www.pwc.de/incident-response

Die Spurenleserin

Katharina Bunzel über digitale Forensik im Incident Response Team bei PwC Deutschland

pwc

Cyber-Straftaten rekonstruieren

Jedes Verbrechen hinterlässt Spuren – auch im Bereich der Cyberkriminalität. Anstelle von Blutspritzern und Fingerabdrücken sind es hier bestimmte Datenmuster in technischen Artefakten. Diese Spuren nach einem Cybervorfall zu sichern und den Tathergang zu rekonstruieren, ist Aufgabe von Forensik-Expert:innen wie Katharina. Seit vier Jahren arbeitet sie im Bereich Incident Response und geht der Ursache von Cyberangriffen auf den Grund.

„Wir kümmern uns am Tatort zunächst um die digital-forensische Datensicherung. Dabei bauen wir unter anderem auch PCs und Laptops auseinander, um an die Datenträger zu kommen und den Datenbestand gerichtsfest aufzunehmen. Oftmals führen wir auch Live-Datensicherungen von Servern und virtuellen Maschinen durch. Danach analysieren wir die Daten und gehen auf Spurensuche“, erklärt Katharina. Ähnlich wie bei konventionellen Kriminalfällen wird die Arbeit dadurch erschwert, dass die Kriminellen versuchen, so wenige Spuren wie möglich auf den Systemen zu hinterlassen. Aber: „Egal wie gut ein Angreifer ist, irgendetwas wird immer übersehen. Und das zu finden, ist unser Ziel“, ergänzt Katharina.

Schnitzeljagd im digitalen Raum

Bei der Analyse klopfen die Forensiker:innen systematisch verschiedene Punkte ab. Wie haben sich die Angreifer von System zu System bewegt? Welche Malware und ggf. Software für bspw. Datenexfiltration kamen zum Einsatz? Was wurde im Falle eines Ransomware-Angriffs verschlüsselt? „Die Analyse ist manchmal wie eine Schnitzeljagd. Ich finde auf dem System etwas und kann von da aus auf den nächsten Schritt schließen. Das macht enorm viel Spaß“, sagt Katharina. „Die Spuren bilden eine Geschichte – eine Zeitlinie, die wir nach und nach aufdecken. Wenn wir sie vollständig offenlegen, finden wir auch den Patienten Null – den Ursprungspunkt des Angriffs.“ Die Rekonstruktion des Tathergangs hilft Unternehmen dabei, die Lücken in ihrer Cyberabwehr nachzuvollziehen und sie zielgerichtet zu schließen.

IT-Expertise trifft Faible für Kriminalfälle

Katharina hat sich bereits in ihrem Studium mit digitaler Forensik beschäftigt und sich früh für die technische Seite entschieden. Grundsätzlich ist das Berufsbild aber auch für Quereinsteigende interessant. „Im Grunde genommen ist hier jeder gut aufgehoben, der ein tiefes Interesse an IT und Kriminalfällen hat“, sagt Katharina. „Man benötigt außerdem eine ausgeprägte Neugier. Die Technik und die Methodik der Angreifer entwickeln sich ständig weiter. Man lernt bei jedem Fall etwas dazu und muss sich regelmäßig weiterbilden.“

Auch sehr wichtig sind Teamplay und eine offene Kommunikation: „Niemand kann alles wissen. Wir machen die Analysen deshalb immer zusammen und bauen die Story gemeinsam auf. Und unser Team ist wirklich cool. Hier hilft jeder jedem.“ Neben der Abstimmung innerhalb des Teams spielt auch der Austausch mit der IT-Abteilung der angegriffenen Unternehmen eine wichtige Rolle. „Wenn wir direkt vor Ort miteinander sprechen können, geht vieles schneller. So können wir bei einem verdächtigen Fund fragen, ob es sich um einen normalen Kundenprozess handelt. Sonst wissen wir direkt: Hier wurde etwas von den Angreifern eingeschleust.“

Jeder Einsatz ist ein Abenteuer

Die Fälle, in denen Datenforensiker:innen zum Einsatz kommen, sind vielfältig. Sie rücken bei Cybervorfällen wie Ransomware-Attacken aus, helfen aber auch bei der Aufklärung von Compliance-Verstößen –Ç zum Beispiel, um herauszufinden, ob ein Mitarbeitender nach Verlassen eines Unternehmens Daten mitgenommen hat. „Einmal hatten wir auch den Fall, bei welchem wir rausfinden sollten, ob ein Mitarbeitender Kryptowährung gemint hatte“, erinnert sich Katharina.

Wann und wo ein Cybervorfall auftritt – ob in München, Hamburg oder Berlin – ist im Vorfeld stets ungewiss. Das erfordert laut Katharina auch Flexibilität: „Man muss sich bewusst machen, dass es kein 9-to-5-Job ist. Es gibt sehr intensive und dann aber auch wieder ruhige Phasen – ähnlich wie bei der Feuerwehr. Dafür ist aber auch jeder Einsatz ein echtes Abenteuer.“

Hinter den Kulissen

Spurensicherung und forensische Analyse von Cyberangriffen

Wie konnte es nur so weit kommen? Diese Frage stellt sich jede Organisation nach einem Cyberangriff. Um den Tathergang zu rekonstruieren und den initialen Einfallsvektor herauszufinden, kommen Analyst:innen für digital-forensische Datensicherung und Systemanalyse zum Einsatz. Als Teil des Incident Response Teams kümmern sie sich um eine gerichtsfeste Datensicherung. Darüber hinaus analysieren sie die Spuren und rekonstruieren die Schritte der Täter. So machen sie das initiale Einfallstor des Angriffs ausfindig und helfen damit Unternehmen, sich gezielt zu schützen und die Lücken in der Verteidigung zu füllen – je nach Fall zum Beispiel durch Awareness-Trainings für Mitarbeitende oder ein verbessertes Patchmanagement. Die Ergebnisse der forensischen Analysen sind außerdem wichtig, um Cyberversicherungen den Schadensfall nachzuweisen.

Mehr Informationen zu PwCs Incident Response unter
www.pwc.de/incident-response

Join our community of solvers

Hier gibt's die Jobs für dich:
www.karriere.pwc.de/cybersecurity

Kontakt

Katharina Bunzel
Incident Response Team
PwC Deutschland
Tel.: +49 69 9585-3925
katharina.bunzel@pwc.com

www.pwc.de