Asset- & System-Inventar mit Kritikalität

Das IR-Team muss binnen Stunden wissen: **Was gibt es überhaupt, was davon ist geschäftskritisch, wo läuft es – und wer kennt es?** Ohne Kritikalitätsbewertung ist die Priorisierung von Forensik und Wiederanlauf reines Raten. Und was nicht im Inventar steht, wird bei der Bereinigung übersehen – der klassische Weg zur Re-Infektion.

Warum dieses Dokument?

Gerade die vergessenen Systeme (alte Server, Appliances, OT) sind häufig das Einfallstor. Dazu gehören auch Domains, Zertifikate, SaaS-Dienste – und die Log-Quellen, ohne die Forensik blind ist.

Wann brauchen Sie es?

In Stunde 1 zur Priorisierung der Forensik (flüchtige Log-Quellen zuerst!), danach für Isolations-Entscheidungen (IR-15) und die Wiederanlauf-Reihenfolge.

Wo aufbewahren?

VERTRAULICH: Für Angreifer ist diese Liste ebenso wertvoll wie für Responder. Nur ausgedruckt im Tresor + zweiter Brandabschnitt, nie unverschlüsselt aufs Fileshare.

So sieht ein ausgefüllter Eintrag aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg, 1.200 MA, Automobilzulieferer (fiktiv)

Host	Funktion	Krit.	RTO	Standort	Abhängig von	Internet?
DC-01/DC-02	Active Directory	K1	4 h	RZ Augsburg / Azure	–	nein
ERP-DB-01	ERP-Datenbank (Produktion + Faktura)	K1	8 h	RZ Augsburg	DC, SAN-01	nein
TS-02	Terminalserver Vertrieb	K2	24 h	RZ Augsburg	DC, ERP	nein
WEB-SHOP	Ersatzteil-Shop	K2	24 h	Hoster CloudNord, FRA	Shop-DB	ja: 443
CNC-GW-03	OT-Gateway Halle 2	K1	2 h	Halle 2	keins (autark)	**ja: Fernwartung TCP 5900 (!)**

⚠ **Der Eintrag CNC-GW-03 zeigt, warum diese Liste Gold wert ist:** eine vergessene Fernwartung, die vor dem IR-Team niemand auf dem Schirm hatte. Nehmen Sie bewusst auch die „unwichtigen" Systeme auf – Appliances, Altsysteme, Testserver: Was nicht im Inventar steht, wird bei der Bereinigung übersehen.

Halbjährliche Prüfung: ☐ neue Systeme ergänzt ☐ Zertifikats-Abläufe geprüft ☐ Log-Aufbewahrung 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

SYSTEME – EINE ZEILE PRO SYSTEM (K1 = ÜBERLEBENSWICHTIG, K2 = WICHTIG, K3 = VERZICHTBAR/TAGE)

System- / Hostname	Funktion (was tut es fürs Geschäft?)	Kritikalität	RTO	Standort · Phys/VM/ Cloud/SaaS	OS + Version	IP-Adresse(n) / Netzsegment	Abhängig von (AD, DB, Lizenzserver ...)	Verantwortlich intern / Dienstleister	Aus dem Internet erreichbar? Ports?
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:

RTO = maximal tolerierbare Ausfallzeit. Dienstleister-Betreuung mit Namen eintragen – Notfallnummern gehören in IR-01.

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

SYSTEME (FORTSETZUNG)

System- / Hostname	Funktion (was tut es fürs Geschäft?)	Kritikalität	RTO	Standort · Phys/VM/ Cloud/SaaS	OS + Version	IP-Adresse(n) / Netzsegment	Abhängig von (AD, DB, Lizenzserver …)	Verantwortlich intern / Dienstleister	Aus dem Internet erreichbar? Ports?
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:
		☐ K1 ☐ K2 ☐ K3							☐ nein ☐ ja:

NOTIZEN

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

DOMAINS & ZERTIFIKATE

Domain / Zertifikat	Zweck	Registrar / CA	Ablaufdatum	Zugang verwaltet von	DNS-Hoster

SAAS-DIENSTE

Dienst	Zweck	Admin-Konto-Inhaber	Kritikalität	SSO?
			☐ K1 ☐ K2 ☐ K3	☐ ja ☐ nein
			☐ K1 ☐ K2 ☐ K3	☐ ja ☐ nein
			☐ K1 ☐ K2 ☐ K3	☐ ja ☐ nein
			☐ K1 ☐ K2 ☐ K3	☐ ja ☐ nein
			☐ K1 ☐ K2 ☐ K3	☐ ja ☐ nein
			☐ K1 ☐ K2 ☐ K3	☐ ja ☐ nein
			☐ K1 ☐ K2 ☐ K3	☐ ja ☐ nein

Tipp aus der Einsatzpraxis: Abgelaufene Zertifikate und vergessene Domains blockieren im Ernstfall die Wiederherstellung (Mail-Zustellung, VPN, Shop). Ablaufdaten hier pflegen – und bei SaaS prüfen: Hängt der Admin-Zugang am kompromittierten SSO?

LOG-QUELLEN – WAS WIRD WO WIE LANGE GESPEICHERT?

Quelle	Wo gespeichert (lokal / Syslog / SIEM / Cloud)	Aufbewahrungs-dauer	Zeitzone / NTP-Sync?	Wie exportieren (Tool, Format, wer kann es?)	Zentral gesammelt?
Firewall					☐ ja ☐ nur lokal (flüchtig!)
VPN					☐ ja ☐ nur lokal (flüchtig!)
AD / DC Security-Log					☐ ja ☐ nur lokal (flüchtig!)
M365 / Entra Sign-in					☐ ja ☐ nur lokal (flüchtig!)
Mail-Gateway					☐ ja ☐ nur lokal (flüchtig!)
Proxy / DNS					☐ ja ☐ nur lokal (flüchtig!)
Endpoint / EDR / AV					☐ ja ☐ nur lokal (flüchtig!)
Server-Eventlogs					☐ ja ☐ nur lokal (flüchtig!)
Hypervisor					☐ ja ☐ nur lokal (flüchtig!)
Physische Zutrittssysteme					☐ ja ☐ nur lokal (flüchtig!)
					☐ ja ☐ nur lokal (flüchtig!)
					☐ ja ☐ nur lokal (flüchtig!)

⚠ **Wenn die Firewall nur 7 Tage speichert und der Initial Access drei Wochen her ist, ist die Spur weg.** Diese Übersicht entscheidet in Stunde 1, welche flüchtigen Quellen zuerst gesichert werden. Zeilen mit „nur lokal“ und kurzer Aufbewahrung heute entschärfen.