Personalakten nach dem Dritten Weg, AVR-Eingruppierungen, Daten aus dem Meldewesen und, im schlimmsten Fall, Aufzeichnungen aus Kontexten, die überhaupt nicht im Dateisystem hätten liegen dürfen. Wie du diese Kategorien auseinanderhältst, steht in den Beiträgen zu [Klientendaten in Diakonie und Caritas](#) und zum [Seelsorgegeheimnis und Beichtgeheimnis in Microsoft 365](#). Für die Notfallübung genügt eine Erkenntnis: Die Veröffentlichungsdrohung wiegt bei einem kirchlichen Träger schwerer als der Betriebsausfall — und sie lässt sich durch kein Backup der Welt entschärfen.

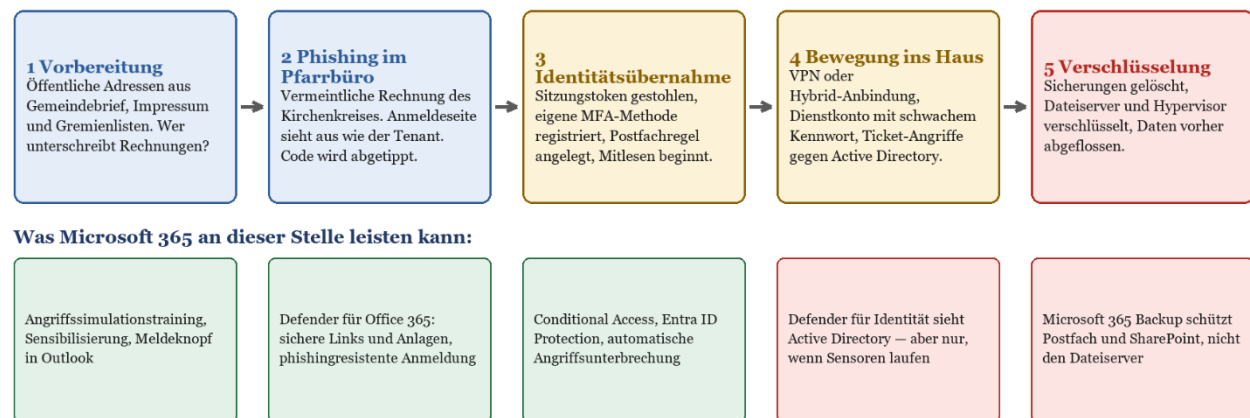
WARNUNG · Der Denkfehler, der am meisten kostet

„Wir haben doch ein Backup“ ist eine Antwort auf die Frage nach Verfügbarkeit. Sie ist keine Antwort auf die Frage nach Vertraulichkeit. Wenn 400 Beratungsakten abgeflossen sind, hilft dir die schnellste Wiederherstellung nichts: Du hast trotzdem eine meldepflichtige Verletzung des Schutzes personenbezogener Daten, eine Benachrichtigungspflicht gegenüber den Betroffenen und ein Gespräch mit Menschen, denen du Vertraulichkeit zugesagt hattest.

Merkmal	Kommune / Mittelstand	Kirchlicher Träger	Folge für die Übung
Rechtsrahmen	DSGVO und BDSG, staatliche Aufsicht	DSG-EKD oder KDG, eigene kirchliche Aufsicht	Meldeweg und Fristen gesondert üben
Aufsicht	Landesbeauftragte für Datenschutz	BfD EKD bzw. Diözesandatenschutzbeauftragte, Katholisches Datenschutzzentrum	Kontaktdaten und Meldeformular vorab im Notfallordner
Beschäftigtenvertretung	Personalrat oder Betriebsrat	Mitarbeitervertretung nach MVG-EKD oder MAVO	MAV gehört von Anfang an in den Krisenstab

Entscheidungsweg	Verwaltungsspitze, klare Hierarchie	Geschäftsführung, Vorstand, Gremium — je nach Satzung	Vollmacht für den Betriebsstopp schriftlich klären
Datenarten	Melde-, Steuer-, Sozialdaten	zusätzlich Beratungs-, Pflege- und Seelsorgekontexte	Abflussszenario getrennt vom Ausfallszenario üben
Betriebszwang	Amt kann tageweise schließen	Pflegeheim und Krankenhaus können nicht schließen	Papier-Rückfallebene ist Pflicht, nicht Kür
Öffentlichkeit	Lokalpresse, Ratssitzung	Gemeindebrief, Gottesdienst, Angehörige, Ehrenamt	Kommunikation mehrkanalig und seelsorglich denken

Skizze 1: Der typische Weg vom Pfarrbüro zum Dateiserver



Die Kette reißt selten an einer Stelle. Sie reißt dort, wo Identität, Endgerät und Rechenzentrum niemandem gemeinsam gehören.

Faustregel aus der Praxis: Zwischen Schritt 2 und Schritt 5 liegen Tage bis Wochen. Genau dieses Fenster verschenken die meisten Träger.

Skizze 1: Der typische Angriffsweg — und an welcher Stelle Microsoft 365 tatsächlich eingreifen kann.

Wie der Angriff läuft — und was Microsoft 365 abfängt

Die gute Nachricht zuerst: Der Weg ist langweilig. Er ist seit Jahren derselbe, und er ist an mehreren Stellen unterbrechbar. Die schlechte: Er funktioniert trotzdem, weil die Unterbrechungen Geld, Lizenzen und Entscheidungen kosten, die niemand treffen will, solange nichts passiert ist.

Schritt eins: Phishing im Pfarrbüro

Das Pfarrbüro ist der ideale Einstieg. Die Adresse steht im Gemeindebrief, im Impressum und auf dem Schaukasten. Die Zuständigkeit ist breit: Rechnungen, Anmeldungen, Belegungen, Kollektenabrechnung, Friedhofsverwaltung. Und die Bereitschaft, eine E-Mail zu öffnen, ist beruflich vorgeschrieben. Eine angebliche Rechnung „aus dem Kirchenkreis“ oder eine Nachricht „zur Freigabe der Sammlung“ hat eine Klickrate, von der Marketingabteilungen träumen.

Microsoft 365 kann hier viel: Defender für Office 365 prüft Links beim Klick und Anlagen in einer isolierten Umgebung, der Meldeknopf in Outlook bringt verdächtige Nachrichten in die Auswertung, und das Angriffssimulationstraining im Defender-Portal lässt dich genau solche Nachrichten gefahrlos an die eigene Belegschaft schicken. Die verfügbaren Social-Engineering-Techniken sind bis auf die reinen Lehrmodule aus dem MITRE-ATT&CK-Katalog abgeleitet: Abgreifen von Anmeldedaten, Schadsoftware im Anhang, Link im Anhang, Link auf Schadsoftware, Drive-by-URL und missbräuchliche OAuth-Zustimmung — inzwischen auch als QR-Code, weil

genau das gerade in den Briefkästen landet. Das Ganze braucht Defender für Office 365 Plan 2 oder Microsoft 365 E5; für E3 gibt es nur einen kleinen Ausschnitt.

