
PATECCO
dynamic identity systems.
YOUR CEO IS ON VACATION.
IS YOUR IT INFRASTRUCTURE
PROTECTED?

VACATION SEASON = NEW CYBER RISKS

When people are away, security gaps can appear.

Vacation periods create new challenges for organizations

- ✓ Reduced security capacity
- ✓ Fewer IT and security specialists available
- ✓ Longer response times during incidents
- ✓ Limited availability of key decision-makers

Temporary access changes

- ✓ Employees receive additional permissions to cover colleagues
- ✓ Temporary accounts may remain active longer than necessary
- ✓ Access approval processes may become less strict

Increased human risk

- ✓ Employees work remotely from unfamiliar environments
- ✓ Phishing attempts exploit urgency and absence
- ✓ Attackers impersonate executives or colleagues on leave

ATTACKERS TARGET IDENTITIES, NOT JUST SYSTEMS

Modern cyberattacks increasingly focus on gaining access through compromised identities.

WHAT ATTACKERS ARE REALLY LOOKING FOR

Compromised identities are the gateway to sensitive data, critical systems and business operations.

User identiites: Stolen passwords, Phishing campaigns Compromised accounts

Privileged identities: Administrator accounts, Service accounts, Emergency access accounts

Cloud identities: SaaS applications, Remote access environments, Hybrid IT infrastructures

Protecting identities means protecting the entire organization.

5 IAM CONTROLS EVERY COMPANY NEEDS

Identity security starts with controlling who has access to what.

Apply the Principle of Least Privilege

- ✓ Users receive only the permissions they need
- ✓ Reduce excessive access rights
- ✓ Minimize the impact of compromised accounts

Implement Multi-Factor Authentication (MFA)

- ✓ Add additional verification layers
- ✓ Protect against stolen passwords
- ✓ Secure remote access

Automate Access Reviews & Recertification

- ✓ Regularly verify existing permissions
- ✓ Remove outdated access rights
- ✓ Ensure compliance requirements are met

Use Role-Based Access Control (RBAC)

- ✓ Assign permissions based on business roles
- ✓ Reduce manual access management
- ✓ Improve consistency and transparency

Establish Strong Identity Governance

- ✓ Define clear approval workflows
- ✓ Ensure segregation of duties (SoD)
- ✓ Maintain audit trails

PRIVILEGED ACCOUNTS REQUIRE EXTRA PROTECTION

Privileged access must be controlled, monitored and continuously reviewed.

Secure privileged credentials

- Password vaulting
- Automatic password rotation

Monitor privileged activities

- Session recording
- Real-time monitoring

Control privileged access

- Just-in-time access
- Time-limited permissions
- Approval workflows

Audit privileged actions

- Complete traceability
- Compliance reporting

VACATION CYBERSECURITY CHECKLIST FOR COMPANIES

Before vacation	During vacation	After vacation
Review access rights	Monitor critical systems	Remove temporary access
Check privileged accounts	Follow escalation processes	Perform access reviews
Update emergency contacts	Monitor unusual activities	Analyze incidents
Test backup recovery	Maintain MFA enforcement	Document lessons learned

CYBERSECURITY DOES NOT TAKE A VACATION

VACATION PERIODS SHOULD NOT BECOME SECURITY GAPS

Your employees may be offline, but your cybersecurity controls should never be.

Organizations can strengthen their cyber resilience by combining:

- Strong Identity Governance
- Privileged Access Management
- Continuous Monitoring
- Clear Security Processes

STRENGTHEN YOUR IDENTITY SECURITY WITH PATECCO

Get in touch. We are ready to support!

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