Entra Diagnostiker: Sicherheitsanalyse für Microsoft Entra ID

Dein Entra-ID-Tenant ist über Jahre gewachsen, und mit ihm die globalen Admins, die Ausnahmen im Conditional Access und die App-Registrierungen, die keiner mehr zuordnen kann. Der Entra Diagnostiker liest den Tenant ausschließlich lesend aus, prüft ihn in 14 Analysemodulen und liefert dir einen priorisierten Bericht mit konkretem Aktionsplan.

Der Tenant, den keiner mehr ganz überblickt

Montagmorgen, IT-Runde. Die Frage des neuen CISO ist harmlos formuliert: „Wie viele globale Administratoren haben wir eigentlich?“ Der Administrator schaut ins Portal und sagt „sieben“. Dann fällt ihm das Dienstkonto für die alte Synchronisation ein. Und der externe Dienstleister von damals. Und das Konto, das beim letzten Notfall angelegt und nie wieder gelöscht wurde. Am Ende sind es elf, zwei davon ohne MFA, und eines hat sich seit Monaten nicht mehr angemeldet.

Das ist kein Versagen der IT. Das ist der ganz normale Alltag in einem Tenant, der seit Jahren läuft, durch mehrere Projekte, Dienstleister und Notfälle gegangen ist und in dem niemand die Zeit hat, alle Ecken regelmäßig auszuleuchten. Im Entra Admin Center steht zwar alles irgendwo, aber verteilt auf zwei Dutzend Blätter, Filter und Berichte. Den Zusammenhang musst du dir selbst bauen.

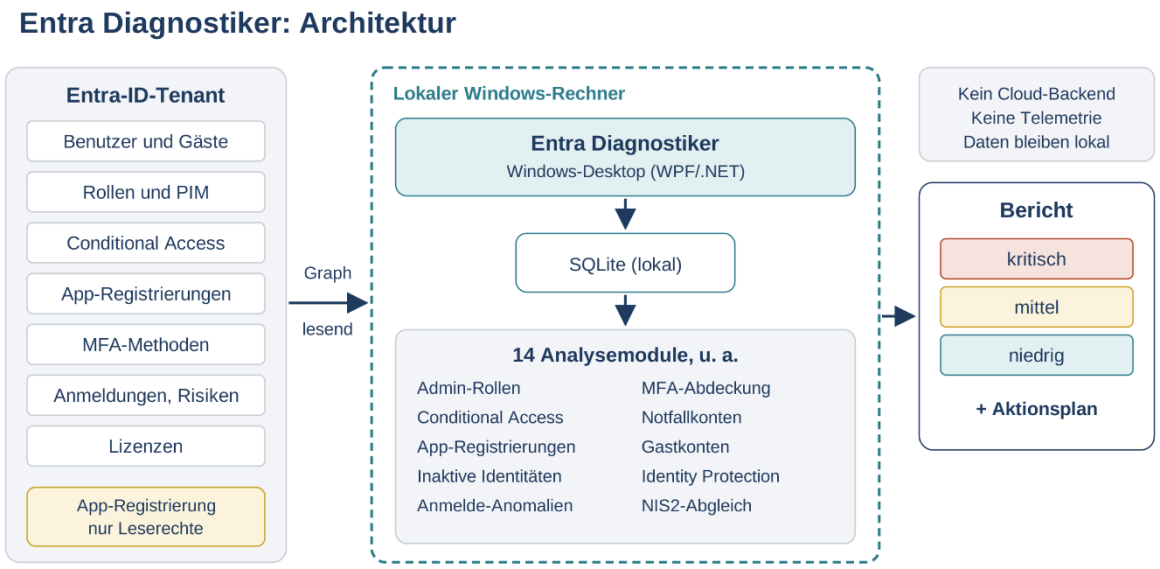
> **Angreifer lesen deinen Tenant gründlicher als du**
> Wer einmal ein Konto in deinem Tenant übernommen hat, schaut sich in aller Ruhe um: Welche Konten kommen an der MFA vorbei, welche App hat zu viele Rechte, welche Ausnahme im Conditional Access ist ein Scheunentor? Die Frage ist nicht, ob jemand diese Analyse macht, sondern ob du sie zuerst machst.

