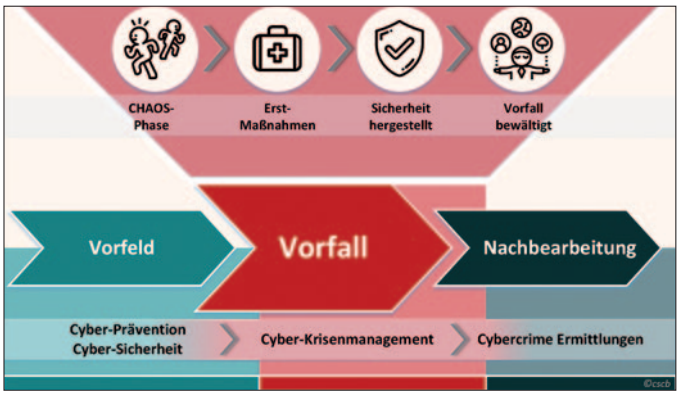
Digitaler Tatort

Die zunehmende Digitalisierung stellt die Ermittlungsbehörden in der digitalen Ermittlung und Forensik vor Herausforderungen. Dazu bedarf es an Zusammenarbeit, technologischer Innovation und Weiterbildung.

Mit dem Begriff Tatort verknüpfen die meisten ein klassisches Verbrechen und die Zuständigkeit der Polizei. Doch auch die Digitalisierung hinterlässt an Tatorten ihre Spuren. Die Bearbeitung digitaler Tatorte kann daher herausfordernd sein. Sie erfordert wie bei analogen Tatorten Know-how, um sicherzustellen, dass digitale Beweismittel erkannt und richtig gesichert werden können.



Ein Cyber-Sicherheitsvorfall in drei Phasen mit den allgemeinen und sicherheitspolizeilichen Aufgabenstellungen

Die Sicherstellung digitaler Beweismittel, egal ob im Kriminaldienst, Verkehrsdienst oder in anderen Bereichen der Polizei, gehört mittlerweile zur Routine, obwohl selten ein Fall dem anderen gleicht. Das können Mobiltelefone, Festplatten, DVDs, PCs, Notebooks oder sogar Kraftfahrzeuge sein. Die falsche Handhabung von Datenträgern bei der Sicherstellung kann zu deren Beschädigung und somit zum Verlust von digitalen Beweismitteln führen.

Den Polizeibediensteten stehen zu diesem Zweck Richtlinien zur Verfügung. Diese können über die Vorschriftensammlung der Polizei nachgeschlagen werden. Im Assistenzbereich IT-Beweissicherung/Erkennungsdienst (AB 06 IT-B) im Landeskriminalamt (LKA) Kärnten wurde überdies eine eigene IT-Policy (IT-Sicherheitsrichtlinie) geschaffen, um einen höheren Grad an Schutz für sichergestellte Beweismittel zu schaffen.

Der digitale Tatort: Nicht mehr nur Polizeisache. In der Polizei sind in der Regel Einheiten wie das *Cybercrime-Competence-Center (C4)* im Bundeskriminalamt (BK), der Assistenzbereich 06 in den Landeskriminalämtern (LKAs) oder die IT-Forensikerinnen und -Forensiker aus den Bezirken mit der Sicherstellung, Sicherung und Aufbereitung von Daten und Datenträgern betraut. Auch in der Direktion Staatsschutz und Nachrichtendienst (DSN) und den Landesämtern Verfassungsschutz und Terrorismusbekämpfung (LVTs) sind Forensik-Expertinnen und -Experten tätig. Auch außerhalb der Polizei gibt es Expertenwissen in diesen Bereichen. Dazu gehören zum Beispiel Sachverständige oder spezialisierte Unternehmen in der Wirtschaft.

Vieles wird in Computersystemen und Netzwerken automatisch digital protokolliert und ist Schritt für Schritt auch im Nachhinein nachvollziehbar. Kleinste Fehler können ein Gerichtsverfahren vor ernste Probleme stellen, etwa wenn Daten nicht verfügbar, nicht nachvollziehbar oder verloren gegangen sind.

Beispiel digitaler Tatort-Bearbeitung. Im Assistenzbereich IT-Beweissicherung/Erkennungsdienst im LKA Kärnten wurde die Qualität der digitalen Beweismittelsicherstellung immer weiter verbessert. Im LKA Kärnten wurde ein eigener Landes-IT-Dienst – kurz LIT – ins Leben gerufen, der allein im ersten Jahr über 450 Serviceleistungen für Dienststellen und Kollegen rund um die Uhr und am Wochenende bereitgestellt hat. Er setzt sich aus Mitarbeiterinnen und Mitarbeiter des AB 06 IT-B sowie aus IT-Ermittlerinnen und -Ermittler aus den Bezirken zusammen. Jede Dienststelle und jeder Polizeibedienstete hat in Kärnten 24/7 einen kompetenten Ansprechpartner aus der digitalen Forensik zur Verfügung.

Auch Fragen zur Cyber-Kriminalität und digitalen Ermittlungsansätzen sowie Hilfestellungen bei komplexen IT-Sachverhalten werden vom Landes-IT-Dienst angeboten. Die Unterstützung erfolgt in erster Linie telefonisch oder bei Bedarf persönlich in der Dienststelle des Anforderers, z. B. bei einer Sicherstellung von Datenträgern, beispielweise an einem Wochenende oder in den Nachtstunden. Der einschreitende Beamte kann telefonisch notwendige Erstmaßnahmen erfragen oder jemanden aus der IT-Forensik für die korrekte Sicherstellung beiziehen. Probleme bei der Administration von polizeilichen Systemen fallen nicht in die Zuständigkeit des Landes-IT-Dienstes. Der Landes-IT-Dienst in Kärnten wird auch nach der Umsetzung der Kriminaldienstreform bestehen bleiben.

