Rechtskompass für Forensik und Incident Response

Von Datenschutz bis Lösegeld: Unternehmen und Forensiker können rechtliche Risiken bei der Bewältigung von Cyberangriffen effektiv minimieren. Es empfiehlt sich, nicht erst in einer Krisensituation zu handeln, sondern Rechtsfragen präventiv zu klären.

Von Johann Rabbow

Rechtliche Fragen sollten im Rahmen eines „Digital Forensics and Incident Response"-Einsatzes (DFIR) mindestens grundlegende Aufmerksamkeit erhalten. Dies betrifft sowohl die angegriffenen Organisationen als auch die Experten, die Unterstützung leisten. Viele Rechtsfragen können die verantwortlichen Parteien bereits im Vorfeld klären, müssen also nicht erst in einer Krisensituation spontan entscheiden. Eine gründliche Vorbereitung ist möglich und reduziert das Risiko, dass sie sich in rechtlich bedenkliche oder sogar strafbare Handlungen begeben.

Dieser Artikel bietet einen Überblick über die Themen Datenschutz und Lösegeldzahlungen, mit denen sich Unternehmen präventiv auseinandersetzen sollten; zugleich ist dieses Wissen auch für Incident-Responder und IT-Forensiker während ihrer Einsätze von Bedeutung. Letztlich sind sie die Fachleute, die präzise Antworten auf grundlegende rechtliche Fragen parat haben sollten.

Datenschutz: Was zu beachten ist

Gute Nachrichten zu Beginn: Die wichtigsten datenschutzrechtlichen Fragen können Incident-Responder und IT-Forensiker ohne große Mühe klären und bearbeiten. Wichtige Aspekte umfassen: Auftragsverarbeitung gemäß Artikel 28 DSGVO, Erhebung und Auswertung von Logdateien sowie Ermittlungen gegen eigene Mitarbeiter.

Unternehmen müssen einen grundlegenden Datenschutzgrundsatz beachten: das Verbot mit Erlaubnisvorbehalt. Dieser Grundsatz besagt, dass die Verarbeitung personenbezogener Daten ohne ausdrückliche Erlaubnis verboten ist. Daher ist es wichtig, dass Unternehmen sicherstellen, dass die Voraussetzungen einer einschlägigen Erlaubnisnorm erfüllt sind, bevor sie personenbezogene Daten verarbeiten. Die relevanten Normen für forensische Einsätze finden sich vor allem in Artikel 6 DSGVO und § 26 BDSG. Eine Verarbeitung ohne Einhaltung dieser Voraussetzungen ist unzulässig und kann gemäß Artikel 82 ff. DSGVO zu Bußgeldern führen. Diese Strafen richten sich gegen das verstoßende Unternehmen. Persönliche Haftungen aufgrund von Datenschutzverstößen sind möglich, aber in der Praxis selten.

Weitere datenschutzrechtliche Themen, die bei Incident-Response-Einsätzen eine untergeordnete Rolle spielen, können vertrauensvoll Juristen und Datenschützern überlassen werden. Es ist entscheidend, dass DFIR-Experten datenschutzrechtliche Vorschriften einhalten, da sie bei Einsätzen zwangsläufig personenbezogene Daten wie zum Beispiel IP-Adressen verarbeiten.

Auftragsverarbeitung

Wenn ein Dienstleister forensische Untersuchungen durchführt, müssen Unternehmen das als Auftragsverarbeitung gemäß Artikel 28 DSGVO klassifizieren, denn der Dienstleister (Auftragsverarbeiter) verarbeitet die Informationen nach Weisung und im Auftrag des Verantwortlichen (Auftraggebers). Dabei sind sowohl der Auftragsverarbeiter als auch der Auftraggeber verpflichtet, eine Auftragsverarbeitungsvereinbarung (AVV) abzuschließen, und nicht nur der Auftraggeber, wie oft fälschlicherweise angenommen wird.

