Admin- & Break-Glass-Konten

Das IR-Team braucht sofort privilegierten Zugriff auf Firewall, Hypervisor, AD und Cloud – **über Konten, die nicht kompromittiert sind.** Diese Liste enthält KEINE Passwörter: Sie dokumentiert, welche Notfallkonten existieren und wo deren Zugangsdaten sicher verwahrt sind (versiegelter Umschlag im Tresor, Offline-Passwortmanager).

Warum dieses Dokument?

Hat der Angreifer Domain-Admin, ist jedes Alltagskonto verdächtig. Dedizierte Break-Glass-Konten sind der einzige saubere Weg zurück in die eigene Infrastruktur.

Wann brauchen Sie es?

In Stunde 1, wenn Firewall, Hypervisor oder Tenant erreichbar sein müssen, ohne kompromittierte Konten zu benutzen – und bei jedem Test und Passwortwechsel der Notfallkonten.

Wo aufbewahren?

Nur als Ausdruck im Tresor, Zweitexemplar im anderen Brandabschnitt oder Bankschließfach. Die Umschläge mit den Zugangsdaten getrennt von dieser Liste versiegeln.

Break-Glass richtig benutzen

1. **Umschlag öffnen** – nur nach Freigabe, 4-Augen-Prinzip
2. **Ins Logbuch** – Öffnung sofort in IR-03: wer, wann, warum
3. **Konto nutzen** – Alarm bei Login ist gewollt
4. **Danach rotieren** – Passwort wechseln, neu versiegeln, Test terminieren

Grundregel: Break-Glass-Konten werden nie im Alltag benutzt – jede Anmeldung außerhalb eines Notfalls ist ein Alarmsignal.

So sieht ein ausgefüllter Eintrag aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg (fiktiv)

System	Konto	Typ	Verwahrort	Letzter Test
AD Forest	bg-admin-01	Break-Glass	Umschlag 1, Tresor GF Augsburg	02.05.2026 ok
M365 / Entra	breakglass@musterm.onmicrosoft.com	Break-Glass, MFA-ausgenommen, Alarm bei Login	Umschlag 2, Tresor GF + Kopie Bankschließfach	02.05.2026 ok
FW-01	fw-emergency	dediziert, nur Konsole	Umschlag 3, Serverraum-Tresor	14.01.2026 ok

⚠ **Dieses Blatt niemals digital im Firmennetz ablegen.** Nur Ausdruck + Tresor – für Angreifer ist es der Wegweiser zu den Kronjuwelen. Die Öffnung eines Umschlags gehört sofort ins Incident-Logbuch (IR-03), danach: Passwort wechseln und neu versiegeln.

Halbjährliche Prüfung: ☐ alle Logins getestet ☐ Umschläge versiegelt ☐ Zweitverwahrort aktuell
Geprüft am: _____ von: _____

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

UNTERNEHMEN	STAND / VERSION	VERANTWORTLICH	ORT DER OFFLINE-KOPIE	NÄCHSTE PRÜFUNG

BREAK-GLASS- / NOTFALLKONTEN – KEINE PASSWÖRTER EINTRAGEN, NUR VERWAHRORTE

System / Ebene	Kontoname	Kontotyp	MFA?	Verwahrort der Zugangsdaten (Umschlag-Nr., Tresor)	Zweitverwahrort (anderer Brandabschnitt / Standort)
AD Forest		☐ dediziertes Break-Glass ☐ Standard-Admin ☐ Hersteller-Default (!)	☐ ja, Methode: ☐ ausgenommen (bewusst)		
Azure / M365-Tenant		☐ dediziertes Break-Glass ☐ Standard-Admin ☐ Hersteller-Default (!)	☐ ja, Methode: ☐ ausgenommen (bewusst)		
Firewall		☐ dediziertes Break-Glass ☐ Standard-Admin ☐ Hersteller-Default (!)	☐ ja, Methode: ☐ ausgenommen (bewusst)		
Hypervisor		☐ dediziertes Break-Glass ☐ Standard-Admin ☐ Hersteller-Default (!)	☐ ja, Methode: ☐ ausgenommen (bewusst)		
Backup-Konsole		☐ dediziertes Break-Glass ☐ Standard-Admin ☐ Hersteller-Default (!)	☐ ja, Methode: ☐ ausgenommen (bewusst)		
Core-Switch		☐ dediziertes Break-Glass ☐ Standard-Admin ☐ Hersteller-Default (!)	☐ ja, Methode: ☐ ausgenommen (bewusst)		
		☐ dediziertes Break-Glass ☐ Standard-Admin ☐ Hersteller-Default (!)	☐ ja, Methode: ☐ ausgenommen (bewusst)		

„Hersteller-Default (!)“ heißt: Standard-Zugangsdaten des Herstellers – sofort ändern, das ist keine Notfall-Lösung, sondern eine offene Tür.

FREIGABE & PFLEGE DER NOTFALLKONTEN

System / Konto (wie Blatt 1)	Wer darf öffnen? (Rollen, 4-Augen-Prinzip?)	Letzter Test des Kontos (Datum – funktioniert Login noch?)	Letzter Passwortwechsel

PRIVILEGIERTE ROLLEN IM ALLTAG – WELCHE KONTEN SIND BEI KOMPROMITTIERUNG EINER PERSON ZU SPERREN?

Person	Systeme mit Admin-Rechten	Konto-Namen

Tipp aus der Einsatzpraxis: Testen Sie jedes Break-Glass-Konto halbjährlich per echtem Login – abgelaufene Passwörter und deaktivierte Konten fallen sonst erst im Ernstfall auf. Jeden Test hier dokumentieren.