cycura

Measurably Secure in Microsoft 365

The 10 most critical M365 misconfigurations – and how to systematically eliminate them

The 10 Most Critical M365 Misconfigurations

Microsoft 365 provides powerful security features – but most organizations only use a fraction of them. The result: preventable vulnerabilities that attackers exploit systematically.

What you can expect from this guide

- The 5 most common configuration gaps found in 90% of tenants
- Concrete risks and attack scenarios for each misconfiguration
- Step-by-step instructions for verification in your tenant
- Our proven approach to systematic remediation
- A 15-point risk check for your current security posture

The Good News

Most of these misconfigurations can be fixed within days – not months. The key is knowing where to look and prioritizing correctly.

The Problem: Security Without Measurability

Most organizations have implemented Microsoft 365 Security – but not completely, not systematically, and not measurably. The result: A false sense of security that quickly crumbles upon closer inspection.

The Three Levels of the Problem

1 Level: Missing Configuration

Microsoft 365 provides the tools, but not the finished security. Conditional Access rules, DLP policies, PIM configurations – all of this must be carefully set up. In practice, most tenants are only 30-40% configured.

- MFA is activated, but with too many exceptions
- Conditional Access exists, but doesn't cover all scenarios
- DLP policies are present, but not adapted to your own data classifications

2 Level: Missing Transparency

Even where configurations exist, there's no overview of their effectiveness. Who has access to what, when? How many exceptions are there? Are the policies still current?

- No central overview of all security configurations
- No regular review of exceptions and permissions
- No metrics for measuring security effectiveness

3 Level: Missing Governance

Security is not a one-time project, but a continuous process. Without clear responsibilities, regular reviews, and established processes, every tenant drifts apart over time.

- No defined process for security reviews
- No clear escalation paths for incidents
- No regular employee training

> *"We thought we were secure because we have E5. The truth was: We had a sense of security, but not security."*
>
> — IT Manager, Insurance Group

5 Configuration Gaps That Exist in 90% of Tenants

1 Hundreds of App Registrations with Highly Privileged Graph API Permissions

Criticality: High | Frequency: 90% of tenants

The Gap

By default, users are allowed to create App Registrations in Entra ID. Each app can request Microsoft Graph permissions – and if an admin grants consent once, the app has permanent access.

The Concrete Risk

A Service Principal with Directory.ReadWrite.All can manipulate the entire Directory: create users, change groups, assign admin roles. A Service Principal with User.ReadWrite.All can modify all user accounts in the tenant.

What we find in assessments

- Several hundred App Registrations per Enterprise tenant
- 60-70% of them with unclear business case or forgotten owner
- Service Principals with Directory.ReadWrite.All, User.ReadWrite.All, Group.ReadWrite.All
- Service Principals with Mail.Read.All, Calendars.ReadWrite, Files.Read.All
- No documented justification for these permissions

Azure AD Path for Verification

```
Entra ID > App registrations > All applications
Filter by: Microsoft Graph API Permissions
```

Our Approach

- Inventory of all Service Principals with Directory-Write, User-Write, or Mailbox access
- Implementation of App Consent Policies with Publisher Verification
- Removal of unnecessary permissions

⚠️ **There are two types of Microsoft Graph Permissions:**

Delegated Permissions
→ act in the context of a user
→ risk corresponds to the user's rights

Application Permissions (critical)
→ run without user context
→ often have permanent, unmonitored access

2 Client Secrets Without Rotation for Highly Privileged Service Principals

Criticality: Critical | Frequency: 85% of tenants

The Gap

Service Principals with critical permissions (e.g., Directory.ReadWrite.All) often use Client Secrets that are never rotated. When a Secret is compromised, the attacker has permanent access to the entire Directory – without a user account, without MFA.

The Concrete Risk

A Service Principal with Directory.ReadWrite.All and a Secret unchanged for 3 years. The Secret leaks (GitHub, Phishing). The attacker can now: create users, assign admin roles, establish backdoors – all as a "legitimate" app.

What we find in assessments

- Service Principals with Directory.ReadWrite.All and Secrets older than 2 years
- No central overview of which apps use which Secrets
- No documented justification for Directory-Write permissions

Azure AD Path for Verification

```
Entra ID > App registrations > [App] > Certificates & secrets
Check the creation date of all Secrets
```

Our Approach

- Automated inventory of all Secrets with age analysis
- Introduction of rotation policies (max. 180 days) for all Service Principals with Directory- or User-Write permissions

Attacks via compromised Client Secrets **bypass classic protection mechanisms** like MFA, Conditional Access, and User Risk Policies completely, as they are not tied to a user context.

Many **security concepts simply don't work** here.

3 Conditional Access Gaps in Azure Management and Device Code Flow

Criticality: High | Frequency: 80% of tenants

The Gap

Many tenants have Conditional Access rules that only cover Office 365, but not Azure Management. Additionally, Device Code Flow (used by Microsoft Graph PowerShell) is often not restricted. A token issued via Device Code Flow can persist for a long time if not actively revoked.