Ohne eine solche Vereinbarung besitzt der Dienstleister keine Rechtsgrundlage

iX-TRACT

- Ob Lösegeldzahlungen oder forensische Analysen – rechtlich gibt es bei Incident Response und Forensik einige Punkte, die zu beachten sind, möchte man nicht Gefahr laufen, mit Bußgeld belegt zu werden oder sich strafbar zu machen.
- Empfehlenswert ist die Beschäftigung mit den rechtlichen Fallstricken im Vorfeld; strafbare Handlungen lassen sich nicht zurücknehmen.
- Eine pragmatische Umsetzung der rechtlichen Vorgaben ist möglich. Das Wissen hierzu ist sowohl für Forensiker als auch betroffene Organisationen von Vorteil.

Auftragsverarbeitung: Praxistipps

- **Vertragsdokumentation:** Die Auftragsverarbeitungsvereinbarung (AVV) sollte dem schriftlichen Dienstleistungsangebot beiliegen.
- **Vertragsgegenstand:** Ein Verweis auf den Hauptvertrag ist bei der Definition des Verarbeitungsgegenstands möglich.
- **Art und Zweck der Verarbeitung:** Dies umfasst das Auswerten von Benutzeraktivitäten, das Analysieren von Benutzerkonten, das Überprüfen von Anmeldeverhalten, das Zugreifen auf Systeme mit personenbezogenen Daten und das Auswerten bereitgestellter Logfiles.
- **Art der personenbezogenen Daten:** Zu den Daten gehören Namen, Adressen, E-Mail-Adressen, Korrespondenzen, Bankdaten, Gesundheitsinformationen, Logdaten sowie alle weiteren Informationen, die auf den geschäftlichen digitalen Infrastrukturen des Verantwortlichen gespeichert sind.
- **Kategorien betroffener Personen:** Dazu zählen aktuelle und ehemalige Mitarbeiter des Auftraggebers, Endkunden des Auftraggebers, deren Dienstleister und Geschäftspartner.

für die Verarbeitung personenbezogener Daten, was zu bußgeldbewährten Konsequenzen führt. Hinweise zur Ausgestaltung der AVV zeigt der Kasten „Auftragsverarbeitung: Praxistipps“.

Erheben und Auswerten von Logdateien

Logdateien stellen für DFIR-Experten ein datenschutzrechtliches Dilemma dar, denn sie enthalten oft zahlreiche personenbezogene Daten, die einerseits sehr sensibel sein können, andererseits für Analysen unverzichtbar sind. Hier trifft der Datenschutzgrundsatz der Datenminimierung gemäß Artikel 5 Absatz 1 lit. c DSGVO direkt auf den Sicherheitsgrundsatz nach Artikel 32 DSGVO sowie die Meldeverpflichtungen gemäß Artikel 33 und 34 DSGVO (siehe Abbildung).

Auch wenn es das Gesetz nicht direkt sagt, so ist es eine denklogische Notwendigkeit: Nur wer ausreichend einen Vorfall aufklärt, kann seinen Verpflichtungen zur Meldung an die Behörde und zur Benachrichtigung der Betroffenen nachkommen. Ohne Kenntnisse über die genauen Umstände eines Angriffs ist eine Einschätzung der Gefahr für die betroffenen Personen nicht möglich.

Unternehmen sollten also einerseits möglichst wenig personenbezogene Daten erheben, andererseits brauchen sie aber genau diese Daten zur Absicherung von Systemen und zur Aufklärung von Vorfällen. Dieser Konflikt lässt sich durch eine einfache Regel lösen: maximale Datenspeicherung bei minimalem Zugriff. Um den beiden Schutzzielen der DSGVO – Datenminimierung sowie Sicherheit und Aufklärung – gerecht zu werden, müssen Organisationen zunächst festlegen, welche Systeme für welchen Zeitraum Logdateien speichern sollen. Ein guter Anhaltspunkt ist die 90-Tage-Regel der CIS Controls 8.10, wobei 90 Tage das absolute Minimum darstellen (siehe Website der CIS Controls unter ix.de/z689). Besser sind 180 Tage oder mehr, da Angreifer in den meisten größeren Vorfällen über mindestens diesen Zeitraum Zugriff auf die Systeme haben. Ein weiterer wichtiger Hinweis: Auch wenn die Speicherdauer lang eingestellt ist, sollte diese nicht durch eine Speicherplatzbegrenzung eingeschränkt sein – hier ist Großzügigkeit geboten.

