cycura

Ihre größten Risiken sehen Sie nicht

Warum die kritischsten Sicherheitslücken in Ihrer Microsoft-365-Umgebung unsichtbar bleiben – und wie Sie sie systematisch aufdecken

cycura

Die unbequeme Wahrheit

Die meisten Sicherheitslücken entstehen nicht im Angriff – sondern lange davor. Sie entwickeln sich schleichend im laufenden Betrieb, bleiben unentdeckt, weil sie in Standard-Dashboards nicht sichtbar sind, und werden erst kritisch, wenn es zu spät ist.

Was das konkret bedeutet:

- → Ihre Security wirkt vollständig – ist es aber technisch oft nicht
- → Ihre Reports zeigen grüne Ampeln – während reale Risiken unentdeckt bleiben
- → Ihre Annahmen über Sicherheit wurden nie unter Realbedingungen validiert
- → Ihre kritischsten Angriffsflächen sind die, die Sie aktuell nicht sehen

DAS PROBLEM

In 90% der von uns analysierten Unternehmen existieren erhebliche Resilienz-Lücken, die im Alltag nicht auffallen. Sie werden nicht systematisch geprüft, weil sie in bestehenden Monitoring-Systemen nicht sichtbar sind.

Was Sie in diesem Guide erwartet

- Die 8 strategischen Blindstellen, die im Alltag nicht auffallen
- Die 5 Risiko-Bereiche, die ohne strukturierte Analyse unentdeckt bleiben
- Ein 15-Punkte-Selbstcheck zur Einschätzung Ihrer tatsächlichen Sicherheitslage

cycura

Die 8 strategischen Blindstellen

Fast jeder CISO, mit dem wir sprechen, kennt mindestens fünf dieser Muster aus dem eigenen Alltag – ohne sie systematisch adressiert zu haben:

1. Die Kommunikations-Lücke

„Unser Incident Response Plan sieht vor, alle Stakeholder zu informieren. Aber niemand hat geprüft, ob die definierten Kanäle auch funktionieren, wenn die primären Systeme nicht verfügbar sind."

WARUM DAS IM ALLTAG NICHT AUFFÄLLT

Die Kanäle funktionieren im Normalbetrieb einwandfrei. Ihre Limitation wird erst im Ernstfall sichtbar – wenn es zu spät ist, sie zu beheben.

2. Der Annahmen-Blindflug

„Wir gehen davon aus, dass unsere Backups funktionieren. Eine systematische Validierung unter Realbedingungen haben wir nie durchgeführt."

WARUM DAS IM ALLTAG NICHT AUFFÄLLT

Technische Backup-Tests laufen erfolgreich. Aber niemand testet, ob die Wiederherstellung unter Zeitdruck und mit unvollständiger Dokumentation funktioniert.

3. Das Identitäts-Paradox

„Wir haben PIM implementiert. Aber niemand hat analysiert, ob die Notfallzugriffe im kritischen Moment tatsächlich verfügbar sind."

WARUM DAS IM ALLTAG NICHT AUFFÄLLT

Die Technologie funktioniert im Regelbetrieb. Die tatsächliche Verfügbarkeit im Stressfall wird nie validiert.

4. Die Dokumentations-Falle

„Unser Notfallhandbuch ist umfangreich. Aber niemand hat gemessen, wie lange es dauert, im Stress die relevanten Informationen zu finden."

WARUM DAS IM ALLTAG NICHT AUFFÄLLT

Die Dokumentation existiert und ist vollständig. Ihre Praxistauglichkeit unter Realbedingungen wurde nie getestet.

cycura

Die 8 strategischen Blindstellen (Fortsetzung)

5. Der Shadow-Access-Schock

„Externe Partner hatten vor zwei Jahren Admin-Rechte. Eine systematische Überprüfung, ob diese noch aktiv sind, findet nicht statt."

WARUM DAS IM ALLTAG NICHT AUFFÄLLT

Die Zugriffe verursachen keine Probleme im Normalbetrieb. Ihre Existenz wird nicht durch Standard-Monitoring erkannt.

6. Die Hybrid-Kaskade

„Die kritischen Übergänge zwischen Cloud und On-Premises wurden nie für Incident-Szenarien dokumentiert. Die Abhängigkeiten sind nicht transparent."

WARUM DAS IM ALLTAG NICHT AUFFÄLLT

Alle Systeme laufen stabil. Die kaskadierenden Auswirkungen eines Ausfalls wurden nie analysiert.