The Concrete Risk

An attacker compromises user credentials and successfully authenticates once via Device Code Flow. MFA is correctly requested. The resulting Access Token is only valid for a short time, but the attacker also receives a Refresh Token, which can be used to request new tokens. As long as this is not actively revoked, the attacker can continue to access Microsoft Graph – also without renewed MFA request. If Conditional Access does not explicitly secure Microsoft Graph or Azure Management, this access often remains undetected.

What we find in assessments

- CA rules don't cover Azure Portal/Azure CLI
- No session limits for Graph PowerShell
- Device Code Flow is allowed for all users

Azure AD Path for Verification

```
Entra ID > Security > Conditional Access > Policies
Check if "Microsoft Azure Management" and "Microsoft Graph PowerShell" are covered
```

Our Approach

- CA rules for Microsoft Azure Management and Microsoft Graph PowerShell with short session lifetimes (max. 4 hours)
- Blocking or restriction of Device Code Flow to specific admin groups

An attacker only needs one successful MFA login via Device Code Flow.

After that, they can access Microsoft Graph via tokens without renewed MFA, without visible login in the classic sense. Many companies don't see these accesses as "active sessions".

4 Inactive B2B Guest Accounts with Existing Access

Criticality: Medium-High | Frequency: 95% of tenants

The Gap

Every invitation to Teams, SharePoint, or Power Platform creates a B2B guest account in Entra ID. These accounts are rarely systematically reviewed. A guest account remains active even when the business relationship has ended.

The Concrete Risk

A guest account with access to confidential SharePoint sites. The external company is taken over or hacked. The new owner gains access to all documents and chat histories.

What we find in assessments

- Average of 340 guest accounts per tenant
- 60% of them inactive for over 90 days
- No automated cleanup

Azure AD Path for Verification

```
Entra ID > Users > Guest users
Sort by "Last sign-in" and check inactive accounts
```

Our Approach

- Access Reviews for all guest accounts with inactivity > 30 days
- Blocking of "Email One-Time Passcode"
- Enforcement of MFA for all B2B access

You protect your network but simultaneously trust unknown external identities with access to your data?

www.cycura.de/termin

5 PIM Without Approval Workflows and Time Limits

Criticality: High | Frequency: 70% of tenants

The Gap

Privileged Identity Management (PIM) is activated, but without Approval Workflows and with activation times that are too long (often 8 hours or more).

The Concrete Risk

A compromised admin account activates PIM roles itself. The attacker has 8 hours to establish persistence mechanisms.

What we find in assessments

- No approvers defined for "Tier 0" roles
- Activation times of 8 hours or more
- No alerts for unusual activations

Azure AD Path for Verification

```
Entra ID > Identity Governance > Privileged Identity Management > Azure AD roles
Check the settings for each critical role
```

Our Approach

- Enforcement of Approval Workflows for all critical roles
- Reduction of activation time to maximum 4 hours
- Alerts for unusual activation patterns

Is your PIM configured correctly?

We review your PIM settings and identify vulnerabilities.

www.cycura.de/termin

The Solution: The Secure Tenant

The Secure Tenant is not a product you can buy. It is a state – achieved through systematic configuration, continuous monitoring, and clear governance of your Microsoft 365 tenant.

What distinguishes a Secure Tenant

Configuration: All security features systematically activated. Conditional Access covers all access scenarios. MFA without uncontrolled exceptions. DLP aligned with your own data classes.

Transparency: Central dashboard of all security metrics. Regular reports for management. Clear KPIs for security effectiveness. Demonstrable compliance position.

The Secure Tenant Framework

Our proven 5-phase approach leads you from the current state to the Secure Tenant:

1 Discovery & Assessment

Complete analysis of your current tenant: configuration, licenses, exceptions, vulnerabilities. Result: A detailed report with concrete recommendations and prioritization.

2 Quick Wins & Stabilization

Implementation of critical configurations with immediate effect: close MFA gaps, remove excessive admin rights, establish basic Conditional Access.

3 Deep Configuration

Complete implementation of all security features: granular Conditional Access, DLP for data classes, PIM for privileged accounts, SIEM integration...

4 Monitoring & Reporting

Building continuous transparency: security dashboard, regular reports, alerting on critical events, metrics for measuring security effectiveness.

5 Governance & Continuous Improvement

Establishment of sustainable processes: regular reviews, clear responsibilities, training concept, adaptation to new threats and features.

What the Secure Tenant Is NOT

Before we go into details, let's clear up misunderstandings. The Secure Tenant is not software you buy, and not a one-time project that is ever "finished".

Not a Tool Change

We don't replace your existing security landscape. The Secure Tenant maximizes the value of your Microsoft 365 investment.

