

IHR CEO IST IM URLAUB. IST
IHRE IT-INFRASTRUKTUR
GESCHÜTZT?

URLAUBSZEIT = NEUE CYBERRISIKEN

Wenn Mitarbeiter im Urlaub sind, können Sicherheitslücken entstehen.

Urlaubszeiten stellen Unternehmen vor neue Herausforderungen

- ✓ Eingeschränkte Sicherheitskapazitäten
- ✓ Weniger IT- und Sicherheitsexperten verfügbar
- ✓ Längere Reaktionszeiten bei Sicherheitsvorfällen
- ✓ Wichtige Entscheidungsträger sind weniger verfügbar

Temporäre Zugriffsänderungen

- ✓ Mitarbeiter erhalten zusätzliche Zugriffsrechte als Vertretung
- ✓ Temporäre Konten können länger aktiv bleiben als nötig.
- ✓ Zugriffsfreigaben können weniger streng geprüft werden

Erhöhtes menschliches Risiko

- ✓ Mitarbeiter arbeiten aus fremden Umgebungen
- ✓ Phishing-Angriffe nutzen Zeitdruck und Abwesenheiten aus
- ✓ Angreifer geben sich als Führungskräfte oder abwesende Kollegen aus



ANGREIFER ZIELEN AUF IDENTITÄTEN, NICHT NUR AUF SYSTEME

Moderne Cyberangriffe nutzen zunehmend kompromittierte Identitäten, um sich Zugriff zu verschaffen.

WAS ANGREIFER WIRKLICH WOLLEN

Kompromittierte Identitäten öffnen den Zugang zu sensiblen Daten, kritischen Systemen und Geschäftsprozessen.



Benutzeridentitäten: Gestohlene Passwörter, Phishing-Angriffe, kompromittierte Benutzerkonten



Privilegierte Identitäten: Administratorkonten, Dienstkonten, Notfallkonten



Cloud-Identitäten: SaaS-Anwendungen, Remote-Zugriffsumgebungen, hybride IT-Infrastrukturen

Identitäten zu schützen bedeutet, das gesamte Unternehmen zu schützen.

5 IAM-MAßNAHMEN, DIE JEDES UNTERNEHMEN BRAUCHT

Identity Security beginnt mit der Kontrolle darüber, wer auf welche Ressourcen zugreifen darf.

Das Prinzip der geringsten Privilegien anwenden

- ✓ Benutzer erhalten nur die erforderlichen Berechtigungen
- ✓ Übermäßige Zugriffsrechte reduzieren
- ✓ Die Auswirkungen kompromittierter Konten minimieren

Multi-Faktor-Authentifizierung (MFA) implementieren

- ✓ Zusätzliche Kontrollen hinzufügen
- ✓ Protect against stolen passwords
- ✓ Secure remote access

Zugriffsprüfungen und Rezertifizierungen automatisieren

- ✓ Bestehende Berechtigungen regelmäßig überprüfen
- ✓ Veraltete Zugriffsrechte entfernen
- ✓ Compliance-Anforderungen erfüllen

Rollenbasierte Zugriffskontrolle (RBAC) einsetzen

- ✓ Berechtigungen auf Basis von Geschäftsrollen vergeben
- ✓ Manuelles Zugriffsmanagement reduzieren
- ✓ Konsistenz und Transparenz verbessern

Eine starke Identity Governance etablieren

- ✓ Klare Genehmigungsprozesse definieren
- ✓ SoD sicherstellen
- ✓ Audit-Trails führen

PRIVILEGIERTE KONTEN ERFORDERN ZUSÄTZLICHEN SCHUTZ

Privilegierte Zugriffe müssen kontrolliert, überwacht und kontinuierlich überprüft werden.



**Privilegierte Anmeldedaten
sichern**

- Password-vaulting
- Automatische Passwort-Rotation



**Privilegierte Aktivitäten
überwachen**

- Session recording
- Echtzeitüberwachung



Sitzungsaufzeichnung

- Just-in-Time-Zugriff
- Befristete Berechtigungen
- Genehmigungs-Workflows



**Privilegierte Aktionen
auditieren**

- Vollständige Nachvollziehbarkeit
- Compliance reporting

CYBERSICHERHEIT IN DER URLAUBSZEIT: CHECKLISTE FÜR UNTERNEHMEN

Vor der Urlaubszeit	Während der Urlaubszeit	Nach der Urlaubszeit
Zugriffsrechte überprüfen	Kritische Systeme überwachen	Temporären Zugriff entfernen
Privilegierte Konten überprüfen	Eskalationsprozesse befolgen	Zugriffsrechte überprüfen
Notfallkontakte aktualisieren	Ungewöhnliche Aktivitäten überwachen	Vorfälle analysieren
Backup-Wiederherstellung	MFA konsequent durchsetzen	Lessons Learned dokumentieren



CYBERSICHERHEIT
MACHT KEINEN
URLAUB.

URLAUBSZEIT DARF
KEINE
SICHERHEITSLÜCKEN
SCHAFFEN.

Ihre Mitarbeiter mögen zwar offline sein,
Ihre Cybersicherheitsmaßnahmen sollten
es jedoch niemals sein.

Unternehmen können ihre Cyber-
Resilienz stärken, indem sie Folgendes
kombinieren:

- ◆ Starke Identitätsverwaltung
- ◆ Privileged Access Management
- ◆ Kontinuierliche Überwachung
- ◆ Klare Sicherheitsprozesse

STÄRKEN SIE IHRE IDENTITY SECURITY MIT PATECCO

Kontaktieren Sie uns. Wir unterstützen Sie gerne!



- PATECCO GmbH
- +49(0) 23 23 - 987 97 96
- info@patecco.com
- www.patecco.com