Schritt zwei: Identitätsübernahme

Der Angreifer will kein Kennwort, er will eine Sitzung. Moderne Phishing-Seiten schalten sich zwischen Nutzer und Anmeldedienst, leiten den zweiten Faktor durch und stehlen das ausgestellte Token. Der zweite Faktor per Code oder Push ist damit wertlos. Was hilft, sind phishingresistente Verfahren: Passkeys nach FIDO2, zertifikatbasierte Anmeldung, Gerätebindung über Conditional Access. Wie ein Regelwerk aussieht, das Pfarrbüro, Pflegedienst, Verwaltung und Ehrenamt gleichzeitig erträgt, steht im Beitrag [Conditional Access und MFA in Kirche und Diakonie](#).

Direkt nach der Übernahme passieren drei Dinge, die man in den Protokollen sehen kann, wenn man hinsieht: Der Angreifer registriert eine eigene MFA-Methode, legt eine Postfachregel an, die Antworten in einen unauffälligen Ordner verschiebt, und durchsucht das Postfach nach den Stichworten, die überall funktionieren — Rechnung, Zugang, VPN, Kennwort, Bank. In kirchlichen Tenants kommen leider noch Kollekte, Spende und Nachlass dazu.

Schritt drei: der Weg ins eigene Haus

Jetzt wird es unangenehm, denn hier endet für viele Träger die Sichtbarkeit. Der Angreifer nutzt die Verbindung, die zwischen Cloud und Haus ohnehin besteht: Verzeichnissynchronisierung, VPN-Zugang, ein Dienstkonto mit uraltem Kennwort und einem Dienstprinzipalnamen, das sich über klassische Ticket-Angriffe gegen Active Directory offline knacken lässt. Wenn du wissen willst, warum ein einziges schwaches Dienstkonto reicht, um ein ganzes Verzeichnis zu verlieren, ist der Kompetenzbereich [Microsoft Kerberos](#) der richtige Einstieg — und gleichzeitig die Erklärung, warum der Wiederaufbau nach einem Vorfall fast immer den Neuaufbau des Verzeichnisdienstes bedeutet und nicht seine Wiederherstellung.

Schritt vier: Verschlüsselung — und was der Tenant davon merkt

Microsoft Defender XDR korreliert Signale aus Endgeräten, Identitäten, E-Mail und SaaS-Anwendungen und kann einen laufenden Angriff automatisch unterbrechen: Gerät isolieren, IP-Adresse sperren, Benutzerkonto deaktivieren, aktive Sitzungen widerrufen, einen Benutzer netzweit eindämmen. Microsoft gibt für diese Eindämmungsaktionen ein Konfidenzniveau von 99 Prozent oder höher an, alle Aktionen sind durch das eigene Team rücknehmbar, und für besonders kritische Konten oder Geräte lassen sich Ausnahmen definieren. Das ist die Funktion, die in den beschriebenen Nachtstunden tatsächlich Schaden verhindert — vorausgesetzt, die Sensoren laufen auf den Domänencontrollern und auf den Servern, nicht nur auf den Notebooks der Verwaltung.

WICHTIG · Die Lücke, die fast jeder Träger hat

Microsoft 365 Backup sichert SharePoint, OneDrive und Exchange innerhalb der Datengrenze des Dienstes, mit Wiederherstellungspunkten alle zehn Minuten für die zurückliegenden zwei Wochen, Wochenständen darüber hinaus und einem konfigurierbaren Wiederherstellungsfenster von drei Monaten bis zwei Jahren. Der Speicher arbeitet nach dem Anfüge-Prinzip, ist also gegen Überschreiben durch Schadsoftware geschützt. Abgerechnet wird nach Verbrauch pro Gigabyte und Monat, Wiederherstellungen sind kostenlos.

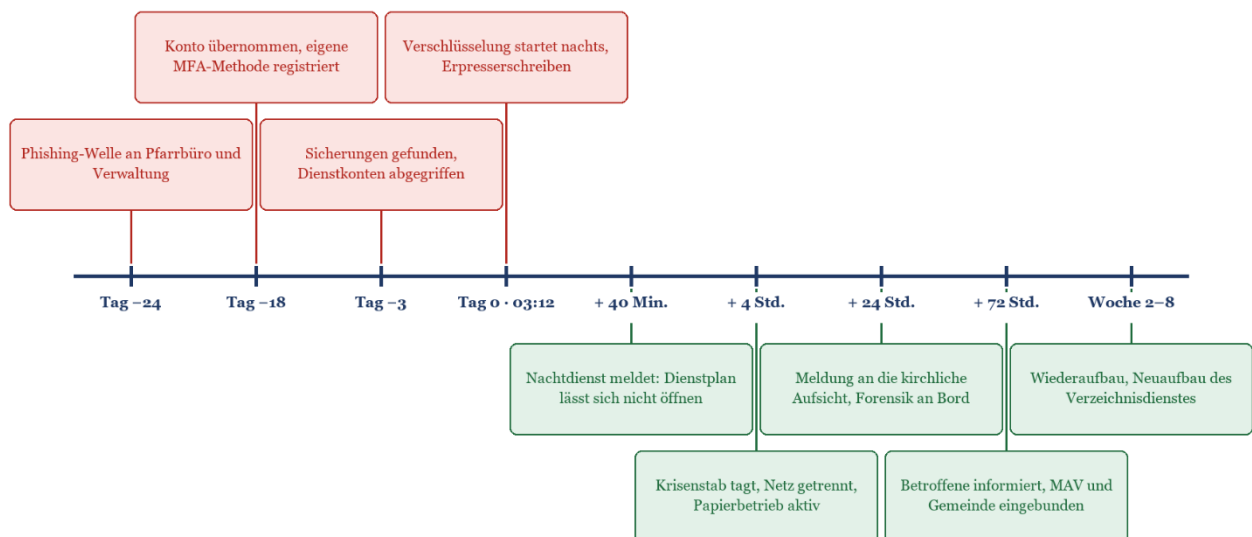
Nur: Der Dateiserver im Keller, die Pflegedokumentation, das Krankenhausinformationssystem, die Finanzbuchhaltung und der Verzeichnisdienst sind nicht dabei. Genau die werden verschlüsselt. Wer in der Übung nur die Cloud wiederherstellt, hat die falsche Übung gemacht.