7. Das Tool-Monopol

„Unsere Detection läuft auf Azure Sentinel. Die Abhängigkeit des Monitorings von der überwachten Infrastruktur wurde nie als Risiko betrachtet."

WARUM DAS IM ALLTAG NICHT AUFFÄLLT

Das Monitoring funktioniert einwandfrei. Seine eigene Verwundbarkeit wird nicht systematisch analysiert.

8. Das Eskalations-Vakuum

„Die Person, die um 3 Uhr nachts entscheiden muss, ist nicht definiert. Die Entscheidungsstrukturen für den Ernstfall existieren nicht."

WARUM DAS IM ALLTAG NICHT AUFFÄLLT

Im Normalbetrieb gibt es klare Zuständigkeiten. Die Notfall-Governance wurde nie etabliert.

Das gemeinsame Muster: Diese Lücken entstehen schleichend im Betrieb. Sie werden nicht durch Standard-Tools erkannt. Sie bleiben unentdeckt, solange sie nicht **gezielt analysiert** werden.

cycura

Das Problem: Sichtbare Security, unsichtbare Risiken

Die meisten Unternehmen haben Microsoft 365 Security implementiert – aber nicht die Transparenz über ihre tatsächlichen Risiken. Das Ergebnis: Ein falsches Sicherheitsgefühl, das durch grüne Dashboards verstärkt wird.

Ebene 1: Fehlende Transparenz

Microsoft 365 liefert Schutzmechanismen, aber keinen Überblick über deren Wirksamkeit unter Realbedingungen. Conditional Access, MFA, PIM – alles ist konfiguriert, aber niemand weiß, ob es im Ernstfall funktioniert.

Ebene 2: Fehlende Analyse

Selbst wo Konfigurationen existieren, fehlt die Analyse von kaskadierenden Abhängigkeiten und realen Angriffspfaden. Wer hat wann Zugriff auf was? Welche externen Identitäten sind aktiv? Diese Fragen werden nicht systematisch beantwortet.

Ebene 3: Fehlende Validierung

Security wird als kontinuierlicher Prozess betrieben, aber die Annahmen über seine Wirksamkeit werden nie validiert. Ohne strukturierte Analyse bleiben kritische Lücken bestehen – unsichtbar, bis sie ausgenutzt werden.

cycura

1

Fehlende Notfall-Kommunikationsanalyse

HÄUFIGKEIT: 90% DER TENANTS | WIRD NICHT SYSTEMATISCH GEPRÜFT

Incident Response Pläne definieren Kommunikationskanäle, aber ihre Funktionsfähigkeit unter realen Bedingungen wird nicht analysiert. Die Annahme, dass definierte Kanäle auch funktionieren, bleibt unvalidiert.

DAS KONKRETE RISIKO

Sie merken erst im Ernstfall, dass Ihre definierten Kommunikationswege nicht funktionieren – wenn es zu spät ist, Alternativen aufzubauen.

WARUM DAS IN STANDARD-REPORTS NICHT SICHTBAR IST

Monitoring-Systeme prüfen die Verfügbarkeit von Diensten, nicht die Funktionsfähigkeit von Notfallprozessen. Die Lücke zwischen „definiert" und „funktioniert" wird nicht gemessen.

WAS WIR IN ASSESSMENTS FINDEN

- Keine Analyse der Kanal-Abhängigkeiten von primären Systemen
- Keine Validierung der Erreichbarkeit unter Stressbedingungen
- Keine Dokumentation alternativer Kommunikationspfade
- Notfallkontakte nur in Systemen hinterlegt, die selbst betroffen sind

Wurde die Funktionsfähigkeit Ihrer Notfallkommunikation systematisch analysiert?
www.cycura.de/termin

cycura

2

Nicht validierte Wiederherstellungsfähigkeit

HÄUFIGKEIT: 85% | WIRD NICHT SYSTEMATISCH GEPRÜFT

Backups und Wiederherstellungspläne existieren, aber ihre Praxistauglichkeit unter Realbedingungen wurde nie analysiert. Technische Tests bestätigen die Funktionalität – nicht die Anwendbarkeit im Stressfall.

DAS RISIKO

Sie merken erst im Ernstfall, dass die Wiederherstellung länger dauert als erwartet, kritische Abhängigkeiten nicht dokumentiert sind oder niemand das Notfallpasswort findet.