In einem zweiten Schritt muss der Zugriff auf die Logdateien streng begrenzt werden, um den Schutzgedanken gemäß Artikel 5 Abs. 1 lit. c DSGVO zu wahren. Die Zugriffsbegrenzungen dürfen jedoch nicht so restriktiv sein, dass sie den Schutzzweck des Artikels 32 DSGVO untergraben.

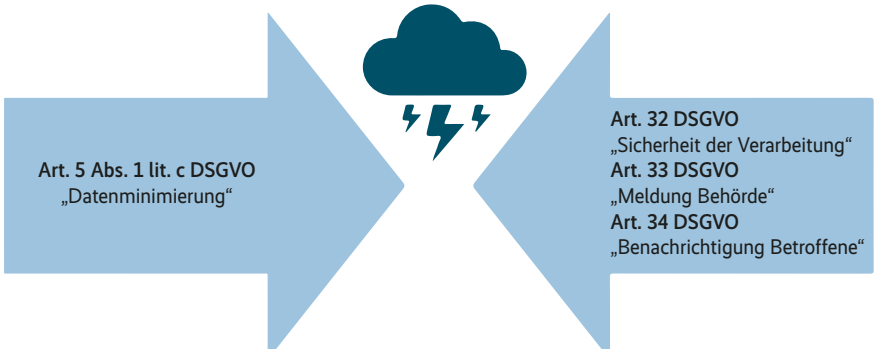
Unternehmen, die eine angemessene Sicherheit gewährleisten möchten, benötigen regelmäßige, automatisierte Auswertungen ihrer Logdateien, was so weit unproblematisch ist. Das bedeutet jedoch nicht, dass IT-Mitarbeiter nach Belieben auf die Dateien zugreifen dürfen. Der Zugriff sollte ausschließlich zweckgebunden und beispielsweise nach dem Vieraugenprinzip erfolgen. Es ist gute Praxis, Logdateien, die älter als etwa 45 Tage sind, auf einem zentralen Logserver, aber in einem gesonderten Pfad, zugriffssicher zu speichern. Bei Bedarf, etwa für Analysen außerhalb der Routine, kann die Organisation den Zugriff unter Einbeziehung des Datenschutzbeauftragten gewähren.

Ermittlungen gegen eigene Mitarbeiter

Interne Untersuchungen gegen Mitarbeiter sind unerfreulich, jedoch manchmal notwendig. Zum Beispiel wenn ein begründeter Verdacht besteht, dass ein Mitarbeiter Unternehmensgeheimnisse an Wettbewerber weitergegeben hat. Da eine IT-forensische Analyse des Arbeitsrechners oder -Smartphones einen erheblichen Eingriff in die Mitarbeiterrechte darstellt, benötigen DFIR-Experten definierte Voraussetzungen für ihre Untersuchungen, ehe sie Maßnahmen ergreifen können.

Die Diskussion beschränkt sich hier auf forensische Untersuchungen von Geräten, die das Unternehmen zur Verfügung stellt. Weitere rechtliche Aspekte wie das Anhörungsrecht des Mitarbeiters oder die Handhabung von privaten Geräten, die unter eine Bring-Your-Own-Device-Richtlinie fallen, werden nicht betrachtet.

Es ist sowohl für das auftraggebende als auch für das durchführende Unternehmen wichtig, sicherzustellen, dass die Analyse rechtmäßig ist. In jedem Fall muss ein Anfangsverdacht bestehen und auf konkreten Tatsachen beruhen. Bloße Vermutungen reichen nicht aus. Eine Untersuchung ist hingegen unumgänglich, wenn sich Verdachtsmomente erhärten, da aus der Sorgfaltspflicht der Geschäftsführung eine Aufklärungspflicht resultiert.



Das Gebot der Datenminimierung führt in Verbindung mit den gleichzeitig gestellten Sicherheitsanforderungen oft zu einem Zielkonflikt.