Angriffsschritt	Was Microsoft 365 leisten kann	Was Microsoft 365 nicht leistet	Was du selbst regeln musst
Phishing-Mail	Sichere Links und Anlagen,	Schutz vor Nachrichten an	Regel, dass dienstliche Post

	Meldeknopf, Angriffssimulationstraining mit Kompromittierungsprognose	private Adressen und Messenger-Kanäle	dienstlich bleibt — auch im Ehrenamt
Anmeldung	Conditional Access, Gerätebindung, Passkeys, Risikobewertung durch Entra ID Protection	Schutz, wenn Ausnahmen für „schwierige Fälle“ dauerhaft bestehen bleiben	Ausnahmeliste regelmäßig prüfen und befristen
Postfachregel und MFA-Registrierung	Protokollierung im einheitlichen Überwachungsprotokoll, Warnungen im Defender-Portal	Auswertung, wenn niemand hinschaut	Verantwortliche Person oder Dienstleister mit Reaktionszeit benennen
Bewegung ins lokale Netz	Defender für Identität erkennt Angriffe gegen Active Directory	Erkennung ohne Sensoren auf den Domänencontrollern	Sensoren ausrollen, Dienstkonten härten, Altlasten abschalten
Verschlüsselung	Automatische Angriffsunterbrechung isoliert Geräte und Konten	Rettung von Systemen ohne Defender-Abdeckung	Getrennte, offline gehaltene Sicherung für alles im eigenen Haus
Datenabfluss	Purview-Klassifizierung, Bezeichnungen, Verhinderung von Datenverlust	Rückholung veröffentlichter Daten	Meldung, Benachrichtigung, Kommunikation — und weniger Daten vorhalten
Nachweis im Nachgang	Überwachungsprotokoll 180 Tage im Standard; mit Audit Premium ein Jahr für Entra, Exchange, SharePoint und OneDrive	Rekonstruktion von Ereignissen jenseits des Aufbewahrungszeitraums	Aufbewahrung passend zur eigenen Erkennungsdauer wählen

Skizze 2: Angriffs- und Reaktionszeitstrahl einer verschlüsselten Diakonie-Verwaltung

OBEN: was der Angreifer tut



UNTEN: was der Träger tut — wenn geübt wurde

Ohne Übung verschiebt sich die untere Zeile um Stunden bis Tage nach rechts. Der Unterschied heißt nicht Technik, sondern Entscheidungsfähigkeit.

Skizze 2: Oben der Angreifer, unten der Träger. Geübte Organisationen verschieben die untere Zeile nach links.

Pflege, Kita und Krankenhaus laufen weiter — notfalls auf Papier

Ein Rathaus kann für zwei Tage schließen. Ein Pflegeheim kann das nicht. Um sechs Uhr morgens braucht der Frühdienst eine Übergabe, eine Medikationsübersicht und die Information, welche Bewohnerin heute zur Dialyse muss. Ob der Dateiserver verschlüsselt ist, interessiert diesen Vorgang nicht. Genau das ist der Unterschied, der kirchliche und diakonische Träger vom normalen Mittelstand trennt — und er wird in Notfallkonzepten regelmäßig unterschätzt, weil die Konzepte von IT-Leuten geschrieben werden, die noch nie eine Dienstübergabe erlebt haben.

Der Ausfall trifft nicht die IT, sondern die Übergabe

In der Rekonstruktion nach einem Vorfall zeigt sich fast immer dasselbe Muster: Die technischen Schäden sind in Wochen behoben, die organisatorischen Schäden in Monaten. Was fehlt, sind nicht die Daten, sondern die kleinen Routinen, die auf Daten aufsetzen: Wer ruft den Bereitschaftsarzt? Wo steht die aktuelle Abholberechtigung für das Kind aus der roten Gruppe? Welche Vollmacht gilt für die Bewohnerin im Zimmer 214? Wie kommt die Zeiterfassung in den Lohnlauf, wenn das Zeitwirtschaftssystem nicht startet?

Für Menschen ohne Schreibtisch — Pflege, Kita, Hauswirtschaft, Fahrdienst — ist die Ausfallsituation ohnehin näher am Alltag als für die Verwaltung. Wie diese Arbeitsplätze im Normalbetrieb aussehen sollten, steht im Beitrag [Kita, Pflege, Jugendhilfe: Frontline-Arbeitsplätze in Microsoft 365](#). Für den Notfall gilt: Je mehr dieser Menschen ein eigenes dienstliches Konto und ein mobiles Gerät haben, desto größer ist die Chance, dass Ebene zwei aus Skizze 3 überhaupt funktioniert. Geteilte Sammelkonten fallen mit dem ersten kompromittierten Kennwort komplett aus.

Was in den Notfallordner gehört

- **Dienstplan und Rufbereitschaft:** aktueller Ausdruck je Wohnbereich, Gruppe oder Station, nicht älter als eine Woche, mit Mobilnummern und Vertretungsregelung.
- **Bewohner- und Kinderdaten im Mindestumfang:** Name, Geburtsdatum, Notfallkontakt, zentrale medizinische Hinweise, Abholberechtigung. Bewusst knapp — der Ordner ist ein Datenschutzrisiko, kein Aktenarchiv.
- **Telefonliste außerhalb des Systems:** Leitung, IT, Datenschutz, MAV, Aufsicht, Dienstleister, Versicherung, Polizei. Auf Papier und als Karte im Portemonnaie der Leitungskräfte.
- **Handlungsanweisung für die ersten dreißig Minuten:** eine Seite, zehn Punkte, keine Fachbegriffe. Wer trennt was, wer ruft wen an, was ausdrücklich nicht getan wird.
- **Vollmachten und Vertretungen:** wer den Betrieb anhalten darf, wer Zahlungen freigibt, wer nach außen spricht — mit namentlicher Vertretung.
- **Formulare für den Handbetrieb:** Übergabebogen, Medikationsnachweis, Anwesenheitsliste, Kassenbuch für Kollekte und Barkasse.

TIPP · Der Test, der zehn Minuten dauert

Geh in eine Einrichtung, such den Notfallordner und schlag ihn auf. Drei Fragen: Ist der Dienstplan aktuell? Steht auf der Telefonliste eine Nummer, die heute noch jemand abnimmt? Und weiß die Person, die gerade Dienst hat, dass es diesen Ordner gibt?

Wenn eine der drei Antworten Nein lautet, brauchst du keine Red-Team-Übung, um zu wissen, wo du anfängst. In der Praxis liegt die Trefferquote bei „mindestens ein Nein“ ungefähr bei neunzig Prozent — und der Ordner ist dabei meistens vorhanden, nur eben aus dem Jahr, in dem er einmal angelegt wurde.