Was der Entra Diagnostiker macht

Der Entra Diagnostiker ist ein Windows-Desktop-Werkzeug (WPF/.NET) aus der Diagnostiker-Familie, eine Eigenentwicklung von boddenberg.de. Er analysiert Microsoft-Entra-ID-Tenants auf Sicherheitsprobleme. Der Zugriff läuft über **Microsoft Graph** mit einer App-Registrierung, die **ausschließlich lesende Berechtigungen** bekommt. Nach der Analyse kannst du diese App-Registrierung sofort wieder entfernen. Damit bleibt keine Hintertür zurück.

Die Daten landen in einer **lokalen SQLite-Datenbank** auf deinem Rechner. Es gibt kein Cloud-Backend und keine Telemetrie. Was der Diagnostiker über deinen Tenant weiß, bleibt bei dir. Aus den gesammelten Daten bewerten 14 Analysemodule die Lage und erzeugen

einen strukturierten Bericht mit Priorisierung nach kritisch, mittel und niedrig sowie einem konkreten Aktionsplan.



Architektur: Eine App-Registrierung mit reinen Leserechten liefert die Tenant-Daten über Microsoft Graph an den Entra Diagnostiker. Die Analyse läuft lokal mit SQLite, ohne Cloud-Backend und ohne Telemetrie, und mündet in einen priorisierten Bericht.

Nur lesen, nichts anfassen

Ein Sicherheits-Assessment, das selbst Schreibrechte im Tenant verlangt, wäre ein schlechter Witz. Der Entra Diagnostiker arbeitet ausschließlich lesend. Das macht ihn auch für Organisationen tauglich, in denen jede neue Berechtigung durch den Änderungsprozess muss: Leserechte sind schnell begründet und nach der Analyse schnell wieder weg.

Die 14 Analysemodule

Die Module decken die Bereiche ab, in denen sich in gewachsenen Tenants erfahrungsgemäß die meisten Probleme sammeln. Einige davon im Detail:

Admin-Rollen-Wildwuchs und PIM

Wie viele globale Administratoren gibt es, und wer ist dauerhaft zugewiesen, statt die Rolle über Privileged Identity Management (PIM) nur bei Bedarf zu aktivieren? Dauerhafte Admin-Rechte sind wie ein Generalschlüssel, der am Schlüsselbrett neben der Eingangstür hängt. Praktisch, bis jemand anderes ihn mitnimmt.

MFA-Abdeckung und Methoden

Nicht nur „hat MFA oder nicht“, sondern auch welche Methoden im Einsatz sind. Gerade für Administratoren zählt, ob sie phishingresistente MFA verwenden. Eine SMS als zweiter

Faktor für ein Konto mit globalen Rechten ist ungefähr so beruhigend wie ein Fahrradschloss am Tresor.

Conditional Access

Hier prüft der Diagnostiker Vollständigkeit und Konsistenz der Richtlinien, sucht gefährliche Ausnahmen und findet Konten, die an allen Richtlinien vorbeikommen. Das sind die Befunde, bei denen in Workshops typischerweise ein kurzes Schweigen eintritt.

Notfallkonten, Apps und Gäste

Gibt es Notfallkonten (Break Glass), und sind sie sinnvoll eingerichtet? Welche App-Registrierungen sind überprivilegiert, welche verwaist, wo laufen Secrets demnächst ab? Wie sieht es bei Gastkonten und der externen Zusammenarbeit aus? Gerade App-Registrierungen sind ein beliebtes Versteck für Rechte, an die sich niemand mehr erinnert.

Inaktive Identitäten und Anmelde-Anomalien

Konten, die seit Monaten niemand benutzt, sind für Angreifer besonders attraktiv: Wenn dort jemand Fremdes einsteigt, fällt es keinem auf, weil sowieso keiner hinschaut. Der Diagnostiker listet inaktive Identitäten auf und wertet Anmelde-Anomalien und Risikosignale aus. Dazu gehört auch die Frage, ob irgendwo noch Legacy-Authentifizierung verwendet wird. Alte Protokolle ohne moderne Anmeldung sind die Hintertür, durch die MFA elegant umgangen wird, und sie stecken erstaunlich oft noch in einem Multifunktionsdrucker oder einer vergessenen Skriptlösung.