Ermittlungen gegen eigene Mitarbeiter – Praxistipps

Folgende Punkte bieten eine Orientierung für eine Untersuchung. Sie richten sich primär an den Auftraggeber, sollten aber auch dem Auftragnehmer bekannt sein. Denn sofern dieser Ungereimtheiten feststellt, ist ein Hinweis Richtung Auftraggeber angebracht.

- **Dokumentation:** Alle Schritte im Untersuchungsprozess sind schriftlich zu dokumentieren. Dies umfasst sowohl durchgeführte Maßnahmen als auch getroffene Entscheidungen. Bei Gefahr im Verzug dürfen Prozessschritte vereinfacht werden, um den Ermittlungserfolg nicht zu gefährden. In solchen Fällen wird die Einholung juristischen Rates empfohlen, um rechtliche Fallstricke wie etwa Beweisverwertungsverbote zu vermeiden.
- **Anfangsverdacht:** Eine Untersuchung darf nur beginnen, wenn konkrete Tatsachen einen Anfangsverdacht begründen.
- **Umfang der Untersuchung:** Die Datenverarbeitung während der Untersuchung muss zweckgebunden sein, gemäß Art. 5 Abs. 1 lit. b DSGVO. Forensiker müssen den Umfang der Untersuchung daher vorab klar definieren. Dies ist sowohl für den Auftraggeber als auch für den Auftragnehmer von Vorteil.
- **Unschuldsvermutung:** Der Datenschutzbeauftragte und der Betriebsrat sollten von Beginn an in die Untersuchung einbezogen werden, da deren Aufgaben auch den Schutz der Rechte der Arbeitnehmer umfassen. Eine verspätete Hinzuziehung kann einen Verstoß gegen datenschutzrechtliche oder betriebsverfassungsrechtliche Vorschriften darstellen.
- **Beweissicherung:** Die Untersuchung muss forensische Standards zur Sicherung von Beweisen einhalten, insbesondere die Beweismittelkette (Chain of Custody).
- **Gefahr im Verzug:** Wenn die Forensiker während ihrer Analyse auf Anzeichen stoßen, dass unmittelbares Handeln erforderlich ist, ist der Auftraggeber sofort zu informieren.
- **Abschlussbericht:** Alle Ergebnisse, sowohl belastende als auch entlastende Beweise, sollten in einem Abschlussbericht festgehalten und dem Auftraggeber übergeben werden.

Konflikte können auftreten, wenn Untersuchungsgegenstände privat genutzt wurden. Eine Analyse von privaten Daten, die nicht mit dem Untersuchungsziel zusammenhängen, ist unzulässig. Hierbei müssen Unternehmen zwei Fallkonstellationen unterscheiden, von denen jedoch nur eine eine besondere Herausforderung darstellt.

Privatnutzung verboten

Grundsätzlich gilt: Wenn die Privatnutzung beruflicher Geräte betrieblich untersagt ist, dürfen die Geräte unter den zuvor genannten Voraussetzungen analysiert werden. Eine Ausnahme besteht, wenn die Privatnutzung trotz offiziellem Verbot über Jahre hinweg geduldet wurde. In solchen Fällen könnte sich eine „betriebliche Übung“ etabliert haben, und die Geräte müssen behandelt werden, als sei die Privatnutzung erlaubt. Der Mitarbeiter trägt die Beweislast für die Existenz einer solchen betrieblichen Übung. Unabhängig davon ist das Analysieren offensichtlich privater Daten, die keinen Bezug zum Untersuchungsgegenstand haben, stets unzulässig. Beispielsweise sollten Forensiker E-Mail-Korrespondenzen mit Familienangehörigen eines Mitarbeiters nicht auswerten.

Privatnutzung erlaubt oder toleriert

Die Erlaubnis oder Duldung der Privatnutzung führt zu erheblichen rechtlichen Unsicherheiten, die Unternehmen verstehen und bewerten müssen, um die Risiken einschätzen zu können. Das erste Problem besteht darin, dass eine Unterscheidung zwischen betrieblich veranlassten und privaten Daten nicht vorab möglich ist. Eine Klärung ist oft erst nach einer Datenanalyse machbar, was bei privaten personenbezogenen Daten jedoch unzulässig ist.