Einrichtung	Was nach zwei Stunden weh tut	Was nach zwei Tagen kritisch wird	Tolerierbare Ausfallzeit (Richtwert)
Pflegeheim	Dienstübergabe, Medikation, Sturz- und Wunddokumentation	Abrechnung, Heimaufsichtsnachweise, Personaleinsatzplanung	Stunden — Dokumentation muss sofort auf Papier weitergehen
Krankenhaus	Aufnahme, Befundübermittlung, Terminplanung	OP-Planung, Abrechnung, Arztbriefe	Minuten bis Stunden; das KIS ist hier die eigentliche Frage
Kita	Anwesenheit, Abholberechtigung, Allergiehinweise	Elternkommunikation, Beitragsabrechnung, Personalplanung	Stunden — Aufsichtspflicht duldet keine Lücke
Beratungsstelle	Terminübersicht, Erreichbarkeit, Krisenkontakte	Fallverläufe, Nachweise gegenüber Kostenträgern	Ein bis zwei Tage, wenn Erreichbarkeit gesichert ist
Jugendhilfe	Erreichbarkeit der Fachkräfte, Bereitschaftsdienst	Hilfeplanung, Berichte an das Jugendamt	Ein bis drei Tage
Kirchengemeinde	Bestattungstermine, Trauungen, Gottesdienstplan	Gemeindebrief, Kollektenabrechnung, Friedhofsverwaltung	Tage — mit hoher öffentlicher Sichtbarkeit
Verwaltung des Trägers	Zahlungsverkehr, Telefonzentrale	Lohnlauf, Meldewesen, Jahresabschluss	Tage bis Wochen, aber der Lohnlauf hat ein hartes Datum

Skizze 3: Drei Rückfallebenen — was weiterläuft, wenn die Verwaltung steht

Ebene 1 · Normalbetrieb

Microsoft 365 vollständig: Teams, SharePoint, Exchange, Fachverfahren, Dienstplan, Pflegedokumentation, Telefonie.

Ebene 2 · Eingeschränkter Cloudbetrieb

Lokales Netz getrennt, Tenant weiter erreichbar: Teams-Chat und Telefonie über Mobilgeräte, Notfall-Team mit Leitungskreis, Verteiler für Angehörige, Kommunikation nach außen.

Ebene 3 · Papier und Telefon

Alles aus, auch die Identitäten: Notfallordner je Einrichtung, Dienstplan als Ausdruck, Medikationsliste, Notrufnummern, Vollmachten, Schlüsselverzeichnis, Kollektenabrechnung von Hand.

Wer prüft was — und wie oft:

Pflegeheim

Dienstplan, Medikation, Übergabe, Notruf

Notfallordner je Wohnbereich, Quartalsprüfung

Kita

Anwesenheit, Abholberechtigung, Allergien, Elternkontakte

Ausdruck je Gruppe, monatlich aktualisiert

Beratungsstelle

Termine, Erreichbarkeit, Schweigepflichtbereich

Papierkalender, keine Fallakten auf Papier

Verwaltung

Gehalt, Zahlungsverkehr, Meldewesen, Kollekte

Vier-Augen-Vollmacht, Lohnlauf-Notfallpfad

Skizze 3: Wer die zweite Ebene nicht plant, springt von Normalbetrieb direkt auf Papier — und verliert dabei die Kommunikationsfähigkeit.

Die Übung: ein Tabletop mit allen, die entscheiden müssen

Eine Notfallübung für einen kirchlichen Träger ist kein IT-Workshop. Sie ist eine Sitzung, in der ein realistisches Szenario vorgelesen wird und die Beteiligten in Echtzeit entscheiden müssen, was sie tun — mit den Befugnissen, die sie laut Satzung und Dienstanweisung tatsächlich haben. Vier Stunden reichen für den ersten Durchlauf. Was sie kosten, ist überschaubar; was sie sichtbar machen, ist es selten.

Wer am Tisch sitzt

- **Geschäftsführung oder Vorstand:** leitet, entscheidet, trägt die Verantwortung. Ohne diese Rolle ist die Übung ein Planspiel ohne Folgen.
- **IT-Leitung:** liefert die Lage und die Optionen, entscheidet aber nicht über den Betriebsstopp.
- **Örtlich Beauftragte für den Datenschutz:** bewertet, ob eine meldepflichtige Verletzung vorliegt, und formuliert die Meldung.
- **Mitarbeitervertretung:** nach MVG-EKD oder MAVO. Notdienstpläne, Mehrarbeit, Protokollierung und die Auswertung von Anmeldezeiten sind mitbestimmungsrelevant — im Notfall genauso wie sonst.
- **Kommunikation und Öffentlichkeitsarbeit:** eine Stimme nach außen. Gemeinde, Angehörige, Presse, Ehrenamt.
- **Einrichtungsleitungen:** mindestens eine aus Pflege und eine aus Kita oder Beratung. Sie bringen die Wirklichkeit mit.
- **Optional, aber wirksam:** die Aufsicht als Gast oder der externe Dienstleister, der im Ernstfall den Hörer abnehmen soll.

Der Ablauf in vier Stunden

Bewährt hat sich ein Ablauf in fünf Einspielungen. Jede Einspielung ist eine halbe Seite Text, die vorgelesen wird; danach hat die Runde zwanzig Minuten, um Entscheidungen zu treffen und Aufträge zu verteilen. Eine Person protokolliert ausschließlich Entscheidungen, offene Fragen und Zeitstempel — dieses Protokoll ist das eigentliche Ergebnis der Übung.

- **Einspielung 1 — 03:12 Uhr:** Der Nachtdienst im Pflegeheim erreicht die Rufbereitschaft: Der Dienstplan lässt sich nicht öffnen, auf dem Bildschirm steht ein englischer Text.
- **Einspielung 2 — 03:50 Uhr:** Die IT bestätigt: Dateiserver und zwei Hypervisoren sind verschlüsselt, die Sicherung ist mitverschlüsselt. Der Tenant ist erreichbar. Frage an die Runde: Netz trennen, ja oder nein — und wer entscheidet das?
- **Einspielung 3 — 07:30 Uhr:** Die Erpresser melden sich mit einer Liste von Dateinamen aus der Schuldnerberatung. Frist: 72 Stunden. Gleichzeitig ruft die erste Angehörige an, weil sie ihre Mutter nicht erreicht.
- **Einspielung 4 — 11:00 Uhr:** Eine Lokalzeitung fragt an. Zwei Mitarbeiterinnen haben bereits privat in sozialen Netzwerken geschrieben. Die MAV fragt, ob Beschäftigten Daten betroffen sind.
- **Einspielung 5 — Tag 4:** Der Wiederanlauf beginnt. Frage: Welche Systeme kommen in welcher Reihenfolge zurück, wer gibt frei, und woher weißt du, dass das Netz sauber ist?

Meldung an die kirchliche Aufsicht

Hier liegt der handfesteste Unterschied zur Kommune, und hier wird in Übungen am meisten gelernt. Kirchliche Träger melden nicht an die Landesdatenschutzaufsicht, sondern an ihre eigene Aufsicht — auf evangelischer Seite an den oder die Beauftragte für den Datenschutz der EKD beziehungsweise die nach der jeweiligen gliedkirchlichen Regelung zuständige Stelle, auf katholischer Seite an die zuständige diözesane Datenschutzaufsicht, in mehreren Regionen gebündelt bei überdiözesanen Datenschutzzentren.

