365 % Risiko – was Microsoft nicht für Sie übernimmt

DI Gerald Eder

eDay Salzburg 2026

Neue Wege. Neue Lösungen.
Unsere digitale Zukunft.

17.03.2026

WKS
Unternehmensberatung · Buchhaltung · IT

DI Gerald Eder, BA
solbytech – Lieber von uns gehackt als von anderen!

seit Februar 2019

solbytech gmbh

CEO & Geschäftsführer solbytech GmbH

- Mitglied Branchenplattform Cybersicherheit für die Energiewirtschaft der DENA (Deutsche Energieagentur)
- Speaker & Vortragender
- Zertifizierungen: Data & IT-Security Expert

Was schätzen Sie: Wie sicher ist ein Unternehmen mit 65 % Secure Score?

Nehmen Sie sich kurz einen Moment – was ist Ihre spontane Antwort?

A	B	C
Ziemlich gut geschützt	Guter Start, aber mit offenen Risiken	Die Zahl allein sagt noch nicht genug

Was schätzen Sie: Wie sicher ist ein Unternehmen mit 65 % Secure Score?

Nehmen Sie sich kurz einen Moment – was ist Ihre spontane Antwort?

A	B	C ✓
Ziemlich gut geschützt	Guter Start, aber mit offenen Risiken	Die Zahl allein sagt noch nicht genug

Richtig ist **C**. Microsoft Secure Score zeigt, wie viele empfohlene Maßnahmen umgesetzt wurden – aber nicht, wie hoch das echte .
Geschäftsrisiko ist. Zwei Unternehmen mit gleichem Score können sehr unterschiedliche Risiken haben.

> „Secure Score ist ein Navi – aber kein Airbag."

Security Score: wichtig, aber nicht missverstehen

Was Secure Score leistet

- Zeigt, wo Maßnahmen fehlen
- Hilft bei der Priorisierung
- Zeigt Trends über die Zeit
- Ermöglicht Vergleiche mit ähnlichen Unternehmen

Was Secure Score nicht ist

- Kein Sicherheitszertifikat
- Kein Beweis, dass nichts passiert
- Keine absolute Messung des Breach-Risikos
- Kein Ersatz für eine echte Risikobewertung

Security Score: wichtig, aber nicht missverstehen

Was Secure Score leistet

- Zeigt, wo Maßnahmen fehlen
- Hilft bei der Priorisierung
- Zeigt Trends über die Zeit
- Ermöglicht Vergleiche mit ähnlichen Unternehmen

Was Secure Score nicht ist

- Kein Sicherheitszertifikat
- Kein Beweis, dass nichts passiert
- Keine absolute Messung des Breach-Risikos
- Kein Ersatz für eine echte Risikobewertung

Microsoft formuliert das selbst sehr klar: Secure Score ist **keine absolute Messung des Breach-Risikos**. Viele Unternehmen landen nicht bei 90+, sondern im Mittelfeld – typisch sind 40–60 %. Das Problem: Mittelfeld kann trotzdem hochriskant sein.

> „Wer hätte spontan gesagt: Ab 70 % ist man ziemlich sicher?" – Genau das ist der Denkfehler.

Der Kernfehler: Was Microsoft schützt – und was nicht

Microsoft verantwortet

- Rechenzentren & physische Infrastruktur
- Verfügbarkeit der Plattform
- Plattformbetrieb & Updates
- Basissicherheit der Services

Ihr Unternehmen verantwortet

- Identitäten & MFA
- Rollen & Berechtigungen
- Externe Freigaben
- Mail-Weiterleitungsregeln
- Datenklassifizierung
- Reaktion auf Vorfälle

Der Kernfehler: Was Microsoft schützt – und was nicht nicht

Microsoft verantwortet

- Rechenzentren & physische Infrastruktur
- Verfügbarkeit der Plattform
- Plattformbetrieb & Updates
- Basissicherheit der Services

Ihr Unternehmen verantwortet

- Identitäten & MFA
- Rollen & Berechtigungen
- Externe Freigaben
- Mail-Weiterleitungsregeln
- Datenklassifizierung
- Reaktion auf Vorfälle

„Microsoft betreibt die Wohnung. Aber wer einen Schlüssel hat, wer die Tür offen lässt und wer in den Aktenschrank sehen darf — das bleibt Ihre Verantwortung."

Warum KMU besonders gefährdet sind

Nicht weil KMU fahrlässig sind – sondern weil Microsoft 365 so bequem wirkt, dass Sicherheitsfragen im Alltag leicht unsichtbar werden.

