Dropsuite

Verkaufsblatt

Ist Ihre Microsoft 365-Umgebung wirklich geschützt?

Schützen Sie mehr als nur Inhalte. Sichern Sie den Zugriff mit Dropsuite Entra Backup.

Sie vertrauen Ihrem MSP, um Ihr Unternehmen zu schützen – und das tut es auch. Aber die meisten Menschen sind sich nicht bewusst, dass eines der größten Risiken in der heutigen Cloud-Umgebung nicht verlorene Dateien sind. Es ist der verlorene Zugriff.

Microsoft Entra ID (ehemals Azure AD) steuert, wer sich anmelden darf, worauf zugegriffen werden kann und welche Apps oder Geräte vertrauenswürdig sind. Wenn diese Zugriffseinstellungen geändert, gelöscht oder sogar versehentlich kompromittiert werden, kann das Ihre Geschäftsabläufe zum Stillstand bringen.

Warum das wichtig ist

Menschen machen Fehler

Menschliches Versagen ist für 60 % der Datenschutzverletzungen verantwortlich.[1] Ein einziger Fehlklick eines Teammitglieds kann Nutzer aussperren, wichtige Einstellungen löschen oder Ihre Umgebung gefährden.

Cyberangriffe zielen auf Identitätssysteme ab

In einem kürzlich erschienenen Bericht waren gestohlene Zugangsdaten (22 %) und ausgenutzte Schwachstellen (20 %) die wichtigsten Angriffspunkte.[1] Entra ID ist dabei oft das erste Ziel. Einmal eingedrungen, können Angreifer Richtlinien deaktivieren, die Mehrfaktor-Authentifizierung (MFA) umgehen und Anwendungen unbemerkt übernehmen.

Microsoft sichert dies nicht vollständig ab

Microsoft bietet keine vollständige Wiederherstellung für gelöschte Entra-ID-Richtlinien oder -berechtigungen an. Ohne Backup kann die Wiederherstellung des Zugangs Stunden dauern oder gar nicht möglich sein.

Dieses Ausmaß der Störung ist wichtig: 46 % der kleinen Unternehmen wurden Opfer eines Cyberangriffs, und fast jedes fünfte musste seine Tätigkeit einstellen oder Insolvenz anmelden.[2] Schon wenige Stunden Ausfallzeit können für kleine Unternehmen verheerend sein – bereits eine Stunde kann bis zu 100.000 USD an Produktivitäts- und Umsatzeinbußen sowie Wiederherstellungskosten kosten.[3]

Was kann ohne Entra Backup schiefgehen?

> *„Unbeabsichtigte Löschungen und Fehlkonfigurationen werden in Ihrem Tenant passieren. Um die Auswirkungen dieser unbeabsichtigten Ereignisse zu minimieren, müssen Sie darauf vorbereitet sein.“* [4]
>
> **- Microsoft**

Wenn Identitätssysteme ungeschützt sind, treten Störungen schnell und heftig auf:

- Eine gelöschte Richtlinie für bedingten Zugriff sperrt Ihre Remote-Mitarbeiter aus.
- Eine versehentliche Änderung der Compliance-Regeln für Geräte verhindert die Verbindung von Laptops.
- Ein Angreifer schaltet die MFA-Durchsetzung, und niemand bemerkt es, bis es zu spät ist.
- Es gibt keinen Nachweis, welcher Administrator die Änderungen vorgenommen hat, was die Ursachenforschung erschwert.

Ohne Backup können diese Probleme Stunden, den Geschäftsbetrieb stören und das Vertrauen Ihrer Kunden schädigen.

Schützen Sie das System, das alles andere schützt

Ihr MSP führt bereits Backups Ihrer E-Mails und Dateien durch. Aber Entra Backup fügt eine wichtige Ebene hinzu, um die Zugriffsregeln und Sicherheitsrichtlinien zu schützen, die Ihr Geschäft am Laufen halten. Mit Entra Backup kann Ihr MSP Sie dabei unterstützen:

- **Schnelle Wiederherstellung** nach einem Fehler oder Angriff
- **Ausfallzeiten** durch verlorenen Zugriff oder Fehlkonfigurationen **verhindern**
- **Ihre Mitarbeiter, Geräte und Anwendungen** vor unbefugter Nutzung **schützen**
- **Die Einhaltung von Vorschriften sichern** indem Sie eine vollständige Aufzeichnung aller Identitäts- und Zugriffsänderungen führen

Warten Sie nicht, bis der Zugriff verloren geht

Sprechen Sie mit Ihrem MSP über Dropsuite Entra Backup – denn Schutz Ihrer Daten bedeutet auch Schutz des Zugriffs.

1. Verizon, *Data Breach Investigations Report*, 2025.
2. Mastercard, *Cybersicherheit für kleine Unternehmen*, 2025.
3. ITIC, *Bericht zu Server- und Anwendungs-Ausfällen*, 2022.
4. Microsoft, *Best Practices für Wiederherstellbarkeit*, 2024.