Identity Protection, Lizenzen und NIS2

Die übrigen Module schauen auf Identity Protection, also den Umgang mit riskanten Anmeldungen und Benutzern, auf die Lizenz-Auslastung und auf den NIS2-Abgleich. Letzterer übersetzt technische Befunde in die Sprache, die Geschäftsführung und Revision verstehen. Der Sinn dahinter: Eine Analyse, die nur Administratoren lesen können, landet selten auf der Tagesordnung, auf der über Budget entschieden wird.

Analysemodul	Typische Fragestellung
Admin-Rollen	Wie viele globale Admins gibt es, wer ist ohne PIM dauerhaft zugewiesen?
MFA-Abdeckung und Methoden	Wer hat keine MFA, nutzen Admins phishingresistente Methoden?
Conditional Access	Sind die Richtlinien vollständig und konsistent, wer kommt an allen vorbei?
Notfallkonten (Break Glass)	Gibt es Notfallkonten und sind sie sauber eingerichtet?
App-Registrierungen	Welche Apps sind überprivilegiert, verwaist oder haben ablaufende Secrets?
Gastkonten und externe Zusammenarbeit	Wer ist als Gast im Tenant und mit welchen Möglichkeiten?

Analysemodul	Typische Fragestellung
Inaktive Identitäten	Welche Konten werden nicht mehr genutzt, existieren aber weiter?
Anmelde-Anomalien und Risikosignale	Wo gibt es Auffälligkeiten, wird noch Legacy-Authentifizierung verwendet?
Privileged Identity Management	Wird PIM genutzt, und wie konsequent?
Identity Protection	Wie ist der Schutz vor riskanten Anmeldungen und Benutzern eingerichtet?
Lizenz-Auslastung	Werden die vorhandenen Lizenzen genutzt?
NIS2-Abgleich	Wie steht der Tenant im Licht der NIS2-Anforderungen da?

Die Tabelle zeigt eine Auswahl der Module; insgesamt sind es 14. Jedes Modul liefert Befunde, die im Bericht nach Schwere eingeordnet werden, damit du nicht mit einer Liste von 200 gleich lauten Warnungen dastehst, sondern weißt, womit du am Montag anfängst. Das ist auch der Unterschied zu einer Checkliste: Eine Checkliste sagt dir, was man prüfen könnte. Der Diagnostiker sagt dir, was er in deinem Tenant gefunden hat und wie dringend es ist.

Entra Diagnostiker auf einen Blick

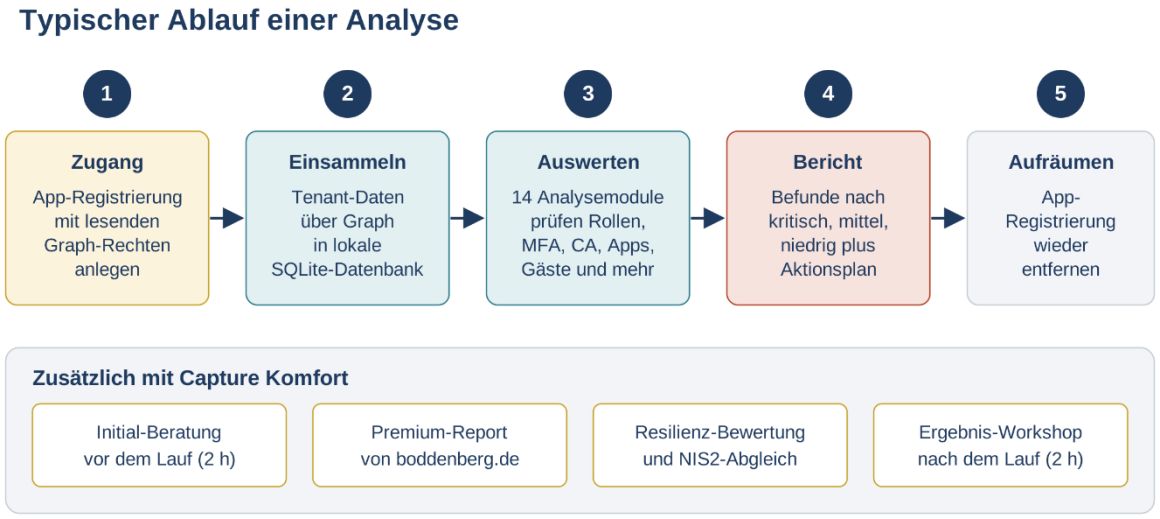
- **Produkttyp:** Sicherheitsanalyse für Microsoft-Entra-ID-Tenants, Diagnostiker-Familie
- **Plattform:** Windows-Desktop-Anwendung (WPF/.NET)
- **Zugriff:** Microsoft Graph über App-Registrierung mit ausschließlich lesenden Berechtigungen, nach der Analyse sofort entfernbar
- **Datenhaltung:** lokal in SQLite, kein Cloud-Backend, keine Telemetrie
- **Umfang:** 14 Analysemodule, Bericht mit Priorisierung kritisch/mittel/niedrig und Aktionsplan
- **Zielgruppe:** Inhouse-IT größerer Mittelständler, Systemhäuser, IT-Prüfer
- **Lizenzmodell:** Capture Basis und Capture Komfort pro Durchlauf, Vollversion als Kauflizenz mit Wartung
- **Hersteller:** Eigenentwicklung von boddenberg.de