Wenig Zeit

Sicherheit konkurriert täglich mit dem operativen Tagesgeschäft – und verliert meistens.

Standard bleibt Standard

Default-Einstellungen werden selten hinterfragt. Was funktioniert, gilt als sicher.

Keine klare Zuständigkeit

Niemand fühlt sich wirklich verantwortlich – Sicherheit ist irgendwie aller und damit niemandes Thema.

„Läuft doch"

Sicherheit wird mit Verfügbarkeit verwechselt. Wenn der Dienst läuft, gilt er als sicher.

Welche Risiken hinter gut gemeinten Defaults stecken

Nicht der eine große Hack ist oft das Problem — sondern mehrere kleine, normale Entscheidungen, die sich summieren.

MFA nicht konsequent

Fast alle haben MFA – außer die drei, bei denen es Probleme gab.

Alte Authentifizierungswege aktiv

Legacy-Protokolle wie SMTP AUTH oder IMAP umgehen moderne Schutzmaßnahmen.

Externe Freigaben zu offen

Anyone-Links, keine Ablaufdaten, keine Kontrolle über Empfänger.

Mailweiterleitungen bleiben unbemerkt

Kompromittierte Konten leiten automatisch nach außen weiter – bleibt unentdeckt.

Zu viele Admins / zu breite Rechte

Berechtigungen wurden nie bereinigt – wer einmal Admin war, bleibt Admin.

Kein sinnvolles Monitoring

Audit-Logging ist nicht aktiviert, Alerts fehlen, niemand schaut hin.

PRAXISFALL 1

MFA „ja eh, aber …"

Praxisszenario: Die Geschäftsführung und die Admins haben MFA. Drei normale Benutzer nicht — weil es bei einem Altgerät Probleme gab oder weil jemand nicht gestört werden wollte.

Das Risiko

MFA in Kombination mit dem Blockieren alter Verfahren kann laut Microsoft **mehr als 99,9 %** identitätsbezogener Angriffe abwehren. Jede Ausnahme öffnet eine Hintertür.

Lösung

- MFA für alle Benutzer, keine dauerhaften Ausnahmen
- Break-Glass-Konten sauber dokumentieren
- Security Defaults oder Conditional Access nutzen
- Einführung stufenweise, aber mit Enddatum

„Halb eingeführte MFA ist wie ein Sicherheitsgurt nur auf dem Fahrersitz."

PRAXISFALL 2

Altprotokolle – der unsichtbare Nebeneingang

Praxisszenario: MFA ist offiziell aktiv. Trotzdem gibt es noch einzelne Sonderwege – Scanner, Altsoftware, Altclients.
Das Unternehmen glaubt sich geschützt zu haben. Real existiert aber noch ein Nebeneingang.

Betroffene Protokolle

- POP, IMAP, SMTP AUTH
- Exchange ActiveSync
- Autodiscover, Remote PowerShell
- Ältere Exchange-Zugriffe

Maßnahmen

- Conditional Access im Report-only-Modus testen
- SMTP AUTH global deaktivieren, wenn nicht nötig
- Altgeräte und Altanwendungen aktiv bereinigen
- Gezielt nur für einzelne Mailboxen erlauben

„Wer weiß heute wirklich, ob noch ein Scanner, ein Multifunktionsgerät oder eine Altsoftware per SMTP AUTH oder ähnlichem sendet?"

PRAXISFALL 3

Externes Teilen – der gut gemeinte Datenverlust

Praxisszenario: Ein Mitarbeiter möchte schnell helfen und teilt einen Ordner per Link. Niemand denkt an Risiko.
Wochen später weiß keiner mehr, wer den Link weitergeleitet hat.

Präventiv

- Default-Linktyp auf intern setzen
- Anyone-Links nur wenn nötig
- Ablaufdaten für offene Links

Nachvollziehbarkeit

- Sharing Auditing im Audit Log
- Ereignisse wie AnonymousLinkCreated prüfen
- Gastfreigaben regelmäßig reviewen

Automatisiert erkennen

- Defender Alert Policies aktivieren
- Meldungen bei externem Sharing
- Optional: Defender for Cloud Apps

„Nicht jede Datenpanne beginnt mit Malware.
Manchmal beginnt sie mit: ”Ich schick schnell einen Link."

PRAXISFALL 4

Automatische Mail-Weiterleitung nach außen

Praxisszenario: Ein kompromittiertes Postfach bekommt unbemerkt eine Weiterleitungsregel. Ab dann gehen Angebote, Rechnungen oder Projektkommunikation automatisch nach außen – täglich, unbemerkt.