Das zweite Problem resultiert aus der strengen Auslegung der Datenschutzkonferenz (DSK), eines Zusammenschlusses deutscher Datenschutzbehörden. Laut DSK werden Unternehmen, die Privatnutzung dulden oder erlauben, zu „Diensteanbietern von Telekommunikationsdienstleistungen“, was sie den Regelungen des TTDSG unterwirft (siehe Orientierungshilfe der Datenschutzkonferenz unter ix.de/z689). Das bedeutet, dass eine Einwilligung des Mitarbeiters vor einer Datenanalyse vorliegen muss. Andernfalls könnte ein strafbares Verhalten gemäß § 202 StGB (Verletzung des Briefgeheimnisses) und § 206 Abs. 1 StGB (Verletzung des Post- oder Fernmeldegeheimnisses) vorliegen. Jeder Beteiligte an der Datenanalyse, ob Entscheider oder Ausführender, wird von diesen Bestimmungen erfasst.

Dass Verdächtige einwilligen, ist unwahrscheinlich, und selbst wenn, ist die Freiwilligkeit dieser Einwilligung aufgrund des Über-/Unterordnungsverhältnisses zwischen Arbeitgeber und Arbeitnehmer oft zweifelhaft. Ohne Freiwilligkeit gibt es keine wirksame Einwilligung und folglich keine rechtmäßigen Ermittlungen.

Relevanz der Meinung der DSK

Die Meinung der DSK ist aber nur dann maßgeblich, wenn sie rechtlich korrekt ist. Dies wäre der Fall, wenn die Auslegung der DSK durch eine höchstrichterliche Entscheidung bestätigt wird, was bisher jedoch nicht erfolgt ist. Es gibt überzeugende Gründe anzunehmen, dass die höchstrichterliche Rechtsprechung diese Auslegung verwerfen wird. Da Unternehmen die Argumente der DSK bis zu diesem Entscheid allerdings nicht ohne Weiteres ignorieren können, besteht weiterhin eine Rechtsunsicherheit. Organisationen, die von dieser Unsicherheit betroffen sind, sollten rechtlichen Beistand hinzuzuziehen, um die spezifischen Risiken abzuwägen.

Wenn die Auslegung der DSK abgelehnt wird, und es gibt triftige Gründe dafür, sind nur die datenschutzrechtlichen Vorschriften zu beachten. Entscheidend ist § 26 Abs. 1 S. 2 BDSG, der die Verarbeitung personenbezogener Daten zur Aufdeckung von Straftaten erlaubt. Die Verarbeitung muss innerhalb der gesetzlichen Grenzen erfolgen. Im Kern ist eine Abwägung zwischen den Rechten der betroffenen Personen und den Interessen des Unternehmens erforderlich. In den meisten Fällen dürfte diese Abwägung zugunsten der Ermittlungen ausfallen, basierend auf der Bestätigung des Anfangsverdachts.

Diese Abwägung muss das Unternehmen selbst treffen. Sie ist nicht Aufgabe eines Forensikers. Für Forensiker gelten die bereits genannten Grundsätze: Sie dürfen keine offensichtlich privaten Daten analysieren, die nicht mit dem Untersuchungsgegenstand in Verbindung stehen, und sie dürfen nicht im Rahmen eines offensichtlich rechtswidrigen Auftrags tätig werden.

Da eine interne Untersuchung immer in die Rechte des Arbeitnehmers eingreift,

empfiehlt es sich, gewisse Prozessschritte einzuhalten, die im Kasten „Ermittlungen gegen eigene Mitarbeiter – Praxistipps“ zusammengefasst sind. Dadurch können Unternehmen das Risiko eines rechtswidrigen Vorgehens minimieren, sodass sich gewonnene Beweise auch in einem anschließenden gerichtlichen Verfahren verwerten lassen.