Der zeitliche Maßstab unterscheidet sich im Wortlaut: Das Kirchliche Datenschutzgesetz der katholischen Kirche nennt ausdrücklich die Meldung unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden, mit Begründungspflicht bei Verzögerung. Das Datenschutzgesetz der EKD verlangt die Meldung unverzüglich, wenn die Verletzung voraussichtlich zu einem nicht unerheblichen Risiko für die Rechte natürlicher Personen führt, ohne im Gesetzestext eine Stundenzahl zu nennen. Praktisch heißt das für beide Seiten dasselbe: Du meldest, sobald du eine

belastbare erste Einschätzung hast, und lieferst nach. Beide Gesetze erlauben ausdrücklich, Informationen schrittweise nachzureichen.

Bei hohem Risiko kommt die Benachrichtigung der betroffenen Personen dazu. Die EKD-Regelung enthält dabei eine Besonderheit, die zu kirchlichen Strukturen passt: Ist die individuelle Benachrichtigung mit unverhältnismäßigem Aufwand verbunden, kann stattdessen öffentlich über die kirchenüblichen Wege informiert werden — Abkündigung, Gemeindebrief, Aushang — sofern das vergleichbar wirksam ist. Den vollständigen Meldeweg mit Formularen, Rollen und Übungsvorlage beschreibt der Beitrag [Datenpannen bei kirchlichen Trägern: Meldung an BfD EKD oder Diözesandatenschutzbeauftragten](#).

WARNUNG · Zwei Fristen laufen gleichzeitig — und niemand merkt es

Die Meldung an die kirchliche Aufsicht ist die eine Uhr. Die zweite läuft, wenn dein Träger zusätzlich unter besondere sektorspezifische Meldepflichten fällt — etwa als Krankenhaus mit kritischer Infrastruktur oder als Einrichtung mit eigener Meldepflicht gegenüber Heimaufsicht, Landesjugendamt oder Kostenträger. In der Übung gehört deshalb auf ein Blatt: welche Meldepflichten gelten für uns, an wen, wie schnell, und wer stellt sicher, dass sie nicht in derselben Nacht vergessen werden.

Kommunikation mit Gemeinde, Angehörigen und Belegschaft

Die Kommunikation ist bei kirchlichen Trägern kein Anhängsel, sondern der halbe Schaden. Angehörige rufen an, weil sie ihre Mutter nicht erreichen. Eltern wollen wissen, ob die Kita öffnet. Ehrenamtliche fragen, ob der Gemeindebrief erscheint. Und die Belegschaft erfährt es sonst aus der Zeitung — was nach dem Selbstverständnis der Dienstgemeinschaft die schlechteste aller Varianten ist.

- **Drei Botschaften, vorformuliert:** eine für Betroffene, eine für die Öffentlichkeit, eine für die Belegschaft. Im Notfallordner, auf Papier, in einfacher Sprache.
- **Ein Kanal, der ohne eigene IT funktioniert:** Telefonansage, eine Seite auf einer extern gehosteten Adresse, Aushang. Die eigene Website liegt erfahrungsgemäß mit.
- **Eine Sprachregelung für die Erpressungsfrage:** Ob gezahlt wird, entscheidet der Träger, nicht die IT — und die Antwort nach außen lautet nicht „kein Kommentar“, sondern eine abgestimmte Formulierung.
- **Seelsorgliche Begleitung mitdenken:** Für Beschäftigte, die Fehler gemacht haben könnten, und für Klientinnen und Klienten, deren Akten betroffen sind. Das ist kein Beiwerk, das ist Kernkompetenz kirchlicher Träger.

Die folgende Tabelle ist der Kern der Übung. Sie gehört ausgedruckt auf den Tisch, und sie gehört nach der Übung ausgefüllt in die Notfalldokumentation — mit Namen statt Funktionen.

Phase	Was passiert	Was der Träger tun muss	Wer entscheidet
0 — Vorlauf (Tage bis Wochen)	Phishing, Identitätsübernahme, stilles Mitlesen, Datenabfluss	Auffälligkeiten auswerten: neue MFA-Methoden, Postfachregeln, Anmeldungen aus unerwarteten Ländern	IT-Leitung in Abstimmung mit der örtlich beauftragten Person für den Datenschutz
1 — Entdeckung	Systeme reagieren nicht, Erpresserschreiben liegt vor	Meldekette auslösen, Krisenstab einberufen, Uhrzeit protokollieren, nichts überschreiben	Rufbereitschaft löst aus; Geschäftsführung oder Vorstand übernimmt die Leitung
2 — Eindämmung	Ausbreitung läuft weiter, jede Minute zählt	Netze trennen, Konten sperren, Sitzungen widerrufen, Fernzugänge schließen,	Geschäftsführung auf Vorschlag der IT — mit vorab erteilter schriftlicher

		Beweise sichern	Vollmacht
3 – Notbetrieb	Einrichtungen arbeiten ohne IT weiter	Papier-Rückfallebene auslösen, Dienstpläne sichern, Erreichbarkeit herstellen, Mehrarbeit regeln	Einrichtungsleitungen; Mehrarbeit und Notdienstpläne mit der MAV
4 – Bewertung und Meldung	Umfang unklar, Datenabfluss wahrscheinlich	Risiko bewerten, an die kirchliche Aufsicht melden, weitere Meldepflichten prüfen, Dokumentation anlegen	Datenschutzbeauftragte Person bereitet vor; Geschäftsführung meldet
5 – Kommunikation	Angehörige, Presse und Belegschaft fragen nach	Vorformulierte Botschaften freigeben, einen Kanal bedienen, Sprachregelung durchhalten	Geschäftsführung gemeinsam mit der Kommunikation
6 – Benachrichtigung Betroffener	Hohes Risiko für einzelne Personen ist erkennbar	Betroffene benachrichtigen oder – bei unverhältnismäßigem Aufwand – kirchenüblich öffentlich informieren	Geschäftsführung auf Empfehlung der datenschutzbeauftragten Person
7 – Wiederanlauf	Systeme kommen zurück, Vertrauen noch nicht	Reihenfolge festlegen, sauber neu aufbauen statt zurücksichern, Zugänge neu ausgeben	IT-Leitung mit Forensik; Freigabe durch die Geschäftsführung
8 – Nachbereitung	Alltag kehrt zurück, Erkenntnisse verflüchtigen sich	Auswertung, Maßnahmenplan, Aktualisierung der Notfallunterlagen, nächste Übung terminieren	Geschäftsführung; Bericht an Gremium und Aufsicht

WICHTIG · Aus der forensischen Praxis: der Moment, in dem niemand den Stecker ziehen durfte