Grenzen der digitalen Ermittlungen zeigen sich als vielschichtige Kombination von auf den ersten Blick trivialen und hochkomplexen Problemen. Technologische Barrieren, wie fortschrittliche Verschlüsselungsmethoden, die Flüchtigkeit digitaler Daten und die weit verbreitete Anonymität im Netz, sind wesentliche Hürden, die Ermittlerinnen und Ermittler bewältigen müssen. In diesem Kontext erweist sich die Zusammenarbeit mit IT-(Sicherheits-)Dienstleistern als wichtig, um digitale Spuren aus den „Incident-Response"-Maßnahmen zu erhalten. „Incident Response" bezeichnet die Reaktion und Sofortmaßnahmen nach einem Cyber-Sicherheitsvorfall in einem Unternehmens-Netzwerk.

Die Kooperation mit Online-Service-Providern kann aus polizeilicher Sicht anspruchsvoll sein, da unterschiedliche Speicher- und Verarbeitungsmethoden der Betreiber zu variierenden Ergebnissen bei Anfragen führen können. Daher ist es wichtig, die zentralen Abfragestellen für Social-Media und Online-Provider (ZASP) im BK und in der DSN auszubauen.

Rechtliche Rahmenbedingungen, etwa beschränkter Zugriff auf Daten aufgrund divergierender Gesetzgebungen,

GRAFIK: CSCB

Die Sicherstellung und Analyse digitaler Beweismittel gehört mittlerweile zur Routinearbeit der IT-Spezialisten der Polizei

können die Arbeit zusätzlich erschweren. Ebenso der Mangel an Expertise und Budgetbeschränkungen. Eine ständig fortschreitende Cyber-Bedrohungslandschaft und die Existenz unterschiedlicher nationaler Normen und Gesetze erschweren zudem die internationale Zusammenarbeit, was eine fortwährende Anpassung und Weiterbildung der Ermittlungsteams erfordert, um eine effektive länderübergreifende Kooperation in der digitalen Spurensuche zu gewährleisten. Der Ausgangspunkt digitaler Ermittlungen bleibt jedoch stets die Identifikation digitaler Spuren und das Verständnis, welche zusätzlichen Informationen daraus abgeleitet werden können.

Vorfälle als neue Normalität. Ein Cyber-Sicherheitsvorfall wird definiert als absichtlicher Angriff auf die Vertraulichkeit, Verfügbarkeit und/oder Integrität von Daten oder IT-Systemen, der Betroffene im großen Ausmaß beeinträchtigt. Ein solcher Vorfall ist für das Bundesministerium für Inneres (BMI) relevant – als Sicherheitsbehörde im Bereich der Cybersicherheit und in der Strafverfolgung. Um die Anzahl an Cyber-Sicherheitsvorfällen möglichst gering zu halten, müssen Ressourcen in die Cyber-Prävention und die Cyber-Sicherheit fließen. Wenn all das nicht genützt hat und es trotzdem zu einem Cyber-Angriff auf ein Netzwerk eines Unternehmens gekommen ist, ist ein gutes Cyber-Krisenmanagement erforderlich. Dabei scheitert es oft an der falschen oder mangelnden Kommunikation innerhalb des betroffenen Unternehmens oder der Organisation und nach außen. Wenn ein solcher Vorfall eintritt, ist die rasche Kommunikation mit der zuständigen Strafverfolgungsbehörde wichtig, da es beispielsweise dort schon Erfahrungswerte gibt und im Krisenmanagement wertvolle Hilfestellungen geliefert werden können.

Es besteht auch hier der Bedarf an der Sicherung digitaler Spuren (IOCs = Indicators of Compomise) und der Aufbereitung digitaler Beweismittel, um die ersten Ermittlungsmaßnahmen zur Strafverfolgung ehestmöglich, aufgrund der Flüchtigkeit der Daten, in die Wege zu leiten. Um sicherzustellen, dass auch komplexe Sachverhalte professionell und bestmöglich bearbeitet werden können, sind ab kommendem Jahr Trainings für Ersteinschreiterinnen und Ersteinschreiter bei Cyber-Sicherheitsvorfällen im kriminalpolizeilichen Bereich geplant.

Ein positiver Ausblick für die Bearbeitung digitaler Tatorte könnte neben organisatorischen Lösungen von Problemen wie z. B. der Umsetzung eines Landes-IT-Dienstes liegen, der Professionalisierung von Ersteinschreitern bei Cyber-Sicherheitsvorfällen sowie neuen Technologien und Methoden für die digitale Forensik. Die Verbesserung von Algorithmen und Analysetools könnte die Aufbereitung von Informationen sowie die Verknüpfung und Interpretation von Daten erleichtern, Trainings und Weiterbildungsangebote, um dem Mangel an Expertise zu kompensieren. Zudem könnten rechtliche Neuregelungen und internationale Abkommen den Zugriff auf grenzüberschreitende Daten vereinfachen.

Christian Baumgartner
Christina Schindlauer

FOTO: GERD PACHAUER