Lösegeldzahlungen leisten oder nicht

Zahlreiche Cyberangriffe zielen darauf ab, ein Lösegeld zu erpressen, was zur Etablierung des Begriffs „Ransomware“ geführt hat. Die Entscheidung, ob ein Lösegeld gezahlt werden sollte, ist komplex und wird von verschiedenen Faktoren beeinflusst. Oft werden pragmatische Überlegungen wie die Kosten und die potenzielle Unterstützung krimineller Aktivitäten gegen die Zahlung ins Feld geführt. Auf der anderen Seite steht die möglicherweise fehlende Alternative, wenn vollständige Verschlüsselungen ohne vorhandene Backups vorliegen.

Unternehmen sollten die strafrechtlichen Risiken, die mit einer Lösegeldzahlung verbunden sind, nicht außer Acht lassen. Eine Zahlung kann zur Unterstützung einer kriminellen Vereinigung gemäß § 129 StGB, zur Terrorismusfinanzierung gemäß § 89c StGB oder zur Untreue gemäß § 266 StGB führen. Zusätzlich könnte der Tatbestand des Umgehens einer wirtschaftlichen Sanktionsmaßnahme nach § 18 Außenwirtschaftsgesetz erfüllt sein.

Im Strafrecht gilt der Grundsatz: Jeder nach seiner Schuld. Es ist daher entscheidend, zwischen den verschiedenen Beteiligten einer Lösegeldzahlung zu differenzieren – dazu zählen üblicherweise die Geschäftsführung, die IT-Leitung, das zahlende Unternehmen und der DFIR-Dienstleister.

Je nach Beteiligungsgrad variiert die Möglichkeit, durch eine Lösegeldzahlung gegen § 129 StGB zu verstoßen. Eine klare Unterscheidung zwischen den Rollen der Beteiligten ist somit erforderlich, um das strafrechtliche Risiko angemessen beurteilen zu können.

§ 129 StGB für Geschäftsführung

Die Geschäftsführung besitzt im Rahmen ihrer Entscheidungsbefugnisse (vgl. § 93 AktG, § 43 GmbHG) die Freiheit, Lösegeld zu zahlen, solange die Handlung nicht gegen geltendes Recht verstößt. Allerdings erfüllen Lösegeldzahlungen im Kontext von Cyberangriffen häufig die Kriterien der Unterstützung krimineller Vereinigungen nach §§ 129 Abs. 1 S. 2, 129b Abs. 1 S. 1, 2 StGB.

In Fällen von Erpressung könnte der rechtfertigende Notstand nach § 34 StGB eine Rolle spielen, auch wenn dessen Anwendbarkeit umstritten ist. Es gibt jedoch starke Argumente dafür, dass Gerichte ihn als Rechtfertigungsgrund akzeptieren könnten. Entscheidend ist die Abwägung zwischen den Interessen des Geschäftsführers und denen der Allgemeinheit, insbesondere der öffentlichen Sicherheit und Ordnung. Der Geschäftsführer muss nachweisen, dass seine Interessen wesentlich die der Allgemeinheit überwiegen.

Eine Faustregel besagt: Wenn das Unternehmen auch ohne Zahlung weiterlaufen könnte, wenn auch nicht reibungslos, dann ist die Argumentation für einen rechtfertigenden Notstand schwierig. Falls jedoch ernsthafte Beeinträchtigungen wie eine mögliche Insolvenz oder dann notwendige Entlassungen drohen, ist eine Rechtfertigung wahrscheinlicher.

Sollte der rechtfertigende Notstand nicht anwendbar sein, gibt es weitere rechtliche Möglichkeiten, einer Strafbarkeit zu entgehen, wie zum Beispiel § 129 Abs. 6 StGB (Absehen von Strafe wegen Geringfügigkeit), § 153c Abs. 1 S. 1 Nr. 3 StPO (Absehen von der Verfolgung bei Auslandstaten) und § 129b Abs. 1 S. 3 StGB (Verfolgung nur auf Antrag des Generalbundesanwalts).