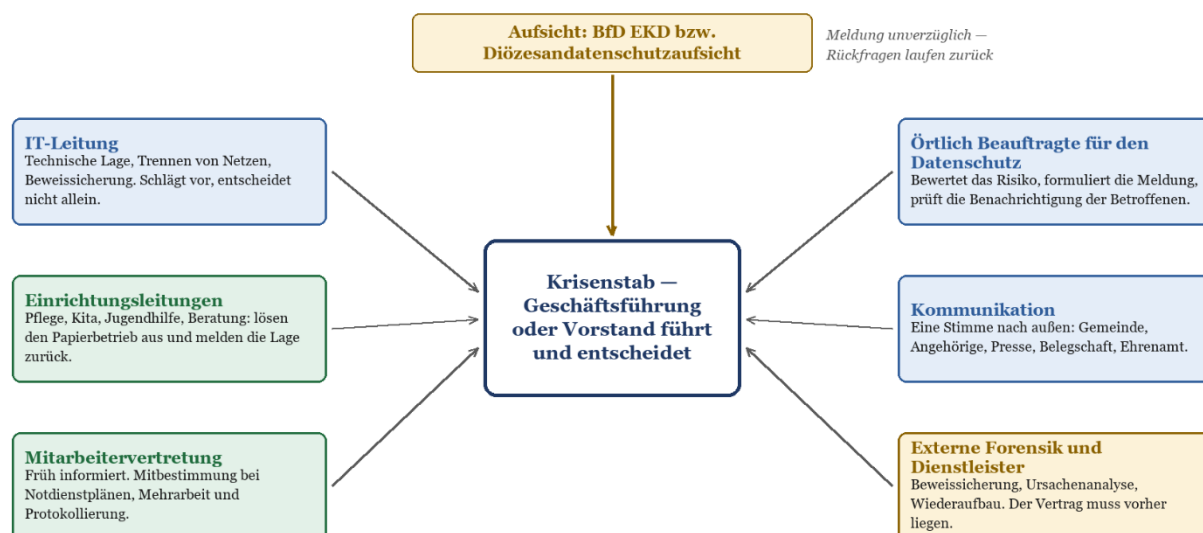
Ein katholischer Krankenhausverbund mit mehreren Standorten, ein Freitag im Spätherbst, kurz nach drei Uhr morgens. Die Verschlüsselung lief seit etwa vierzig Minuten und arbeitete sich über die Standortkopplung vom Verwaltungsstandort zu den Häusern vor. Die technische Frage war zu diesem Zeitpunkt trivial: eine Kopplung deaktivieren, zwei Minuten Arbeit.

Die Frage, die niemand beantworten konnte, lautete: Wer darf das anordnen? Der diensthabende Administrator wollte die Verantwortung nicht allein tragen – verständlich, denn das Trennen betraf auch Systeme mit Patientenbezug. Der IT-Leiter war erreichbar, verwies aber auf die Geschäftsführung. Die Geschäftsführung war zu zweit und beide der Auffassung, dass ein Eingriff dieser Tragweite die Zustimmung des jeweils anderen brauche. Eine Person aus dem Generalvikariat wurde geweckt, weil jemand die Trägerschaft erwähnte. In der Telefonkonferenz saßen nach einer Dreiviertelstunde neun Personen und diskutierten Zuständigkeiten.

Die Kopplung wurde um 05:06 Uhr getrennt. In den einhundertvierzehn Minuten dazwischen kamen zwei weitere Standorte dazu. Der Mehraufwand im Wiederaufbau lag im deutlich sechststelligen Bereich, die Verzögerung im Wiederanlauf bei fast zwei Wochen. Im Nachgespräch sagte einer der Geschäftsführer einen Satz, den man sich aufschreiben sollte: „Wir hatten für jede Beschaffung über 5.000 Euro eine Regelung. Für das Abschalten des Hauses hatten wir keine.“

Die Konsequenz war eine halbe Seite Dienstanweisung: Bei begründetem Verdacht auf laufende Verschlüsselung darf die jeweils diensthabende IT-Rufbereitschaft Netzkopplungen und Fernzugänge ohne Rückfrage trennen; die Entscheidung ist zu protokollieren und unverzüglich der Geschäftsführung anzuzeigen; ein Rückgängigmachen erfordert deren ausdrückliche Freigabe. Diese halbe Seite ist vermutlich das wirtschaftlichste Dokument, das dieser Verbund je erstellt hat.

Skizze 4: Wer entscheidet was — der Krisenstab eines kirchlichen Trägers



Alle sechs Rollen liefern zu. Entschieden wird in der Mitte — und zwar von Menschen mit Namen, nicht von Funktionen.

Die einzige Frage, die vor dem Ernstfall schriftlich beantwortet sein muss: Wer darf den Betrieb anhalten — und wer darf ihn wieder anfahren?

Skizze 4: Entscheidungswege im Krisenstab. Der Pfeil nach oben — zur Aufsicht — wird am häufigsten vergessen.

Red Team: wenn die Übung nicht am Tisch bleibt

Das Tabletop prüft Entscheidungen. Eine Red-Team-Übung prüft, ob die Annahmen stimmen, auf denen diese Entscheidungen beruhen. Der Unterschied ist unangenehm konkret: Im Tabletop sagt die IT, dass die Zwei-Faktor-Anmeldung überall greift. Im Red Team stellt sich heraus, dass vierzehn Konten eine dauerhafte Ausnahme haben, weil das vor drei Jahren einmal nötig war.

Was ein Red-Team-Einsatz bei kirchlichen Trägern prüft

- **Erreichbarkeit von außen:** welche Dienste, Fernwartungszugänge und Altanwendungen aus dem Internet erreichbar sind — inklusive der Systeme, von denen niemand mehr wusste.
- **Phishing-Resistenz in der Fläche:** gezielte, abgestimmte Simulation gegen Pfarrbüros, Verwaltung und Einrichtungen, ausgewertet nach Bereich statt nach Person.
- **Identitätsschicht:** Ausnahmen im Conditional Access, privilegierte Rollen ohne zeitliche Begrenzung, Gastkonten aus dem Ehrenamt, Anwendungsberechtigungen mit weitreichendem Zugriff.
- **Weg vom Konto zum Verzeichnis:** Dienstkonten, veraltete Protokolle, Vertrauensstellungen zwischen Landeskirche, Verband, Träger und Einrichtung.
- **Widerstandsfähigkeit der Sicherung:** ob ein Konto mit administrativen Rechten die Sicherungen löschen kann — die Frage, die nach jedem echten Vorfall zuerst gestellt wird.
- **Erkennung und Reaktion:** ob die Aktivität überhaupt auffällt, wie lange es dauert und wer am Ende angerufen wird.

Was vorher schriftlich geregelt sein muss

Ein Red Team ohne saubere Beauftragung ist kein Test, sondern ein Vorfall. Für kirchliche Träger kommen zu den üblichen Punkten einige hinzu, die man nicht improvisieren sollte.

