CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

CloudCommand GmbH chr.schumacher@gmx.tm

Incident Response Plan

Aufbau

- Klar definierte Rollen
- Kontaktlisten
- Meldewege
- Eskalationsstrategie
- Verantwortungen gegenüber Dritten
- Kritische Prozesse/Assets
- Dokumentation des Vorfalls
- Klassifizierung
- Regelmäßige Simulation
- Werkzeuge

Kontaktlisten

Incident Manager

- Störfallkoordination
- Bestätigung Störfallfeststellung und -schwere
- Bestätigung Störfallbehebung
- Koordination der Störfallkommunikation
- Beauftragung externer technischer Experten

Kontaktlisten

Incident Response Team / Sicherheitsbetrieb

- Sicherheitsüberwachung/Störfallerkennung
- Störfallfeststellung
- Störfallnachverfolung und -dokumentation
- Durchführung der Incident-Response-Aktivitäten
- Störfallbehebung
- Technische Analyse
- Forensische Analyse (falls intern durchgeführt)

Kontaktlisten Beispiel

Incident Manager

- Name: Anna Aal
- Mobil: +49 123 456789
- E-Mail: aal@mycompany.de

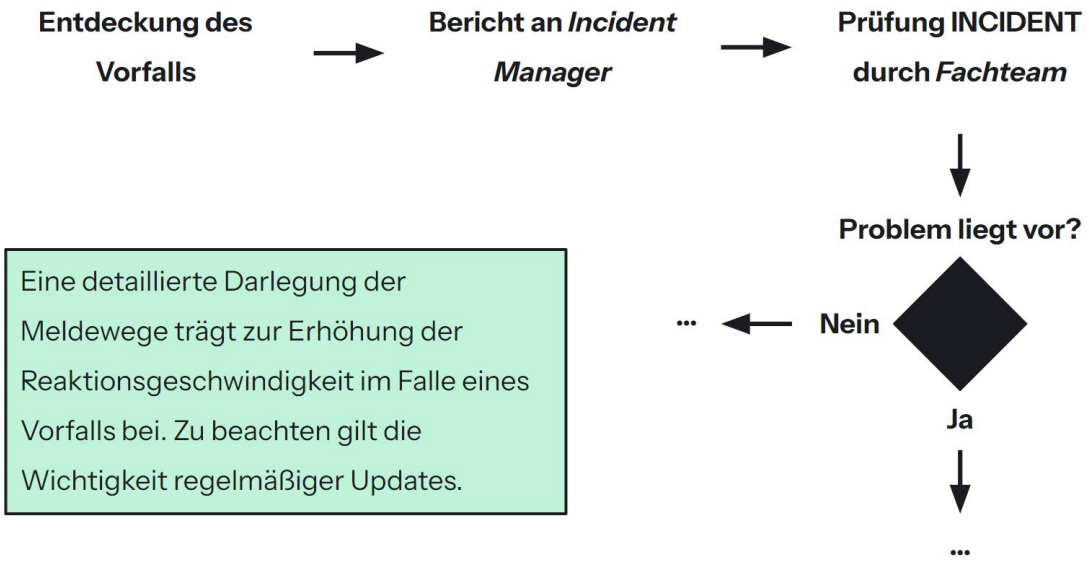
Incident Manager

- Name: Bert Barsch
- Mobil: +49 333 889900
- E-Mail: bbarsch@hotmail.de

ISB

- Name: Carla Carpfen
- Mobil: +49 898 345782
- E-Mail: carla.carpfen@web.de

Meldewege



Eine detaillierte Darlegung der Meldewege trägt zur Erhöhung der Reaktionsgeschwindigkeit im Falle eines Vorfalls bei. Zu beachten gilt die Wichtigkeit regelmäßiger Updates.

Meldewege

Betreiber Kritischer Infrastrukturen und Betreiber von Energieversorgungsnetzen

- Meldepflicht des § 8b Absatz 4 BSIG oder § 11 Absatz 1c EnWG

Anbieter digitaler Dienste

- Meldepflicht auf Grundlage des §8c Absatz 3 BSIG

Betreiber von öffentlichen Telekommunikationsnetzen und Erbringer öffentlich zugänglicher Telekommunikationsdienste

- Meldepflicht gemäß § 109 Absatz 5 TKG

Meldepflicht nach der Verordnung über elektronische Identifizierung und Vertrauensdienste

- eIDAS-Verordnung

Sonstige Verträge oder Verpflichtungen

Kritische Prozesse/Assets

Nr.	Prozess	Benötigte Anwendungen	Vertraulichkeit	Integrität	Verfügbarkeit
P-001	Buchhaltung	A001 - A004	Sehr hoch	Sehr hoch	Normal
P-002	Personalwesen	A005	Hoch	Normal	Normal
P-003	Kundenservice	A006 - A008	Hoch	Normal	Hoch
...	...	...	...	...	...

