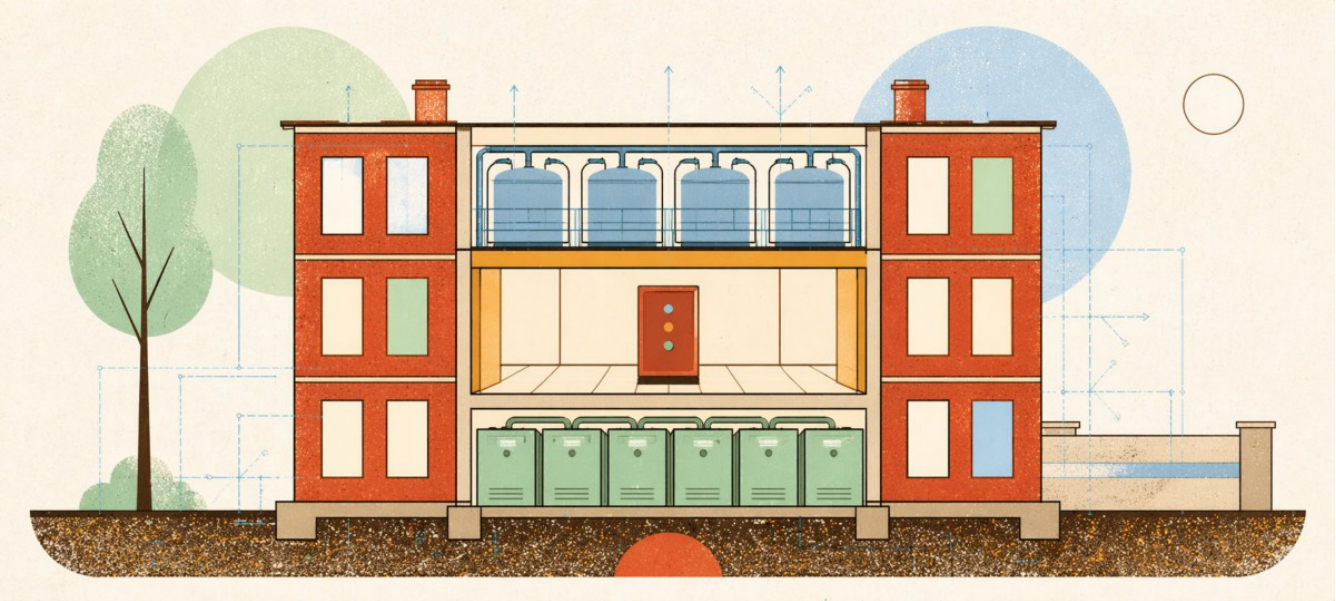
SICHERHEIT FÜR IHREN EIGENEN STACK

Ihre Unternehmensdaten im NexaStack – *wie sicher ist das wirklich?*



Wer heute aus den großen Abo-Plattformen aussteigt und auf einen eigenen, selbst betriebenen Software-Stack umstellt, fragt zurecht: Sind meine Firmendaten auf einem eigenen Server eigentlich sicherer oder unsicherer als bei Microsoft, Google oder Dropbox?

Die ehrliche Antwort: Auf einem schlecht eingerichteten Server — unsicherer. Auf einem so eingerichteten Server wie Ihrem NexaStack — deutlich sicherer. Und vor allem ist klar, wo Ihre Daten liegen, wer Zugrif hat und wer im Notfall verantwortlich ist. Beides ist bei einer amerikanischen Cloud nicht der Fall.

> **Das Bild: Ihr NexaStack als Firmengebäude.** In diesem Gebäude liegen alle Unternehmensdaten: Dokumente, Kalender, Kontakte, Passwörter, Chats, Verträge. Ein Angreifer aus dem Internet müsste *fünf Hürden nacheinander* überwinden, um an

> Daten zu kommen. Reißt eine, steht er vor der nächsten. Er müsste alle fünf gleichzeitig und unbemerkt schaffen — in derselben Nacht.

HÜRDE 1

Der Standort

01

Das Gebäude steht nicht irgendwo, sondern in einem bewachten, zertifizierten Rechenzentrum in Karlsruhe. Zutrittskontrollen, Videoüberwachung, Brandschutz, Notstromversorgung. Deutsches Recht, deutsche Datenschutzbehörden, DSGVO-konform. Dass kein amerikanischer Anbieter beteiligt ist, hat einen konkreten Wert: Kein US-Gericht kann den Betreiber verpflichten, Ihre Firmendaten herauszugeben — bei US-Cloud-Anbietern ist das rechtlich sehr wohl möglich (Stichwort CLOUD Act). Mit dem Rechenzentrumsbetreiber besteht ein schriftlicher Auftragsverarbeitungsvertrag, der alle datenschutzrechtlichen Pflichten festhält.

