Oneconsult 360-Grad-Checkliste

für die Bewältigung eines Cyber-Vorfalls

Follow us & stay informed!

oneconsult.com

/oneconsult-ag

/OneconsultAG

Newsletter

Oneconsult

Zürich | Bern | München | Auckland

Die Oneconsult 360-Grad-Checkliste

für die Bewältigung eines Cyber-Vorfalls

Anleitung und Struktur

Die 360-Grad-Checkliste besteht aus einer Liste von Aufgaben, an die Sie bei einem Cyber-Vorfall denken sollten. Ziel ist es, einen Überblick über die zu berücksichtigen Dinge und die Verantwortlichkeiten und Aufgaben jedes Einzelnen zu geben, damit während der Stresssitutation nichts vergessen wird.

Die 360-Grad-Checkliste orientiert sich an den sechs Phasen des Incident-Response-Prozesses (IR) des SANS-Institutes (Vorbereitung, Identifizierung, Eindämmung, Beseitigung, Wiederherstellung und Erkenntnisse) und wird in Form einer DEBI-Matrix dargestellt. Die gelisteten Aufgaben sind in einer groben Reihenfolge aufgeführt, da der IR-Prozess ein Zyklus mit vielen Feedback Loops ist.

Damit die 360-Grad-Checkliste für das eigene Unternehmen stimmig ist, sollte sie unbedingt auf die lokalen Gegebenheiten adaptiert werden.

Legende

- D: Durchführung – Wer (welche Person, Rolle, Organisationsabteilung) erledigt die Aufgabe?
- E: Entscheidung – Wer entscheidet und trägt die Gesamtverantwortung oder berichtet zur korrekten Ausführung der Aufgabe?
- B: Beratung – Wer kann beraten und mit Fachwissen unterstützen?
- I: Informationsrecht («zu informieren») – Wer muss informiert werden bzw. wer kann Informationen anfordern?

Themengebiete

Die 360-Grad-Checkliste umfasst folgende fünf Themengebiete:

- Technik: Relevant für die technischen Abteilungen (bspw. IT)
- Organisation: Taskforce
- Personal: vor allem HR
- Juristische Themen: Juristen, Anwälte
- Experten/Externe: IT-Partner, IR/Forensik-Partner (z.B. Oneconsult)

Beispiele

Die Tabelle wird auf folgende Weise gelesen, zum Beispiel für die erste Zeile:

- Die IT-Abteilung (Technik) erstellt während der Vorbereitungsphase einen Netzwerkplan, um die Visibilität zu erhöhen.
- Der Netzwerkplan wird der Taskforce (Organisation) und den Experten/Externen während dem Einsatz zur Verfügung gestellt.

Die Oneconsult 360-Grad-Checkliste

für die Bewältigung eines Cyber-Vorfalls

Legende: D: Durchführung | **E:** Entscheidung | **B:** Beratung | **I:** Informationsrecht