Typischer Einsatz: vom Leserecht zum Aktionsplan

Ein Durchlauf folgt immer demselben Muster. Zuerst legst du die App-Registrierung mit den lesenden Graph-Berechtigungen an und erteilst die Zustimmung. Dann startest du den Diagnostiker, der die Daten einsammelt und in seiner lokalen Datenbank ablegt. Die 14 Module werten aus, und am Ende steht der Bericht mit Befunden nach Schwere und dem

Aktionsplan. Zum Schluss entfernst du die App-Registrierung wieder. Kein Agent bleibt zurück, kein Dienst läuft weiter.

Für Capture Komfort kommen eine zweistündige Initial-Beratung vor dem Lauf, ein Premium-Report und ein zweistündiger Ergebnis-Workshop dazu. In dieses Paket gehören auch die **Resilienz-Bewertung gegen Angriffsszenarien** und der **NIS2-Abgleich**. Gerade die Resilienz-Bewertung ist für die Geschäftsführung oft der Teil, der aus technischen Befunden eine nachvollziehbare Risikoeinschätzung macht.



Typischer Ablauf: App-Registrierung mit Leserechten anlegen, Daten einsammeln, in 14 Modulen auswerten, Bericht mit Aktionsplan erhalten und die App-Registrierung wieder entfernen.

> **Nimm den Bericht in deine Risikoplanung mit**
>
> Die Einteilung in kritisch, mittel und niedrig ist bewusst so gewählt, dass sie in Risikoregister und Maßnahmenpläne passt. Kritische Befunde gehören in die nächste Woche, mittlere in das nächste Quartal, niedrige auf die Liste für ruhige Tage, die es in der IT natürlich nie gibt.

Die Vollversion für den Dauereinsatz

Sicherheit ist kein Zustand, den man einmal herstellt und dann abhakt. Neue Apps kommen hinzu, Dienstleister wechseln, Ausnahmen werden „nur kurz“ eingetragen. Die Vollversion ist für Organisationen gedacht, die ihren Tenant regelmäßig prüfen wollen. Sie bietet unter anderem einen **Alarm bei ablaufenden Secrets** von App-Registrierungen und einen **Verlauf über mehrere Läufe**, sodass du siehst, ob sich die Lage verbessert oder ob sich still und leise neue Baustellen eingeschlichen haben.

Ablaufende Secrets sind übrigens einer der Klassiker für unnötige Ausfälle: Eine Schnittstelle läuft jahrelang problemlos, dann ist das Secret abgelaufen, und am Freitagnachmittag steht die Anbindung. Ein Alarm vorher ist deutlich entspannter als die Fehlersuche hinterher.

Für wen der Entra Diagnostiker gedacht ist

Der Entra Diagnostiker richtet sich an drei Gruppen:

- **Inhouse-IT größerer Mittelständler:** Teams, die ihren Tenant selbst betreiben und eine unabhängige, strukturierte Bestandsaufnahme brauchen, ohne gleich ein großes Audit-Projekt aufzusetzen.
- **Systemhäuser:** Dienstleister, die ihren Kunden ein wiederholbares Assessment anbieten wollen, mit gleichbleibender Methodik und vergleichbaren Ergebnissen. Systemhäuser und Partner bekommen eigene Konditionen auf Anfrage.
- **IT-Prüfer:** Prüfer, die eine nachvollziehbare, lesend erhobene Datengrundlage für ihre Bewertung suchen.