HÜRDE 2

Die Eingangstür

02

Ein normales Firmengebäude hat viele Türen, Fenster und Lieferanteneingänge. Ihres nicht. Von außen existiert nur ein einziger Eingang. Alle anderen Wände sind fensterlos und verschlossen. Das nennt man Firewall — eine digitale Brandschutzwand, die alles blockiert, was nicht ausdrücklich erlaubt ist.

Und diese einzige Tür hat **kein Schloss, in das sich ein Passwort eintippen ließe**. Das ist kein Versehen, sondern Absicht: Die Möglichkeit, sich mit einem Passwort anzumelden, gibt es schlicht nicht. Die Tür öffnet nur, wenn ein ganz bestimmter digitaler Schlüssel vorgezeigt wird — ein mathematisch einzigartiger Code, der ausschließlich auf einem einzigen Administrations-Gerät existiert und nirgendwo sonst auf der Welt. Dieser Schlüssel lässt sich nicht erraten, nicht abfangen, nicht per Wörterbuch knacken. Das klassische Passwort-Raten, das Hacker in Schleife probieren, läuft bei Ihrem Server ins Leere — weil es nichts zu raten gibt.

Wer es trotzdem versucht, fliegt hart raus: Drei Fehlversuche, und die Internet-Adresse des Angreifers wird für 24 Stunden komplett gesperrt. Bei Wiederholung wird die Sperre automatisch verlängert. Aktuell sind auf diese Weise über 80 Angreifer dauerhaft ausgesperrt — die meisten geben nach dem ersten Bann für immer auf.

Zusätzlich ist auch der klassische Generalschlüssel des Servers — der sogenannte Administrator-Zugang, der alles darf — komplett deaktiviert. Niemand kann sich direkt als „Super-Admin" einloggen. Dieser Zugang lässt sich erst nach einer regulären Anmeldung und einem bewussten zweiten Schritt aktivieren. Klingt nach einer Kleinigkeit, ist aber eine der häufigsten Ursachen, warum fremde Server übernommen werden: Viele Betreiber lassen diesen Generalschlüssel aus Bequemlichkeit offen — und genau darüber werden sie ausgeraubt.

HÜRDE 3

03

Die einzelnen Büros im Inneren

Nehmen wir rein hypothetisch an, ein Angreifer hätte doch einen Weg durch die Tür gefunden. Was findet er dann vor?

Nicht einen großen, offenen Raum mit allen Daten, sondern ein Gebäude voller einzeln abgeschlossener Büros. Jede Anwendung hat ihr eigenes Büro mit eigener Tür, eigenem Schlüssel und eigenem Aktenschrank: Nextcloud in seinem Büro, OnlyOffice in seinem Büro, Vaultwarden in seinem Büro, Paperless in seinem Büro. Etwa 50 solcher Büros insgesamt, auf 22 voneinander abgetrennten Fluren.

Der entscheidende Punkt: **Diese Büros haben untereinander keine Verbindungstüren.** Wer ins Nextcloud-Büro käme, steht dort ausschließlich vor den Nextcloud-Akten. Er sieht keine Passwörter aus Vaultwarden, keine Dokumente aus OnlyOffice, keine Rechnungen aus der Buchhaltung. Er sieht nicht einmal, dass diese anderen Büros existieren. Jede Anwendung hat zusätzlich ihren eigenen, getrennten Aktenschrank mit eigenem Schlüssel — ein Einbruch in eine Anwendung ist also niemals automatisch ein Einbruch in alle.

In jedem Büro sitzt außerdem ein strenger digitaler Aufpasser. Er überwacht jede Handlung der Software in diesem Büro und lässt nur genau das zu, was die Software für ihren eigentlichen Zweck braucht. Gelänge es einem Angreifer, eine Anwendung zu übernehmen und für andere Zwecke zu missbrauchen — etwa Daten zu kopieren, andere Bereiche anzugreifen oder Schadsoftware nachzuladen — blockiert der Aufpasser das sofort und schlägt Alarm. Auf einer übernommenen Nextcloud-Instanz lässt sich deshalb nicht „mal schauen, was sonst noch auf dem Server liegt". Der Angreifer sitzt in diesem einen Büro fest.

Noch eine Sache, die unsichtbar, aber wichtig ist: Jede Kommunikation von Ihrem Laptop oder Handy zum Server läuft verschlüsselt. Niemand, der sich dazwischenschaltet — in einem Café-WLAN, bei einem Hotel-Zugang, bei einer öffentlichen Veranstaltung — kann mitlesen, welche Dokumente geöffnet oder welche Passwörter eingegeben werden.