Punkt	Warum er bei kirchlichen Trägern besonders zählt	Wer zustimmt
-------	--	--------------

Auftrag und Umfang	Genaue Abgrenzung, welche Träger, Einrichtungen und Rechtsträger überhaupt zum Umfang gehören — Gemeinden sind eigenständig	Geschäftsführung, gegebenenfalls Gremium
Tabubereiche	Seelsorge, Beichte, Beratungsverläufe und Patientenversorgung bleiben außen vor; das ist keine Verhandlungssache	Geschäftsführung und datenschutzbeauftragte Person
Beteiligung der MAV	Simulierte Angriffe erzeugen personenbezogene Auswertungen; MVG-EKD und MAVO greifen	Mitarbeitervertretung, in der Regel per Dienstvereinbarung
Auswertungstiefe	Ergebnisse nach Bereich statt nach Person; keine Leistungskontrolle durch die Hintertür	MAV und Geschäftsführung gemeinsam
Auftragsverarbeitung	Der Dienstleister sieht personenbezogene Daten; Vertrag nach DSGVO-EKD oder KDG erforderlich	Datenschutzbeauftragte Person, Geschäftsführung
Abbruchkriterien	Klare Regel, wann und durch wen abgebrochen wird, wenn die Versorgung berührt wird	Geschäftsführung, IT-Leitung, Testleitung
Notfallkontakt rund um die Uhr	Damit ein echter Vorfall während der Übung nicht für die Übung gehalten wird	IT-Leitung und Testleitung

Vorher aufräumen — sonst übst du das Offensichtliche

Es gibt einen Reihenfolgeeffekt, den man in der Beratung immer wieder sieht: Wer ein Red Team auf einen ungeprüften Tenant loslässt, bekommt einen Bericht, in dem zehn Befunde stehen, die man auch ohne Test gefunden hätte — und bezahlt dafür einen Angriffssimulationspreis. Sinnvoller ist es, die Identitätsschicht vorher zu sortieren. Eine strukturierte [Entra-ID-Tenant-Überprüfung für kirchliche Träger](#) findet Ausnahmen, verwaiste Berechtigungen und privilegierte Rollen deutlich billiger als ein Red Team. Ebenso gehört das Regelwerk aus dem Beitrag [Conditional Access und MFA in Kirche und Diakonie](#) vorher in einen belastbaren Zustand, und die Architektur der Identitäten zwischen Landeskirche, Verband, Träger und Einrichtung sollte geklärt sein — dazu der Beitrag [Entra ID für kirchliche Träger](#).

TIPP · Zwei Dinge, die vor jeder Übung erledigt sein sollten

Erstens: Notfallzugriffskonten. Microsoft empfiehlt mindestens zwei reine Cloudkonten in der Standarddomäne des Tenants, ohne Verbindung zum lokalen Verzeichnis, abgesichert mit phishingresistenten Verfahren wie FIDO2-Passkeys oder zertifikatbasierter Anmeldung, ausgenommen von blockierenden Conditional-Access-Regeln, in Privileged Identity Management dauerhaft aktiv statt nur berechtigt, mit Alarmierung bei jeder Anmeldung und einer Funktionsprüfung mindestens alle 90 Tage. Die Zugangsdaten gehören an getrennte, gesicherte Orte — nicht in den Kennworttresor, der mitverschlüsselt wird.

Zweitens: die Aufbewahrung der Protokolle. Im Standard hält das einheitliche Überwachungsprotokoll in Microsoft Purview 180 Tage vor. Wenn ein Angreifer vier Monate im Tenant war, bevor er zuschlägt, ist das knapp. Mit Audit Premium liegen Protokolle aus Entra ID, Exchange, SharePoint und OneDrive standardmäßig ein Jahr vor. Diese Entscheidung triffst du vor dem Vorfall oder gar nicht.

FAKTEN · Wenn du das nicht allein stemmen willst

Eine begleitete Notfall- und Red-Team-Übung bringt genau das mit, was intern fehlt: ein realistisches Szenario, eine neutrale Moderation, jemanden, der die unangenehmen Fragen stellt, und ein Protokoll, das anschließend als Maßnahmenplan taugt. Für kirchliche Träger kommt dazu, dass Meldewege, Mitbestimmung und Gremienlogik von vornherein richtig eingebaut sind statt nachträglich erklärt.

Die Details zu Vorgehen, Umfang und Festpreis stehen auf der Beratungsseite. Wenn im Anschluss

die Belegschaft mitgenommen werden soll — Pfarrbüro, Verwaltung, Pflege, Kita, Ehrenamt — passen dazu die Schulungsangebote für kirchliche Träger.

- › [Microsoft 365 Beratung für kirchliche Träger](#)
- › [Microsoft 365 Schulungen für kirchliche Träger](#)

Häufige Fragen

Wie oft sollten wir eine Notfallübung machen?

Einmal im Jahr ein Tabletop mit dem vollständigen Krisenstab, dazu einmal jährlich eine kleine Überprüfung der Papier-Rückfallebene in jeder Einrichtung. Eine technische Red-Team-Übung ist kein Jahresritual; sie lohnt sich, wenn sich die Architektur wesentlich geändert hat oder wenn seit der letzten Prüfung mehr als zwei Jahre vergangen sind. Wichtiger als die Frequenz ist, dass nach jeder Übung ein Maßnahmenplan mit Namen und Terminen entsteht — sonst übst du jedes Jahr dieselben Erkenntnisse.

Wir sind eine kleine Kirchengemeinde ohne eigene IT. Ist das für uns überhaupt relevant?

Ja, aber in kleinerem Format. Für eine Gemeinde reichen drei Dinge: eine Telefonliste auf Papier, eine Handlungsanweisung für die ersten dreißig Minuten und die Klarheit darüber, wer im Kirchenkreis oder Dekanat angerufen wird. Die eigentliche Übung findet sinnvollerweise auf der Ebene statt, die die Technik betreibt — also beim Kirchenkreis, beim Verband oder beim Träger. Die Gemeinde übt ihren eigenen Teil mit: Wer schließt das Pfarrbüro, wer informiert das Presbyterium oder den Kirchenvorstand, wie erreichen uns Menschen, wenn weder Mail noch Telefonanlage funktionieren.

Müssen wir die Mitarbeitervertretung wirklich in die Übung einbeziehen?

Einbeziehen ja, und zwar aus zwei Gründen. Rechtlich, weil im Notfall genau die Themen entstehen, die nach MVG-EKD und MAVO mitbestimmungsrelevant sind: Notdienstpläne, Mehrarbeit, Auswertung von Protokolldaten, gegebenenfalls Verdacht gegen einzelne Beschäftigte. Praktisch, weil eine MAV, die den Krisenstab aus der Übung kennt, im Ernstfall in Stunden statt in Wochen zustimmt. Wie das dauerhaft geregelt wird, steht im Beitrag zur Mitarbeitervertretung und Microsoft 365.