Zwei wichtige Klarstellungen: Erstens kann die Zahlung durch einen Angestellten der Geschäftsführung zugerechnet werden, da diese eine Überwachungspflicht hat und sicherstellen muss, dass keine unzulässigen Handlungen erfolgen. Ein Abwälzen der Verantwortung auf Mitarbeiter ist also nicht ratsam. Zweitens schützt Unwissenheit nicht vor Strafe. Ein Geschäftsführer, der sich auf Vermutungen verlässt, eine Zahlung sei wahrscheinlich unproblematisch, ohne sich angemessen zu informieren, erfüllt nicht die erforderliche Rechtsvergewisserungspflicht.

§ 129 StGB für den Leiter der IT

Da der IT-Leiter in seiner Funktion nicht die letzte Entscheidungsbefugnis besitzt, kommt für ihn lediglich eine Beihilfe (§ 27 StGB) zur Unterstützung einer kriminellen Vereinigung infrage. Dies hängt von seinem Beteiligungsgrad ab, insbesondere, ob er aktiv an der Zahlung mitwirkt und ob der Geschäftsführer für diese Haupttat verurteilt wird, da ohne eine solche Haupttat keine Beihilfe möglich ist.

In Bezug auf Erpressung könnte ebenfalls eine Strafbarkeit wegen Beihilfe zur Erpressung des eigenen Unternehmens durch Unterlassen (gemäß §§ 253 Abs. 1, 13, 27 StGB) bestehen. Voraussetzung hierfür ist, dass der IT-Leiter eine Garantenstellung hat, beispielsweise wenn ihm eine kritische Sicherheitslücke bekannt ist und er diese wissentlich nicht schließt, wodurch Angreifer diese Lücke ausnutzen können. Die Absicherung der Systeme gehört zu seinen Kernaufgaben, und durch die Nichterfüllung dieser Aufgabe handelt er sorgfaltswidrig. Sein Unterlassen kann damit kausal für die Erpressung durch die Angreifer sein.

Zurechenbarkeit für das zahlende Unternehmen

Die Handlungen der Führungskräfte sind einem Unternehmen gemäß § 9 in Verbindung mit § 30 OWiG zurechenbar, ebenso die Handlungen weiterer Verantwortlicher gemäß § 130 OWiG. Dies bedeutet, dass neben der persönlichen Strafbarkeit der Beteiligten auch ein Bußgeld gegen das Unternehmen selbst verhängt werden kann, wenn ein Verstoß gegen eine relevante Norm vorliegt.

Beihilfe durch den DFIR-Dienstleister

DFIR-Dienstleister, die bei einem Vorfall hinzugezogen werden, beraten oft auch bezüglich Lösegeldzahlungen. Ihre Aufgaben können die Verhandlungen mit Angreifern sowie die praktische Veranlassung von Lösegeldzahlungen umfassen. Je nach Grad der Beteiligung kann auch für sie, ähnlich wie beim IT-Leiter, eine Beihilfe zur Unterstützung einer kriminellen Vereinigung begründet werden.

Verstoß gegen das Außenwirtschaftsgesetz

Das Ziel von § 18 Abs. 1 AWG ist es, Verstöße gegen Bereitstellungsverbote – insbesondere im Rahmen von Sanktionsmaßnahmen der Europäischen Union – unter Strafe zu stellen. Zahlt ein Geschäftsführer ein Lösegeld an eine Ransomwaregang, die selbst oder deren einzelne Mitglieder auf einer Embargoliste der EU stehen, kann dies schnell zu einem Verstoß gegen § 18 Abs. 1 AWG führen (siehe Verordnung unter ix.de/z689).

Oft ist allerdings unklar, an wen das Geld überwiesen wird. Liegen jedoch öf-

fentlich zugängliche Informationen vor, kann sich ein Geschäftsführer nicht auf Unwissenheit berufen. Bei Fahrlässigkeit wird die Handlung gemäß § 19 Abs. 1 AWG als Ordnungswidrigkeit bewertet. Auch hier kann der rechtfertigende Notstand nach § 34 StGB relevant sein. Die Strafbarkeit von IT-Leitern und Dienstleistern in Bezug auf das Außenwirtschaftsgesetz wird analog zu den Ausführungen zu § 129 StGB behandelt.