WARUM DAS IN STANDARD-REPORTS NICHT SICHTBAR IST

Backup-Reports zeigen erfolgreiche Jobs, nicht die tatsächliche Wiederherstellungszeit unter Stress. Die Diskrepanz zwischen technischer und prozessualer Funktionsfähigkeit bleibt unentdeckt.

TYPISCHE ERKENNTNISSE AUS ANALYSEN

- Das Break-Glass-Passwort existiert, aber niemand weiß, wo es physisch lagert
- Die Wiederherstellung dauert 10x länger als dokumentiert
- Kritische Abhängigkeiten zwischen Systemen wurden nie analysiert
- Das Team kennt die Priorisierung für Notfall-Wiederherstellungen nicht

Wurde Ihre Wiederherstellung unter Realbedingungen systematisch validiert? www.cycura.de/termin

cycura

3

Undokumentierte kritische Abhängigkeiten

HÄUFIGKEIT: 80% | WIRD NICHT SYSTEMATISCH GEPRÜFT

Hybrid-Umgebungen (Cloud ↔ On-Premises) mit nicht analysierten Übergängen. Die Abhängigkeiten zwischen Systemen wurden nie systematisch erfasst und für Ausfallszenarien bewertet.

DAS RISIKO

Sie merken erst im Ernstfall, dass der Ausfall eines scheinbar sekundären Dienstes kaskadierende Effekte hat – weil niemand die Abhängigkeiten analysiert hat.

WARUM DAS IN STANDARD-REPORTS NICHT SICHTBAR IST

System-Monitoring zeigt individuelle Status, nicht kaskadierende Abhängigkeiten. Die Architektur-Analyse für Resilienz-Szenarien wird nicht durch Standard-Tools abgedeckt.

WAS WIR IN ASSESSMENTS FINDEN

- Keine systematische Dokumentation kritischer Übergänge zwischen Cloud und On-Prem
- Keine Analyse von Single-Points-of-Failure in der Architektur
- Unklare Abhängigkeiten zwischen Identitäts-Systemen
- Fehlende Resilienz-Architektur-Dokumentation

Wurden die kritischen Abhängigkeiten in Ihrer Hybrid-Umgebung systematisch analysiert?
www.cycura.de/termin

cycura

4

Nicht analysierte privilegierte Identitäten

HÄUFIGKEIT: 95% | WIRD NICHT SYSTEMATISCH GEPRÜFT

Externe Partner, Dienstleister oder ehemalige Mitarbeiter mit dauerhaften Zugriffen, die nie systematisch analysiert wurden. Die vollständige Übersicht über alle Identitäten mit kritischem Zugriff fehlt.

DAS RISIKO

Sie merken erst im Ernstfall, dass vergessene Gastkonten oder Service Principals mit weitreichenden Berechtigungen existieren – wenn sie ausgenutzt werden.

WARUM DAS IN STANDARD-REPORTS NICHT SICHTBAR IST

Standard-Monitoring fokussiert auf aktive Nutzung, nicht auf potenzielle Risiken inaktiver oder vergessener Identitäten. Die systematische Analyse aller Identitäten mit kritischem Zugriff wird nicht durchgeführt.

TYPISCHE FUNDE IN ANALYSEN

- Gastkonten von Partnern, die seit Monaten nicht genutzt, aber nie deaktiviert wurden
- Service Principals mit weitreichenden Berechtigungen, deren Zweck niemand mehr kennt
- Externe Berater mit Admin-Rechten, die nie systematisch reviewed wurden
- Kein regelmäßiger Analyse-Prozess für externe Identitäten

Haben Sie eine vollständige Übersicht über alle Identitäten mit kritischem Zugriff? www.cycura.de/termin

cycura

5

Nicht analysierte Entscheidungsstrukturen

HÄUFIGKEIT: 70% | WIRD NICHT SYSTEMATISCH GEPRÜFT

Eskalationswege und Entscheidungsbefugnisse sind definiert, aber ihre Anwendbarkeit unter Realbedingungen wurde nie analysiert. Wer entscheidet, wenn die definierten Personen nicht erreichbar sind?

DAS RISIKO

Sie merken erst im Ernstfall, dass die definierten Entscheidungsstrukturen nicht funktionieren – wenn klare Verantwortlichkeiten kritisch sind.