Erkennen

- Alerts in Microsoft Defender / Defender XDR nutzen
- Audit-Logs und Exchange-Regeln prüfen
- Externe Auto-Forwarding standardmäßig blockieren

Reagieren bei Kompromittierung

- Passwort & Sessions sofort zurücksetzen
- Weiterleitungsregeln entfernen
- MFA-Status prüfen & erzwingen
- Mailflow & Angreiferaktivitäten untersuchen

PRAXISFALL 4

Automatische Mail-Weiterleitung nach außen

Praxisszenario: Ein kompromittiertes Postfach bekommt unbemerkt eine Weiterleitungsregel. Ab dann gehen Angebote, Rechnungen oder Projektkommunikation automatisch nach außen – täglich, unbemerkt.

Erkennen

- Alerts in Microsoft Defender / Defender XDR nutzen
- Audit-Logs und Exchange-Regeln prüfen
- Externe Auto-Forwarding standardmäßig blockieren

Reagieren bei Kompromittierung

- Passwort & Sessions sofort zurücksetzen
- Weiterleitungsregeln entfernen
- MFA-Status prüfen & erzwingen
- Mailflow & Angreiferaktivitäten untersuchen

> „Wenn heute in einem Postfach eine unsichtbare Weiterleitung aktiv wäre — wer würde das in Ihrer Organisation innerhalb eines Tages merken?"

Warum Secure Score trotzdem wertvoll ist

Wichtig für die Balance: nicht gegen Microsoft argumentieren, sondern sauber einordnen. Secure Score ist ein nützliches Werkzeug – – wenn man es richtig einsetzt und versteht.

Secure Score hilft bei …

- Transparenz über den Konfigurationsstand
- Priorisierung von Maßnahmen
- Fortschrittsmessung über Zeit
- Governance-Gesprächen mit der Geschäftsführung

Secure Score ersetzt nicht …

- Eine echte Risikobewertung
- Den Business-Kontext Ihres Unternehmens
- Die Prüfung realer Ausnahmen und Altlasten
- Menschliche und organisatorische Schwächen

Microsoft positioniert Secure Score ausdrücklich als Hilfe zur **Verbesserung der Sicherheitslage** – nicht als vollständigen Realitätsersatz. Nutzen Sie ihn als Startpunkt, nicht als Entwarnung.

So würde ich es als KMU praktisch angehen

Stufe 1 – In wenigen Tagen

- MFA für alle aktivieren
- Security Defaults prüfen / aktivieren
- Externe Weiterleitungen blockieren
- Sharing-Defaults härten
- Audit-Logging und Alerts aktivieren

Stufe 2 – In wenigen Wochen Wochen

- Conditional Access sauber aufbauen
- Admin-Rollen und Ausnahmen bereinigen
- Review der externen Freigaben
- Regelmäßiger Secure Score Review

Stufe 3 – Mit externer Unterstützung

- Tenant Review / Audit
- Rechte- und Rollenreview
- Prüfung von Altlasten und Altprotokollen
- Risikoübersetzung für Geschäftsführung

Die 5 Dinge, die Sie morgen umsetzen

1

MFA wirklich für alle

Nicht „fast alle". Nicht „außer …". Jede Ausnahme ist ein offenes Fenster.

2

Alte Anmeldewege sichtbar machen

Report-only testen, Altpfade abbauen, SMTP AUTH hinterfragen.

3

Externes Teilen bewusst steuern

Default intern, offene Links begrenzen, Ablaufdaten setzen, Audit aktiv nutzen.

4

Weiterleitungen überwachen

Alerts aktivieren, externe Auto-Forwarding-Regeln standardmäßig unterbinden.

5

Secure Score als Startpunkt

Score lesen, Trends beobachten – aber echte Risiken zusätzlich prüfen.

Fragen und Antworten

Jetzt ist der richtige Zeitpunkt

> „Wenn Sie sich heute bei ein oder zwei Punkten wiedererkannt haben, dann ist das keine schlechte Nachricht.
> Es heißt nur: Jetzt ist der richtige Zeitpunkt, Ihre Microsoft-365-Umgebung bewusst sicherer zu machen."

Was solbytech für Sie tut

solbytech hilft Unternehmen, Microsoft 365 nicht nur zu nutzen — sondern zu verstehen, richtig zu entscheiden und nachhaltig sicher zu betreiben.

Nächster Schritt

Sprechen Sie uns an. Ein kostenfreies Erstgespräch zeigt Ihnen, wo Ihr Tenant heute wirklich steht.

www.eday-salzburg.at/download

Danke

17.03.2026

WKS Unternehmensberatung · Buchhaltung · IT