Terrorismusfinanzierung und Untreue

Zusätzlich sind zwei weitere Straftatbestände zu betrachten, die zwar theoretisch möglich sind, aber in der Praxis keine Rolle spielen dürften. Die Wahrscheinlichkeit, dass sich ein Geschäftsführer wegen Terrorismusfinanzierung gemäß § 89 c Abs. 1 StGB strafbar macht, ist sehr gering, da das gezahlte Lösegeld konkret für die Begehung schwerer Straftaten wie Mord oder Kriegsverbrechen verwendet werden müsste, ein Umstand, den der Zahlende zum Zeitpunkt der Zahlung kennen müsste – ein eher unwahrscheinliches Szenario.

Bezüglich der Untreue gemäß § 266 Abs. 1 StGB wäre ein Tatbestand nur erfüllt, wenn durch die Zahlung des Lösegeldes gegen die Vermögensbetreuungspflicht verstoßen wird. Dies könnte der Fall sein, wenn der Geschäftsführer das Lösegeld ohne dringende Notwendigkeit zahlt – ebenfalls ein eher unwahrscheinliches Szenario. Realistischer ist die Zahlung, um die Interessen des Unternehmens zu schützen.

Lösegeldzahlungen

Es ist offensichtlich, dass die meisten Unternehmen Lösegeld nicht freiwillig, sondern unter erheblichem Druck zahlen. Strafverfolgungsbehörden nehmen dies zur Kenntnis und haben bisher keine Lösegeldzahlungen strafrechtlich verfolgt, zumindest sind keine solchen Verfahren bekannt.

Hier noch ein paar Praxistipps zur Vorbereitung auf Lösegeldzahlungen: Unvorbereitete Zahlungen in größeren Beträgen an Kryptowährungen, üblicherweise in Bitcoin oder Monero, benötigen erhebliche Vorbereitungszeit. In Notfällen steht diese Zeit oft nicht zur Verfügung, insbesondere weil Angreifer in der Regel eine enge Frist für die Zahlung setzen. Diese Fristen sind oft verhandelbar, doch darauf sollte man sich nicht verlassen. Folgende Maßnahmen sollten als Teil einer sorgfältigen Vorbereitung erwogen werden.

Da das Thema mittlerweile große Aufmerksamkeit erlangt hat, haben sich spezialisierte Dienstleister für die Zahlung von Lösegeld in Kryptowährungen etabliert. Es ist ratsam, mit einem solchen Dienstleister Kontakt aufzunehmen, um Modalitäten und Möglichkeiten zu klären. Stellen Sie sicher, dass der Dienstleister offiziell im eigenen Land registriert ist. Ein erster Ansatzpunkt wäre die eigene Bank. Relevante Fragen für einen ersten Austausch sind:

- Welche Kryptowährungen sind verfügbar?
- Innerhalb welches Zeitraums sind Zahlungen möglich?
- Bis zu welchem Betrag lassen sich Kryptowährungen erwerben?
- Ist eine Registrierung oder Kontoerstellung vorab erforderlich?
- Gibt es eine 24/7-Hotline für Notfälle am Wochenende oder an Feiertagen?

Fazit

Die Möglichkeit, gegen Straf- oder Bußgeldvorschriften im Rahmen von DFIR-Einsätzen zu verstoßen, besteht. Es ist jedoch möglich, das Risiko einer strafrechtlichen Verfolgung signifikant zu minimieren. Wie in allen rechtlichen Angelegenheiten ist es praktisch unmöglich, alle Regeln und Gesetze perfekt zu befolgen. Strafverfolgungsbehörden sind sich dessen bewusst und agieren in der Regel mit Augenmaß, solange sich betroffene Organisationen nicht bewusst und grundlos über geltende Regeln hinwegsetzen. (nb@ix.de)

Quellen

CIS Controls, EU-Verordnung und Informationen der Datenschutzkonferenz: ix.de/z689

JOHANN RABBOW

ist Head of Digital Forensics & Incident Response der Oneconsult Deutschland AG in München. Als IT-Forensiker und Volljurist unterstützt er Unternehmen bei der Bewältigung von Cyberangriffen.