IR-PHASEN	AUFGABEN	TECHNIK	ORGANISATION	PERSONAL	JURISTISCHE THEMEN	EXPERTEN/ EXTERNE
Vorbereitung	Netzwerkplan	D	I			I
	Inventarisierung der Assets	D	I			I
	Assets nach Wichtigkeit fürs Bestehen/ Betrieb des Unternehmens klassifizieren	D	I			I
	Schutzlösung (bspw. AV)	D	I			D/B
	Logging- und Monitoring-Lösungen (bspw. EDR/NDR)	D	I			D/B
	Security/Vulnerability Scans	D	I			I/D
	AD Überblick (PingCastle)	D	I			I/D
	Patch-/Vulnerabilitymanagement	D	E			D/B
	Daten aus Logging- und Monitoring-Lösungen wegsichern	D	I			D/B
	Berechtigungen für die Datensammlung und Analyse	I	I		D	B
	Backup-Konzept	D	E			D/B
	Zugriffskonzept (Schlüssel, usw.)	I	D			
	Kontaktliste (Mitarbeitenden, Geschäftsleitung, IT-Partner, usw.)	I	D	(I)	(I)	I
	Kommunikationsplan	I	D	(I)	(I)	I/B
	Kommunikationswege und Tools für Gespräche, Sitzungen und Datenaustausch definieren	I	D	(I)	(I)	I
	Kommunikation gegenüber Mitarbeiter, Partnern, Öffentlichkeit, Behörden (wenn Meldepflicht)	I	E	D	I	B
	Rollen und Verantwortlichkeiten festlegen	I	D	I		I
	Verträge und Konditionen klären und überprüfen (IR/ Forensik-Partner, Cyberversicherung, IT-Partner, usw.)	I	D			I/B
	Incident Response Plan	D	I	I	(I)	D/B
	Strategie bei Erpressung (bspw. Ransomware/Datenveröffentlichung)	I	D		B	B
	Juristische Einschränkungen (z.B. andere Länder)		I		D	B
	Personelle Konsequenzen/Schadenersatz gegenüber Institutionen/Partnern		I		D	B
	Meldepflicht (DSGVO, Verbandsauflagen, branchenspezifische Auflagen, usw.)		I/D		D	B
	Versicherung informieren		I/D		D	B
	Polizeianzeige erstatten		I/D		D	B
Identifikation	AV-Scans überall durchführen	D				D/B
	Bestimmung des Krisenstands	I	D			B
	Erfrage des Incidentshergangs (Verdächtige, Hinweise, Spuren, ...)	(D)	I			D
	Erkennung potenzieller Schäden		D			B
	Sind andere Firmen mitbetroffen?		D			I/B
	Worst- und Best-Case Szenario definieren und durchspielen und daraus notwendige Massnahmen ableiten und ggf umsetzen	I	D			I/B
	Von wem und wie oft und soll das Lagebild beurteilt werden?	I	D			I/B
	Status Meetings und Protokoll führen	I	D			I
	Tagesziele kommunizieren	I	D			I/B
	Prioritäten und Strategie festlegen	I	D			B
	Arbeitsteilung	I	D			I
	ToDo-Liste erstellen und Erledigung resp. Abarbeitung der Tasks kontrollieren	I	D			I
	Konfliktpotenzial erkennen (mit anderen Personen/Firmen)		D	(I)		
	Wissensträger/Schlüsselpersonen identifizieren	I	I	D		
	Ansprechpersonen für die Systeme/Bereiche definieren	D	I	I		I
	Verfügbarkeit von Ressourcen (wer, wann, wie) planen	D	E	D	D	D
	Ressourcenplanung technischer Mittel (Storage, Computer, usw.)	D	E/I			
	"War Room" bereitstellen	I	D			I
	Material (Büromaterial, Flipchart, usw.) organisieren		D			
	Verpflegung (Essen und Getränke)	I	D	I		I
	Care Team für betroffenen Personen (persönlich oder psychisch/ Belastung)	I	I	D		

Die Oneconsult 360-Grad-Checkliste

für die Bewältigung eines Cyber-Vorfalls

Legende: D: Durchführung | **E:** Entscheidung | **B:** Beratung | **I:** Informationsrecht

IR-PHASEN	AUFGABEN	TECHNIK	ORGANISATION	PERSONAL	JURISTISCHE THEMEN	EXPERTEN/ EXTERNE
Eindämmung	Systeme isolieren	D				B
	Netzwerk abschalten und Verbindungen von/ zu Externen kappen	D	E			
	Schutz von unbetroffenen Systemen	D				B
	Sicherung von relevanten Daten und Images erstellen	D				D/B
	Bösartige IP-Adressen und Domains blockieren	D				B
	Konten deaktivieren	D				B
	Forensische Analyse	(D)	I			D
	Notbetrieb sicherstellen	D				B
Beseitigung	Prozess für die Aufsetzung von sauberen Systemen bestimmen	I	D			B
	Backups auf Infektionen überprüfen	D				B
	Saubere und isolierte Umgebung für den Restore vorbereiten	D				B
	Zurücksetzen aller Passwörter (auch Admin, Services und Kerberos)	D				B
	Konten auf Legitimität überprüfen	D				B
	Extern erreichbare Dienste aktualisieren und patchen	D				B
Wiederherstellung	Wiederherstellung (Neuaufsetzen, aus Backups, usw.)	D	I			B
	Netzwerkverkehr wiederherstellen	D	E			
	Zuschalten der Dienste	D	E			D/B
	Härten der Systeme, GPO, usw.	D				B
	Management von Firewall	D	I			B
	Logpolicies erstellen	D	I			B
	Verstärkte Überwachung	D	I			B
Erkenntnisse	Dokumentation (Schlussbericht)	D	I	I	I	D/B
	Lessons Learned Meeting/Debriefing des Vorfalles	I	D	I	I	D/B
	Protokoll des Meetings führen	I	D	I	I	D/B
	Prozesse überprüfen und anpassen, Massnahmen umsetzen	D	E/D	(D)	(D)	B

Oneconsult AG
Giesshübelstrasse 45
8045 Zürich
Schweiz

+41 43 377 22 22
info@oneconsult.com
www.oneconsult.com

oneconsult
together against cyberattacks