HÜRDE 4

04

Der Wachdienst

Auf dem Server läuft rund um die Uhr ein digitaler Wachdienst mit zwei Aufgaben.

Erstens: Jede verdächtige Aktivität wird mitgeschrieben. Jede Anmeldung, jeder Zugriff, jede Änderung an einer sicherheitskritischen Datei landet in einem Protokoll, das einsehbar und auswertbar ist. Wenn also tatsächlich etwas Ungewöhnliches passiert, ist es lückenlos dokumentiert — nicht irgendwo im Nebel.

Zweitens: Das System prüft sich selbst. Jede Nacht läuft automatisch eine Kontrolle, ob auch nur eine einzige wichtige Datei unerwartet verändert wurde — so, wie ein Museumswärter jede Nacht prüft, ob alle Bilder noch an ihrem Platz hängen. Wöchentlich suchen zusätzlich spezialisierte Programme gezielt nach bekannter Schadsoftware, versteckten Manipulationen und neu bekannt gewordenen Sicherheitslücken in der installierten Software. Findet sich etwas, wird automatisch alarmiert.

Der in der Praxis wichtigste Punkt: **Sicherheitsupdates werden automatisch eingespielt.** Denn der gefährlichste Server ist nicht der, der angegriffen wird — sondern der, der seit Monaten kein Update mehr bekommen hat und mit bekannten, längst geschlossenen Lücken im Netz steht.

HÜRDE 5

05

Die Rückversicherung: tägliche Sicherungen

Nehmen wir den schlimmsten Fall an: Trotz aller vier vorherigen Hürden passiert doch etwas Schlimmes. Ein Hardware-Defekt. Ein Brand im Rechenzentrum. Oder ein sehr ausgeklügelter Angreifer, der alle Daten verschlüsselt und Lösegeld fordert — das, was in den Nachrichten als „Ransomware" auftaucht.

Dann ist trotzdem nichts verloren. Jede Nacht um 04:00 Uhr wird eine vollständige, verschlüsselte Kopie aller Daten, Datenbanken und Einstellungen an einen zweiten, physisch komplett getrennten Speicherort in Deutschland übertragen (betrieben von Hetzner, ebenfalls deutsches Recht, ebenfalls DSGVO-konform). Diese Kopien werden 14 Tage lang aufbewahrt — ein Rücksprung ist also auch dann noch möglich, wenn ein Problem erst eine Woche später auffällt.

Einmal pro Quartal wird getestet, ob sich aus diesen Sicherungen tatsächlich alles wiederherstellen lässt. Denn eine Sicherung, die nie getestet wurde, ist keine Sicherung, sondern eine Hoffnung. Im schwersten Notfall ist der komplette NexaStack innerhalb von **zwei bis vier Stunden** auf einem neuen Server wieder lauffähig. Kein Datenverlust, nur ein halber Arbeitstag Ausfall.

UND WENN TROTZ ALLEDEM ETWAS PASSIERT?

NexaStack

Zwei schriftliche Pläne greifen sofort.

ICON

Notfallplan bei Sicherheitsvorfällen

Legt minutengenau fest, was in den ersten 60 Minuten, den ersten 4 Stunden und den ersten 72 Stunden passiert: Wer wen informiert, welche Daten sofort gesichert werden, wann die Datenschutzbehörde verständigt wird (innerhalb der 72-Stunden-Frist nach DSGVO) und wann Sie als Geschäftsführer eingebunden werden.

ICON

Notfallhandbuch & TOM

Enthält konkrete Schritt-für-Schritt-Drehbücher für alle realistischen Ausfall-Szenarien — damit im Ernstfall nicht nachgedacht, sondern abgearbeitet wird. Ergänzt durch eine formale Dokumentation nach Art. 32 DSGVO („TOM"), die bei Datenschutz-Prüfungen oder Kundenanfragen vorzeigbar ist.

WAS DAS IN DER SUMME BEDEUTET

Ihre Daten liegen nicht „irgendwo im Internet".

Sie liegen in einem bewachten deutschen Rechenzentrum, hinter einer einzigen Tür, die nur mit einem nicht kopierbaren Schlüssel öffnet, in Einzelbüros, die untereinander keine Verbindung haben, unter permanenter Selbstüberwachung und mit täglicher, verschlüsselter, tatsächlich getesteter Sicherung an einem zweiten Ort.

Das ist keine Theorie und keine Marketing-Aussage. Es ist exakt das Sicherheitsniveau, auf dem auch unsere eigene Produktivinfrastruktur läuft – dieselbe Umgebung, auf der unsere eigenen Kundendaten und unsere eigenen Geschäftsunterlagen liegen. Was für uns selbst gut genug ist, ist auch für Sie gut genug.