

Inhaltsverzeichnis

Hilferuf 7

Teil 1: Angriff der Spinne 9

01 Vorwort des Autors zu Teil 1 10

02 Aufklärung (Reconnaissance) 12

03 Erster Zugang (Initial Access) 19

04 Ausführung (Execution) 26

05 Verwurzelung (Persistence) 34

06 Generalschlüssel (Privilege Escalation) 43

07 Unsichtbar (Defense Evasion) 54

08 Diebstahl (Credential Access) 63

09 Erkundung (Discovery) 72

10 Ausbreitung (Lateral Movement) 80

11 Fernsteuerung (Command and Control) 87

12 Sammlung (Collection) 91

13 Kopieren (Exfiltration) 93

14 Übersicht: MITRE ATT&CK® Taktiken und Techniken 98

Teil 2: Wiederaufbau bei der NovumSpace 101

01 Beteiligte Personen beim Wiederaufbau 102

02 Einschlag (Impact) 103

03 Basar (Verhandlung) 111

04 Ankunft 127

05 Orientierung 133

06 Zahlen? 137

07 Standpunkt bestimmen 142

08 Eindämmung 146

09 Beweissicherung 157

10 Grüne Wiese 162

Teil 3: Resilienz und Verteidigung bei ME Light	177
01 Über die ME Light KG, Führungsteam	178
02 Verstehen	179
Briefing	184
Den Feind kennen	188
Cyber Kill Chain und MITRE ATT&CK®	192
Formales Cyber-Resilienz-Programm	196
Krisenmanagement	197
Business-Continuity-Management-System (BCMS)	200
Information-Security-Management-System (ISMS)	208
NIS-2-Richtlinie	212
98% Schutz mit Basishygiene	215
Workshop zum Schutzbedarf	219
Delta-Analyse	235
Roadmap	239
03 Phase: Sofort	253
Aktive digitale Verteidigung (XDR, SOC, DFIR)	253
Cyber-Resilienz-Leitlinie des Topmanagements	255
MFA für privilegierte/sensitive Benutzer	264
Ausrollen von Endpoint-Detection and Response	266
Erste Zwischenbilanz	267
04 Auf dem Prüfstand	268
05 Phase: Bald	274
Security-Operations-Center und Managed XDR	274
Digitale Forensik und Incident-Response (DFIR)	279
Aktualisierung Konzepte und Dokumente	280
Menschenzentrierung	281
Minimale Berechtigungen (Least Privilege)	283
Stabsrahmenübung für einen Ransomware-Notfall	285
MFA und Passwort-Manager für Standardbenutzer	286
Ständige IT- und Systemhygiene	287
06 Urlaub	288
07 Phase: Später	293
Regelmäßige (Penetration-)Tests des Sicherheitsprogramms	295
Überwachung von Identitäten auf Anomalien	296
Vertrauliche Daten kennzeichnen	297
Zentrales Logging und Protokollierung (SIEM)	298
Ransomware-Schutz auf Dateiebene	298
Schutz für Operational Technology (OT)	299
SOC-Visibility-Triad, Netzwerkerkennung (NDR)	301
08 Cyber-Resilienz-Forum	302
09 Dinner	304