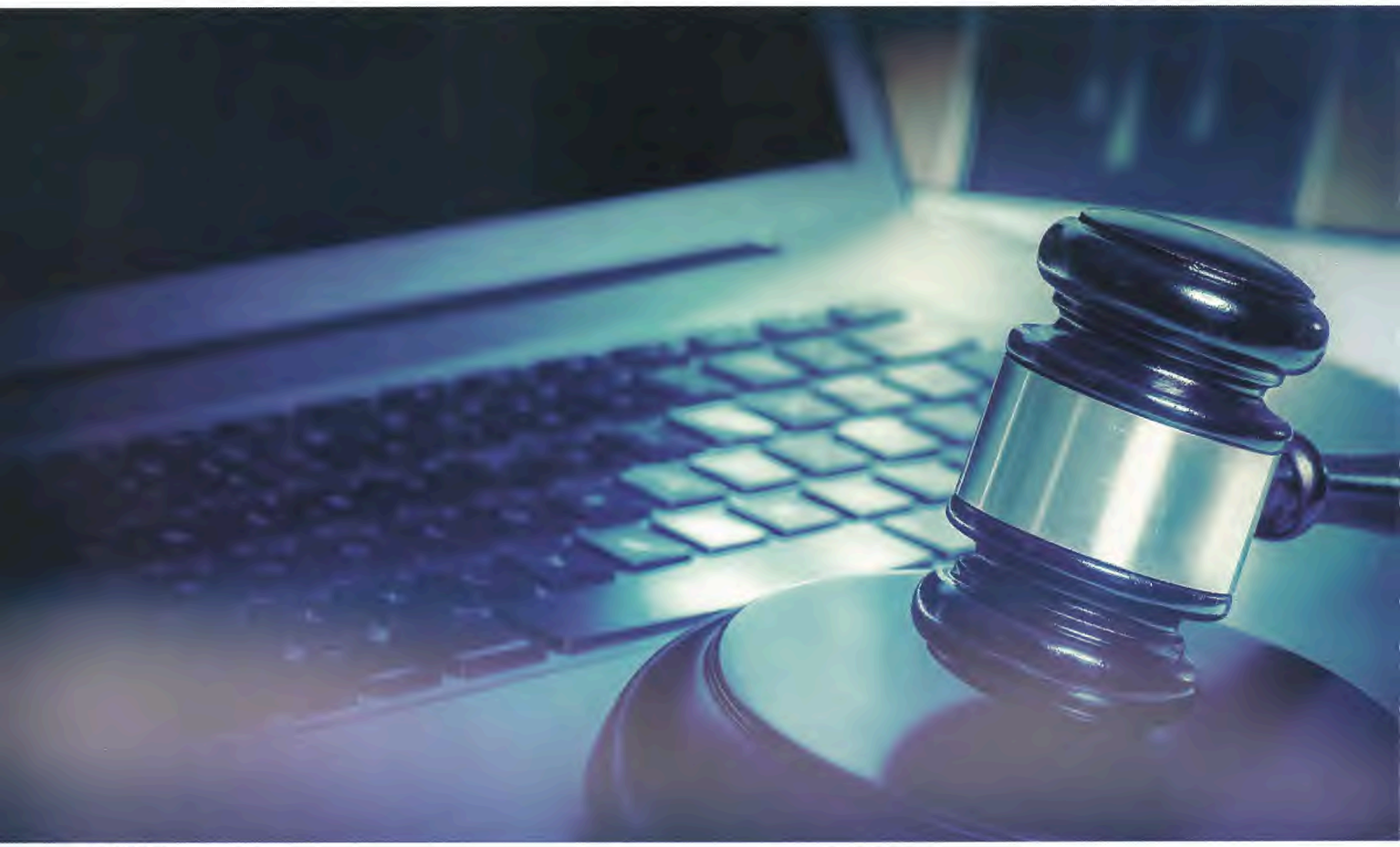

© iStockphoto

IM REGELFALL ÜBERRASCHEND

Axel Anderl, Managing Partner und Leiter des IT/IP- und Datenschutzteams sowie der Digital Industries Group, und Nino Tlapak, Partner im IT- und Datenschutzteam bei DORDA über aktuelle Entwicklungen und ihre praktische Erfahrung im Bereich Cybersecurity.