Schützt uns Microsoft 365 nicht ohnehin vor Ransomware?

Es schützt einen großen Teil des Weges. Defender für Office 365 entschärft Phishing-Mails, Conditional Access erschwert die Übernahme von Konten, und die automatische Angriffsunterbrechung in Defender XDR isoliert Geräte und Konten mitten im laufenden Angriff. Was Microsoft 365 nicht schützt, ist alles, was nicht im Tenant liegt: der Dateiserver, die Pflegedokumentation, das Krankenhausinformationssystem, die Finanzbuchhaltung und der lokale Verzeichnisdienst. Bei den meisten kirchlichen Trägern liegt dort der eigentliche Betrieb — und dort schlägt die Verschlüsselung zu.

Wie lange dauert es realistisch, bis wir wieder arbeiten können?

Für die Cloud-Anteile kann es schnell gehen: Microsoft 365 Backup stellt einzelne Dateien in Minuten wieder her und kleinere SharePoint-Websites mit einem Express-Wiederherstellungspunkt typischerweise in unter zwanzig Minuten; bei sehr vielen Websites oder Postfächern rechnet Microsoft mit bis zu 250 Schutzeinheiten pro Stunde. Für das lokale Umfeld gilt eine andere Rechnung. Wenn der Verzeichnisdienst kompromittiert ist, wird er neu aufgebaut

und nicht zurückgesichert. Realistisch sind für einen mittleren Träger zwei bis acht Wochen bis zum geordneten Betrieb — mit Notbetrieb ab dem ersten Tag.

Dürfen wir Lösegeld zahlen?

Das ist eine Entscheidung des Trägers, keine der IT, und sie gehört ausdrücklich in die Übung — samt der Frage, wer sie überhaupt treffen darf und ob das Gremium einzubinden ist. Aus der forensischen Praxis: Eine Zahlung beseitigt weder die Meldepflicht gegenüber der kirchlichen Aufsicht noch die Benachrichtigungspflicht gegenüber Betroffenen, und sie garantiert keine Rückgabe oder Löschung abgeflossener Daten. Für einen kirchlichen Träger kommt die Frage hinzu, wie sich eine Zahlung an eine kriminelle Organisation zum eigenen Selbstverständnis und zur Verwendung von Kirchensteuer- und Spendenmitteln verhält. Diese Diskussion führt man besser an einem Dienstagnachmittag als um vier Uhr morgens.

Was ist der Unterschied zwischen einer Datenpannen-Übung und einer Notfallübung?

Die Datenpannen-Übung trainiert einen schmalen, präzisen Ablauf: erkennen, bewerten, melden, dokumentieren, gegebenenfalls benachrichtigen. Sie dauert typischerweise zwei Stunden und ist vor allem eine Sache der datenschutzbeauftragten Person und der Leitung. Die Notfallübung ist das größere Format: Sie enthält die Meldung als einen Baustein, behandelt aber zusätzlich Betriebsfortführung, Kommunikation, Mitbestimmung und Wiederanlauf. Sinnvoll ist die Reihenfolge: erst die Datenpannen-Übung, weil sie klein und schnell ist, dann das Tabletop.

Was kostet uns eine solche Übung im Betrieb?

Der direkte Aufwand ist überschaubar: ein halber Tag für sechs bis zehn Personen, dazu Vorbereitung. Der indirekte Aufwand entsteht nach der Übung, weil der Maßnahmenplan Arbeit erzeugt — genau das ist der Zweck. Zur Einordnung: Der Mehraufwand, den die einhundertvierzehn Minuten Zuständigkeitsdiskussion in dem oben beschriebenen Krankenhausfall verursacht haben, entspricht dem Übungsbudget eines mittleren Trägers für die nächsten Jahrzehnte.

Kann die Übung auch remote stattfinden?

Sie kann, aber sie sollte es beim ersten Mal nicht. Der Erkenntnisgewinn entsteht an den Stellen, an denen sich Menschen im Raum ansehen und feststellen, dass beide dachten, der jeweils andere sei zuständig. In einer Videokonferenz verschwindet dieser Moment. Ab dem zweiten Durchlauf, wenn die Rollen sitzen, funktioniert ein Remote-Format für kürzere Auffrischungen gut — auch mit dem netten Nebeneffekt, dass man dann gleich prüfen kann, ob der Krisenstab über mobile Geräte handlungsfähig wäre.

Fazit

Kirchliche Träger werden angegriffen, weil sie erreichbar sind und weil ihre Daten Menschen verwundbar machen. An dieser Lage ändert sich kurzfristig nichts. Was du ändern kannst, ist die Zeit zwischen dem Anruf des Nachtdienstes und der ersten wirksamen Entscheidung.

Microsoft 365 liefert dafür mehr, als viele Träger nutzen: phishingresistente Anmeldung, Angriffssimulationstraining mit Auswertung nach Bereichen, automatische Angriffsunterbrechung über Endgeräte und Identitäten hinweg, unveränderliche Sicherungen für die Cloud-Anteile und Protokolle, die lange genug vorhalten, um einen Vorfall überhaupt rekonstruieren zu können. Diese Bausteine ersetzen aber keine Entscheidung. Sie setzen sie voraus.

Deshalb ist die wirksamste Investition nicht die nächste Lizenzstufe, sondern ein halber Tag, an dem Geschäftsführung, IT, Datenschutz, Mitarbeitervertretung, Kommunikation und Einrichtungsleitungen gemeinsam durchspielen, was passiert, wenn es passiert. Am Ende dieses

halben Tages steht im besten Fall eine unspektakuläre halbe Seite Dienstanweisung — die Antwort auf die Frage, wer den Stecker ziehen darf. In der Nacht, in der es darauf ankommt, ist diese halbe Seite mehr wert als jedes Sicherheitsprodukt im Katalog.

Und falls dir das alles nach viel Aufwand klingt: Der Aufwand entsteht ohnehin. Du kannst ihn planen oder ihn dir von jemandem terminieren lassen, der dafür kein Verständnis hat und in Bitcoin bezahlt werden will.

FAKTEN · Weiter im Thema

Diese Beiträge greifen ineinander — in dieser Reihenfolge ergeben sie einen belastbaren Vorbereitungspfad:

- › [Datenpannen bei kirchlichen Trägern: Meldung an BfD EKD oder Diözesandatenschutzbeauftragten](#)
- › [Entra-ID-Tenant-Überprüfung für kirchliche Träger](#)
- › [Conditional Access und MFA in Kirche und Diakonie](#)
- › [Mitarbeitervertretung und Microsoft 365](#)
- › [Klientendaten in Diakonie und Caritas](#)
- › [Microsoft 365 im kirchlichen Krankenhaus](#)
- › [Kita, Pflege, Jugendhilfe: Frontline-Arbeitsplätze in Microsoft 365](#)