Not a Big-Bang Project

The Secure Tenant develops gradually. Each phase delivers measurable improvements. You don't have to wait for months until "everything is finished" – the first successes often show within weeks.

Not a One-Size-Fits-All Solution

Every tenant is different. Industry, company size, compliance requirements, existing infrastructure – all of this influences the optimal configuration. Our framework is adaptable, not rigid.

What the Secure Tenant REALLY is

- **A State:** Fully configured, monitored, and governed Microsoft 365 tenant
- **A Process:** Continuous improvement instead of one-time installation
- **A Framework:** Proven methodology, adapted to your specific situation
- **An Outcome:** Measurable security that you can demonstrate to management and auditors

The Secure Tenant Maturity Check

Where does your company currently stand? This assessment helps you understand your starting point and plan the next steps.

Maturity Level	Description	Typical Characteristics
Level 1 Ad-hoc	Security is operated reactively, no systematic configuration	Security is based on individual measures and assumptions, there is no transparency about who has access to what and what is actually happening.
Level 2 Defined	Basic security features are activated, but incomplete	Security functions are present, but inconsistently implemented, with blind spots in identities, apps, and access paths.
Level 3 Managed	Security is systematically implemented, but without continuous monitoring	Security is broadly implemented, but control is lacking in detail especially for tokens, privileged access, and external identities.
Level 4 Optimizing	Continuous improvement with clear metrics and governance	Security is measurable and controllable, all accesses, identities, and applications are transparent and actively monitored.
Level 5 Excellent	Security as a differentiating competitive advantage, complete transparency	Security is fully integrated and risk-based controlled attacks are proactively detected and automatically limited.

The Good News

Most companies are at Level 2 or 3 – and can reach Level 4 within 3-6 months with targeted measures. The jump from "managed" to "optimizing" is the most important, because this is where the transparency that convinces management and auditors is created.

Where do you stand?

Answer these questions honestly:

- Can you always say who currently has access to your most critical data, internally and externally?
- Do you know which identities or applications have access without a user logging in?
- Can you trace within minutes why a user or an app received access?
- Would you detect unauthorized access immediately or only in retrospect?
- Can you show an auditor or management at the push of a button what your current security status looks like?

The 15-Point Risk Check

Answer the following questions with Yes or No. Each "No" is a potential risk.

Category: Identity & Access

1. Transparency about all identities

Do you always know which identities (users, guests, apps) currently have access to critical resources – and why?

2. Consistent protection of all access paths

Are all access paths (incl. Azure, APIs, CLI, Service Principals) consistently secured – without blind spots?

3. Justification of privileged permissions

Can you technically justify and defend every privileged permission at any time?

4. Time-limited privileged access

Is privileged access time-limited, traceable, and actively monitored – or de facto permanent?

5. Systematic review of external access

Are external accesses systematically reviewed and revoked as soon as they are no longer needed?

Category: Data & Compliance

6. Transparency about sensitive data

Do you specifically know where your sensitive data is located and who currently has access to it?

7. Context-dependent data access control

Is access to sensitive data controlled context-dependently – or only statically permitted?

8. Demonstrable retention periods

Can you always demonstrate how long data is stored and why?

9. Fast data provision

Are you able to provide all relevant data for an audit or incident within hours?

More than 3x "No"?

Your tenant has significant risks. We help you systematically eliminate them.

The 15-Point Risk Check (Continued)

Category: Threat Protection

10. Real-time attack detection

Would you detect a targeted attack on identities or tokens in real time – or only analyze it in retrospect?

11. Transparency about data access

Do you have transparency about which applications and services access your data – also without user context?

12. Active handling of security events

Are security-relevant events prioritized, correlated, and actively processed – or just collected?

Category: Governance & Monitoring

13. Central overview of security posture

Do you have a current, central overview of your security posture – or multiple unconnected individual views?

14. Demonstrable security improvement

Can you show your management at any time whether your security level has actually improved?

15. Clear security decision processes

Are security decisions and exceptions clearly regulated and verifiable – or grown historically?

Assessment

No Answers	Risk Level	Recommended Action
0-2	Low	Continuous improvement, expand monitoring
3-5	Medium	Implement quick wins, set priorities
6-9	High	Immediate action required, consult experts
10-15	Critical	Urgent action needed, book professional assessment

Unsure about the assessment?

Imprint

cycura GmbH

Your specialist for Microsoft Security

Contact:
E-Mail: info@cycura.de
Web: www.cycura.de

Commercial Register:
Amtsgericht Göttingen HRB 206706

VAT ID: DE354593485

Disclaimer: This guide was created with great care. Nevertheless, errors cannot be completely excluded. cycura GmbH assumes no liability for damages resulting from the use of this guide. All information without guarantee. Microsoft, Microsoft 365, Azure and other product names are trademarks of Microsoft Corporation.

© cycura GmbH 2026. All rights reserved.

Ready to know your risks?

www.cycura.de/termin