Die Digitalisierung betrifft alle Branchen und Bereiche – von der Produktion bis zur Administration. Welche Cyberrisiken gehen damit einher?

Nino Tlapak: Gerade am Beispiel der Industrie zeigt sich auch die Kehrseite der Digitalisierung: Während in der Vergangenheit die Produktionsbetriebe regelmäßig von Angriffen verschont wurden, ändert sich nunmehr das Bild dramatisch. Im Gegensatz zu Branchen wie Pharma, Banken oder Versicherungen war bei Industrieunternehmen die Abwehr potenzieller Cyberattacken bislang nicht im Fokus. Nun sind die Produktionsmaschinen aber dank der Digitalisierung im Netz miteinander verbunden und damit sind sie ebenso angreifbar wie z.B. Kraftwerke oder Ampelanlagen. Hacker suchen daher vermehrt auch in diesen Bereichen nach Schwachstellen im System und nutzen diese.

Axel Anderl: In der Praxis wurden die DDOS-Attacken de facto durch Ransomware-Angriffe abgelöst. DDOS-Attacken waren zwar auch unangenehm, aber mit überschaubarem Aufwand in den Griff zu bekommen. Anders ist die Situation bei Ransomware-Attacken: Hier dringt der Angreifer unbemerkt in das System ein und verschlüsselt alle Daten bzw. löscht diese. Gegen eine zumeist in Bitcoin zu zahlende Lösegeldsumme gibt er sie wieder frei. Oft stellt sich in der Nachbearbeitung des Vorfalls heraus, dass die Angreifer bereits über einen langen Zeitraum im System waren. Auslöser sind oft kleinere Nachlässigkeiten, wie ein falscher Klick einer Mitarbeiter:in oder fehlende Updates und Patches, die bereits bekannte Schwachstellen decken würden und so den Zugriff von außen verhindern. Diese sind auch DSGVO-relevant und so sind Verpflichtungen – wie die Meldepflicht – zu beachten.

Wie kann man sich darauf vorbereiten und das Unternehmen bestmöglich absichern?

Axel Anderl: Im Anlassfall selbst greifen faktisch – durch Vorgabe und Druck der Er-

© Natascha Unkart & Isabelle Köhler

Entscheidend ist, dass das Unternehmen auf den Anlassfall vorbereitet ist und damit richtig reagieren kann. Dafür braucht es entsprechende Awareness und Vorbereitung. Im Regelfall erfolgen Cyberattacken ja überraschend, über Nacht und/oder das Wochenende. Die gesetzlichen Meldefristen nehmen darauf keine Rücksicht.

Axel Anderl
Managing Partner und Leiter des IT/IP und Datenschutzteams sowie der Digital Industries Group bei DORDA

presser – und rechtlich sehr knappe Fristen. Um dann richtig und zeitgerecht reagieren zu können, braucht es eine entsprechende Vorbereitung auf den möglichen Ernstfall. So ist es erforderlich, dass vorab die Zuständigkeiten und Abläufe geklärt werden sowie auch ein festgelegtes Prozedere etabliert wird. Auch die Frage nach dem Pouvoir und Rahmenbedingungen kann vorab dem Grunde nach geklärt werden. Das alles sollte aber nicht im IT-System abgelegt, sondern offline verwaltet werden. Zum einen liest der Angreifer sonst mit und kennt die Abwehrstrategie und Zahlungsbereitschaft schon vorher. Zum anderen besteht sonst im Ernstfall kein Zugriff. Hat man das etabliert, ist man für den Ernstfall gewappnet und kann kurzfristig reagieren.

Nino Tlapak: Bei der Vorbereitung geht es vor allem auch um prozessuale und rechtliche Details: Wer muss wann kontaktiert werden, damit etwa Cyber-Versicherungen in Anspruch genommen werden können oder sichergestellt ist, dass die Datenschutzbehörde rasch und informiert in Kenntnis gesetzt wird? Wie wird das Krisenteam zusammengestellt und auf welche Eigenschaften müssen die Teilnehmer psychologisch (Stresssituation) und strategisch eingestellt sein? Damit man im Anlassfall nicht eiskalt überrascht wird, ist die Präventionsarbeit unumgänglich. Das richtige Verhalten im Anlassfall muss sodann auch in regelmäßigen Abständen geprüft und geübt werden.