WARUM DAS IN STANDARD-REPORTS NICHT SICHTBAR IST

Organisations-Dokumentation zeigt formale Strukturen, nicht ihre Wirksamkeit unter Stress. Die Analyse von Notfall-Governance wird nicht durch technische Tools abgedeckt.

WAS WIR IN ASSESSMENTS FINDEN

- Definierte Entscheidungsbefugnisse, aber keine Analyse ihrer Verfügbarkeit im Ernstfall
- Eskalationswege dokumentiert, aber nicht auf Anwendbarkeit unter Stress geprüft
- Keine alternativen Kommunikationsketten für außerhalb der Geschäftszeiten
- Fehlende Analyse von Vollmachten für kritische Notfallmaßnahmen

Wurden Ihre Entscheidungsstrukturen unter Realbedingungen systematisch analysiert?
www.cycura.de/termin

cycura

Die Lösung: Systematische Risikoanalyse

Preventive Services sind keine Notfalllösung. Sie sind eine strukturierte Methodik, um die Risiken zu identifizieren, die im Alltag unsichtbar bleiben – bevor sie kritisch werden.

Was systematische Analyse auszeichnet

- **Transparenz:** Vollständige Übersicht über reale Angriffsflächen und kaskadierende Abhängigkeiten
- **Validierung:** Überprüfung der Annahmen über Sicherheit unter Realbedingungen
- **Prävention:** Reduktion von Eintrittswahrscheinlichkeit und Ausbreitung durch strukturierte Maßnahmen

Das 5-Phasen Analyse-Framework

- **1. Discovery & Risikoanalyse** – Systematische Identifikation realer Angriffsflächen und unsichtbarer Risiken
- **2. Abhängigkeitsanalyse** – Erfassung kritischer Übergänge und kaskadierender Effekte
- **3. Validierung unter Realbedingungen** – Überprüfung der Funktionsfähigkeit von Prozessen und Strukturen
- **4. Risikoreduktion** – Strukturierte Maßnahmen zur Reduktion identifizierter Risiken
- **5. Kontinuierliche Überwachung** – Etablierung von Prozessen zur fortlaufenden Risikoanalyse

Das Ergebnis: Ein Unternehmen mit transparenter Sicherheitslage – das seine tatsächlichen Risiken kennt und systematisch adressiert.

cycura

Was systematische Analyse NICHT ist

Kein Pentest

Wir finden keine neuen Lücken durch aktive Angriffe. Wir analysieren die bekannten Konfigurationen und identifizieren die Risiken, die daraus entstehen.

Kein Big-Bang-Projekt

Entsteht schrittweise. Jede Phase liefert messbare Erkenntnisse über Ihre tatsächliche Risikolage. Erste Transparenz oft innerhalb von Wochen erreichbar.

Keine Tool-Beratung

Wir ersetzen nicht Ihre Security-Landschaft. Wir maximieren den Wert Ihrer bestehenden Investition durch systematische Analyse und Optimierung.

Kein SOC/MSSP

Kein dauerhaftes Monitoring oder operativer Betrieb. Wir schaffen Transparenz über Ihre Risiken – die Grundlage für gezielte Verbesserung.

Was systematische Analyse WIRKLICH ist:

- Ein Prozess: Kontinuierliche Transparenz über Ihre tatsächliche Sicherheitslage
- Ein Ergebnis: Nachweisbare Risikoreduktion, die Sie Management und Auditoren zeigen können
- Eine Grundlage: Faktenbasierte Entscheidungen über Security-Investitionen

cycura

Der Transparenz-Reifegrad-Check

Wo steht Ihr Unternehmen? Die meisten befinden sich auf Stufe 2 oder 3 – mit erheblichem Potenzial für mehr Transparenz.

Reifegrad	Beschreibung	Typische Merkmale
1 Ad-hoc	Keine systematische Risikoanalyse	Security basiert auf Annahmen, keine strukturierte Überprüfung
2 Definiert	Grundlegende Prozesse existieren, aber nicht analysiert	Dokumentation vorhanden, aber Wirksamkeit nicht validiert
3 Geführt	Systematisch implementiert, aber ohne kontinuierliche Analyse	Tools funktionieren, aber reale Risiken bleiben unentdeckt
4 Analysierend	Kontinuierliche Risikoanalyse mit klaren Metriken	Regelmäßige Validierung; Transparenz über tatsächliche Risiken
5 Optimierend	Systematische Risikoreduktion als kontinuierlicher Prozess	Proaktive Identifikation neuer Risiken; faktenbasierte Entscheidungen

Die gute Nachricht: Der Sprung von „definiert" zu „analysierend" ist der wichtigste – und mit gezielten Maßnahmen innerhalb von 3-6 Monaten erreichbar. Hier entsteht die echte Transparenz über Ihre Risiken.