Fachlich steht der Diagnostiker auf dem Fundament des Kompetenzbereichs Microsoft Entra ID und des Buchs „Microsoft Entra ID in der Praxis“. Die Befunde ordnen sich in die übergreifende Absicherung ein, die der Kompetenzbereich Microsoft 365 Security beschreibt.

In der Diagnostiker-Familie ist der Entra Diagnostiker der Sicherheitsspezialist. Sein Geschwisterprodukt, der Copilot Diagnostiker, untersucht vor allem Compliance-Aspekte wie Oversharing, Metadaten und Vertraulichkeitsbezeichnungen. Beide ergänzen sich, gerade wenn ein Copilot-Rollout ansteht.

Editionen und Lizenzierung

Den Entra Diagnostiker gibt es in drei Editionen. Alle Preise sind Nettopreise zuzüglich Mehrwertsteuer.

Edition	Leistungsumfang	Preis (netto)
Capture Basis	Nur das Werkzeug für einen Durchlauf; du interpretierst die Ergebnisse selbst	1.000 € pro Durchlauf
Capture Komfort	Werkzeug plus Initial-Beratung (2 Stunden), Premium-Report und Ergebnis-Workshop (2 Stunden); inklusive Resilienz-Bewertung gegen Angriffsszenarien und NIS2-Abgleich	2.000 € pro Durchlauf
Vollversion	Dauereinsatz, u. a. mit Alarm bei ablaufenden Secrets und Verlauf über mehrere Läufe	15.000 € zzgl. Wartung 30 % p. a.

Beratung, Einführung und Schulung

Ein Aktionsplan ist nur so gut wie seine Umsetzung. Wenn du beim Abarbeiten der Befunde Unterstützung möchtest, etwa beim Umbau von Conditional Access, bei der Einführung von PIM, beim Aufräumen von App-Registrierungen oder beim Einrichten von Notfallkonten, begleite ich dich gern. Das kann ein einzelner Workshop sein, eine Schulung für das Admin-Team oder eine längere Begleitung, bis die kritischen Punkte erledigt sind. Rund 30 Jahre

Microsoft-Enterprise-Praxis helfen dabei, zwischen „muss sofort“ und „kann warten“ sauber zu unterscheiden.

Häufige Fragen

Welche Berechtigungen braucht der Entra Diagnostiker?

Ausschließlich lesende Berechtigungen für Microsoft Graph, erteilt über eine App-Registrierung. Schreibrechte braucht und bekommt das Werkzeug nicht.

Bleibt nach der Analyse etwas in meinem Tenant zurück?

Nur die App-Registrierung, und die kannst du direkt nach der Analyse entfernen. Ein Agent oder Dienst im Tenant wird nicht installiert.

Wohin fließen die Daten?

In eine lokale SQLite-Datenbank auf dem Rechner, auf dem der Diagnostiker läuft. Es gibt kein Cloud-Backend und keine Telemetrie.

Was bekomme ich als Ergebnis?

Einen strukturierten Bericht, in dem die Befunde nach kritisch, mittel und niedrig priorisiert sind, und einen konkreten Aktionsplan. Mit Capture Komfort kommen der Premium-Report, die Resilienz-Bewertung gegen Angriffsszenarien, der NIS2-Abgleich und ein Ergebnis-Workshop hinzu.

Hilft mir der Diagnostiker bei NIS2?

Ein NIS2-Abgleich gehört zu den Analysemodulen und ist Bestandteil des Komfort-Pakets. Er ersetzt keine vollständige NIS2-Umsetzung, zeigt dir aber, wo dein Entra-ID-Tenant im Licht der Anforderungen steht.

Kann ein Systemhaus den Diagnostiker für seine Kunden einsetzen?

Ja, Systemhäuser mit einem wiederholbaren Assessment-Service gehören ausdrücklich zur Zielgruppe. Für Partner gibt es eigene Konditionen; frag dazu einfach an.

> **Weiter geht's**
>
> - Kompetenzbereich Microsoft Entra ID: Identitäten, Anmeldung und Zugriff in der Praxis
> - Kompetenzbereich Microsoft 365 Security: den ganzen Tenant absichern
> - Kompetenzbereich Kerberos: Authentifizierung im lokalen Active Directory
> - Copilot Diagnostiker: die Schwester für Compliance und Copilot-Readiness
> - PKI Diagnostiker: Bestandsaufnahme der eigenen Zertifizierungsstelle