Axel Anderl: Nur so ist es möglich, zum richtigen Zeitpunkt sowohl intern über Legal, Compliance und IT als auch mithilfe externer Experten – vom IT-Forensiker bis hin zur Krisen-PR – die Weichen zu stellen. Im Fall des Falles macht es auch Sinn, so genannte Negotiators beizuziehen, die entsprechende Erfahrung in Verhandlungen mit unterschiedlichen Hacker-Gruppen mitbringen. Letztendlich geht es auch darum abzuklären, ob Lösegeld überhaupt bezahlt werden darf (oder dies allenfalls strafbar sein kann) und auf welche Abwägungen es dabei ankommt.

Vorbereitung bedeutet neben technischen Einrichtungen vor allem auch die Schulung der Mitarbeiter ...

Nino Tlapak: Ja, die interne Kommunikation ist eine der wichtigsten Säulen für die nachgelagerte Kommunikation nach außen: Was soll und darf Kunden, Kollegen oder auch der Presse bei Anfragen wann geantwortet werden? Welche Informationen darf ich noch, aber welche sollte ich keinesfalls zurückhalten?

In der Prävention geht es genau darum, bei allen Mitarbeitern die erforderliche Awareness aufzubauen und zu sensibilisieren – was löst Angriffe aus und wie kann man das Risiko minimieren und wie ist im Anlassfall dann zu kommunizieren. Bei Cyberattacken ist mittlerweile nicht die Frage, ob, sondern wann man betroffen ist. Seit den Lockdowns und dem breiten Einsatz von Homeoffice ist dies noch deutlicher geworden: So resultiert oft aus der fehlenden örtlichen Bindung an das Unternehmen – ich sitze daheim am Küchentisch statt im Büro – ein fehlendes Bewusstsein für potenzielle Lücken und Gefahrenquellen. Was kann passieren, wenn ein Dienstlaptop in der Familie für Hausaufgaben oder Unterhaltung eingesetzt wird? Wo erledige ich meine Telefonate und Videokonferenzen? Wie gehe ich mit Ausdrucken um – landen die im normalen Altpapiercontainer im Innenhof der Wohnhausanlage?

Das sind konkrete Beispiele aus dem beruflichen Alltag, die schon Auslöser für Angriffe waren. Erfolgreiche Abwehr- und Präventionsmaßnahmen beginnen schon bei einfachen Dingen, wie dem richtigen Umgang mit privaten und beruflichen Passwörtern und enden bei der Implementierung komplexer IT-Sicherheits- und -Warnsysteme durch das Unternehmen. Doch selbst die beste Vorbereitung kann ein Eindringen eines Angreifers nicht zu 100 % ausschließen (z.B. gezielter und vorbereiteter CEO Fraud). Ein gut vorbereitetes Unternehmen kann aber auf einen etablierten Krisenplan zurückgreifen und sinnvolle Schritte setzen.

© DORDA

Gerade die Zunahme an Cyberattacken während der Corona-Pandemie hat gezeigt, dass die Präventionsarbeit das Um und Auf ist. Attacken lassen sich nicht ganz verhindern, das Risiko lässt sich aber signifikant senken. Ein gut vorbereitetes Unternehmen überwindet die Krisensituation auch schneller und kosteneffizienter.

Nino Tlapak
Partner im IT- und Datenschutzteam bei DORDA

Was muss das Unternehmen also dann im Anlassfall tun?

Axel Anderl: Neben der Evaluierung des Schadensausmaßes, der forensischen Aufarbeitung und dem Wiederaufbau der Technik geht es auch um die Einhaltung der anwendbaren rechtlichen Vorgaben und Fristen, um Schadenersatzansprüche, Strafen und Rufschädigung hintanzuhalten. Allen voran ist die Datenschutzbehörde binnen 72 Stunden zu informieren – je nach Branche können aber auch weitere Behörden ähnlich rasch einzubinden sein. Daneben kommt es auf die Kommunikation mit der Versicherung und den Strafverfolgungsbehörden an. Für alle Bereiche und insbesondere die Frage der (persönlichen) Haftung gilt: Eine saubere Dokumentation und laufende Abstimmung mit Experten ist der Schlüssel zum Erfolg. ■

MARTIN MÜHL