Wo steht Ihr Unternehmen auf dieser Skala? Wir bewerten Ihre Transparenz und erstellen einen priorisierten Analyseplan. **www.cycura.de/termin**

cycura

Der 15-Punkte Transparenz-Check

Beantworten Sie die folgenden Fragen mit Ja oder Nein. Jedes „Nein" deutet auf einen Bereich hin, der systematisch analysiert werden sollte.

Transparenz & Risikoanalyse

1. **Vollständige Identitätsübersicht** – Wissen Sie jederzeit, welche Identitäten aktuell Zugriff auf kritische Ressourcen haben – inklusive externer und vergessener Konten?
2. **Validierte Notfallprozesse** – Wurden Ihre Notfallprozesse unter Realbedingungen auf Funktionsfähigkeit geprüft?
3. **Getestete Wiederherstellung** – Wurden Ihre Backup- und Wiederherstellungsprozesse unter Zeitdruck und unvollständiger Information validiert?
4. **Analysierte Entscheidungsstrukturen** – Wurden Ihre Eskalationswege auf Anwendbarkeit unter Stressbedingungen analysiert?
5. **Dokumentierte kritische Abhängigkeiten** – Können Sie alle kritischen Übergänge zwischen Cloud und On-Premises systematisch dokumentieren?
6. **Analysierte externe Zugriffe** – Werden externe Zugriffe systematisch auf Aktualität und Notwendigkeit analysiert?
7. **Validierte Notfallzugriffe** – Wurden Ihre Break-Glass-Konzepte unter Realbedingungen auf Funktionsfähigkeit geprüft?

Governance & Technische Transparenz

8. **Nachweisbare Risikoreduktion** – Können Sie Ihrem Management nachweisen, wie sich Ihre Risikolage in den letzten 12 Monaten entwickelt hat?
9. **Analysierte Governance** – Wurden Ihre Notfall-Governance-Strukturen auf Praxistauglichkeit analysiert?
10. **Angriffserkennung** – Würden Sie einen gezielten Angriff auf Ihre Identitätsinfrastruktur erkennen, auch wenn Ihre primären Logs beeinträchtigt sind?

cycura

Der 15-Punkte Transparenz-Check (Fortsetzung)

11. **Unabhängige Überwachung** – Sind Ihre Monitoring-Systeme unabhängig von den überwachten Systemen analysiert und validiert?
12. **Redundanzanalyse** – Existieren für geschäftskritische Prozesse analysierte Alternativen, wenn primäre Dienste nicht verfügbar sind?
13. **Rollenklarheit** – Wissen alle Beteiligten, wer für welche Entscheidung zuständig ist – auch unter Stressbedingungen?
14. **Externe Kommunikationsfähigkeit** – Können Sie Kunden und Partner auch dann erreichen, wenn primäre Kommunikationskanäle beeinträchtigt sind?
15. **Validierte Annahmen** – Wurden Ihre Annahmen über Sicherheit und Verfügbarkeit in den letzten 6 Monaten systematisch validiert?

Auswertung

Nein-Antworten	Transparenzstufe	Empfohlene Aktion
0-2	Hoch	Kontinuierliche Analyse, regelmäßige Validierung
3-5	Mittel	Prioritären Bereiche identifizieren und analysieren
6-9	Niedrig	Systematische Risikoanalyse empfohlen
10-15	Kritisch	Umfassende Transparenz-Analyse dringend empfohlen

Unsicher bei der Auswertung? Wir analysieren Ihre Antworten und erstellen einen priorisierten Analyseplan – unverbindlich. **www.cycura.de/termin**

cycura GmbH

Ihr Spezialist für Microsoft-Security
E-Mail: info@cycura.de | Web: www.cycura.de
Handelsregister: Amtsgericht Göttingen HRB 206706 | USt-IdNr.: DE354593485

Finden Sie heraus, wo Ihre Umgebung heute angreifbar ist

Systematische Analyse. Transparente Risiken. Faktenbasierte Entscheidungen.

www.cycura.de/termin