Dokumentation des Vorfalls

Anlage 1 zu
VCV - IT-Vorfallsmeldung Meldekategorien

Formular Meldung IT-Vorfall

TLP:	☐ White	☐ Green	☐ Amber	☐ Red
	Meldung IT-Vorfall			
Behörde:				
Meldender:				
Erreichbarkeit:	(Telefon)	(E-Mail)		
Rückfragen:	(Telefon)	(E-Mail)		Sofern abweichend von Erreichbarkeit Meldender
Datum:	**Uhrzeit:**			Wann ist das Ereignis eingetreten?

Dokumentation des Vorfalls

Vorläufige Klassifizierung durch den Meldenden:		**Sachverhalt** Verweis auf beigefügteZusatzdokumente möglich
Externer Angriff	☐	Leitfragen: • Was wurde festgestellt / was ist passiert? • Wer bzw. was ist betroffen? Welcher Schaden wurde bereits festgestellt? • Ist eine Kompromittierung weiterer Systeme in anderen Organisationen wahrscheinlich? • Wurden bereits (Gegen-) Maßnahmen ergriffen? Wenn ja, welche? • Wurden bereits weitere Stellen informiert?
Datenverlust	☐	
Sicherheitslücke	☐	
Störung von SW/HW-Komponenten	☐	
WiderrechtlicheAktion	☐	
Interne Ursachen	☐	
Externe Einflüsse	☐	
Besondere Erkenntnisse	☐	
Zweck der Information / Erwartete Reaktion durch CERT-Bund		Mehrfachauswahl möglich
	☐ Zur Kenntnisnahme ☐ Bitte um Rückruf	☐ Freigabe zur Aufnahme in Lagebericht ☐ Bitte um Einschätzung / Stellungnahme	☐ Explizite Freigabe der Endfassung zur Aufnahme in Lagebericht durch Meldenden erforderlich ☐ Unterstützung erforderlich ☐

Dokumentation des Vorfalls

Optional: Vorschläge des Meldenden zum weiteren Vorgehen	Verweis auf beigefügte Zusatzdokumente möglich
Optional: Sonstiges / freie Anmerkungen	Verweis auf beigefügte Zusatzdokumente möglich
Zu melden an:	BSI IT-Lage- und Analysezentrum; <lagezentrum@bsi.bund.de>; Telefon: 022899 9582 -5110 oder -5499

Klassifizierung

Als Sicherheitsvorfall wird ein Ereignis bezeichnet, das die **Vertraulichkeit**, **Verfügbarkeit** und **Integrität** von IT-Services, IT-Systeme oder IT-Anwendungen mit hohem oder sehr hohem Schutzbedarf derart beeinträchtigt, dass ein großer Schaden für ein Unternehmen oder seine Kunden und Geschäftspartner entstehen kann.

Klassifizierung

0 (gering)

- **Vorfall mit minimalem Einfluss**
- Beispiele hierfür sind E-Mail-SPAM, isolierte Virenfälle usw.

1 (medium)

- **Vorfälle mit signifikantem Einfluss**
- Beispiele sind eine verzögerte Bereitstellung von Diensten, Beeinträchtigung unserer Mission, verspätete Zustellung von wichtigen E-Mails oder Datenübertragungen usw.

Klassifizierung

2 (hoch)

- **Vorfälle mit schwerwiegendem Einfluss**
- Beispiele sind eine Beeinträchtigung der Dienste und/oder der Erfüllung unserer Mission. Unsere proprietären oder vertraulichen Informationen wurden kompromittiert, ein Virus oder Wurm hat sich weit verbreitet und betrifft mehr als 1% der Mitarbeiter, öffentliche Sicherheitssysteme sind nicht verfügbar, oder unser Führungsteam wurde benachrichtigt.

Klassifizierung

3 (sehr hoch)

- **Vorfälle mit katastrophalem Einfluss**
- Beispiele sind die Abschaltung aller unserer Netzwerkdienste. Unsere proprietären oder vertraulichen Informationen wurden kompromittiert und auf einer öffentlichen Website veröffentlicht. Öffentliche Sicherheitssysteme sind nicht verfügbar. Das Führungsteam muss eine öffentliche Erklärung abgeben.

Klassifizierung

VORFALL KLASSE	BESCHREIBUNG
Missbräuchliche Inhalte	Spam, Belästigung, Gewalt
Schadcode	Ransomware, Infection, Malicious Connection
Informationsbeschaffung	Scanning, Sniffing, Phishing
Intrusion Attempts	Exploiting, Login Versuche, IDS Alert
Intrusion	Successful Exploitation, Account Beschlagnahmung

Klassifizierung

VORFALL KLASSE	BESCHREIBUNG
Verfügbarkeit	DoS, DDoS, Sabotage
Informationssicherheit	Unerlaubter Zugang, Unerlaubte Modifikation
Betrug	Unerlaubte Nutzung von Ressourcen, Copyright
Sonstige	Alles andere...

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm