Was der Cyber-Vorstand leisten sollte

Über Aufgaben, Pflichten und Haftung einer neuen Position – Angriff auf das eigene Unternehmen ist keine Frage des Ob, sondern nur noch des Wann

Von Kristina Schreiber und Eren Basar *)

Börsen-Zeitung, 22.4.2023

Der Digitalisierungsschub der letzten drei Jahre hat die Grundlage zu mehr Cyberangriffen gelegt. Börsengeführte Unternehmen sind ebenso betroffen wie Banken und der Mittelstand. Hacker greifen Unternehmen jeder Branche an. Cybersecurity ist längst Managementaufgabe: der Cybervorstand – eine neue Position mit IT-Verständnis.

Auf den ersten Blick scheint die Aufgabe klar: finanzielle und reputative Schäden für das Unternehmen verhindern und persönliche Haftung reduzieren. Denn die müssen Vorstände, Aufsichtsräte, Management Board und Geschäftsführung fürchten, wenn es zu einer Cyberattacke kommt. Die Challenge ist, schnell und professionell zu reagieren, wenn der Angriff passiert.

Aber: Ist in Unternehmen die benötigte Kompetenz zur Herstellung der Informationssicherheit vorhanden? Unsere Erfahrung zeigt, dass noch Lücken klaffen. Oft werden Führungspersonen mit dieser Aufgabe betraut, die schon andere Bereiche verantworten. In der Regel stecken sie zu wenig in der Materie. Sie bewerten Risiken falsch und haben zu wenig Sensibilität für die rechtlichen Auswirkungen von Cyberrisiken. Woher auch? Das Thema ist neu, die Risiken sind enorm. Die persönliche Verantwortung von Cybervorständen wiegt schwer.

Imageschäden und Klagen drohen

Neben Erfolgen, die Unternehmen durch die Digitalisierung erzielen, macht ebendiese Digitalisierung Unternehmen auch verwundbarer. Wenn Systeme ausfallen, infiltriert werden oder es zum Datendiebstahl kommt, drohen Imageschäden und Schadenersatzklagen. Am schlimmsten ist es, wenn Unternehmen lahmgelegt werden. In manchen Branchen, wie z. B. im Notfallwesen, können sogar Leben auf dem Spiel stehen. Auf jeden Fall laufen die Kosten mit jeder Minute weiter und reißen tiefe ökonomische Löcher.

Auf Vorstandsebene allerdings werden die Folgen des Ausfallrisikos noch zu wenig wahrgenommen. Immer noch glauben viele, eine Cyberattacke betreffe nur die anderen. Doch laut Spezialisten ist der Cyberangriff auf das eigene Unternehmen keine Frage des Ob, sondern nur noch des Wann. Der Fokus auf Cybersicherheit ist heute eine zentrale Aufgabe für den Vorstand zur Steuerung des strategischen Unternehmensrisikos.

Chefsache Cybersicherheit

Wer IT-Prozesse steuern will, muss selbst kein Informatiker sein. Allerdings muss er die Bereitschaft mitbringen, sich die Kompetenz zur Erstellung, Bewertung und Verbesserung eines Informations-Sicherheits-Management-Systems (ISMS) anzueignen. Wenn man so will, muss sich der Vorstand auf Stufe 1 das notwendige Know-how erst noch erarbeiten. Sie bietet die Grundlage, sensibilisiert und zeigt Möglichkeiten für neuralgische Punkte im Unternehmen auf. Damit ist auf Stufe 2 eine zielgerichtete und wirkungsvolle Delegation der zu erfüllenden Aufgaben an Spezialisten in den Bereichen Informationssicherheit, Datenschutz und Compliance möglich.

Stufe 3 lenkt den Blick auf das Unternehmen insgesamt und seine Belegschaft: Ein wesentlicher Faktor für Cybersicherheit ist die Achtsamkeit im Team. Die meisten Hacker gelangen auf internen Wegen auf die Systeme.

Beispiele sind der berühmte arglose Klick auf eine nicht erkannte Phishing-Mail oder auch das zielgerichtete Öffnen digitaler Türen durch (unzufriedene oder abwanderungswillige) Mitarbeiter. Angriffe erfolgen also entweder über Mitarbeiter oder über technische Sicherheitslücken. An beiden Themenfeldern lässt sich hervorragend arbeiten.

Bei der Etablierung der Prozesse muss der Cybervorstand die Datenschutz-Compliance und IT-Sicherheit des Unternehmens fit machen. Die Datenschutz-Grundverordnung (DSGVO) verlangt eine angemessene Datensicherheit. Einmal im Jahr gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) das sogenannte Grundschutz-Kompendium mit Bausteinen zur Umsetzung eines Informations-Sicherheits-Management-Systems (ISMS) auf.

Behandelt werden alle Gefährdungen wie z. B. Schadprogramme, Denial-of-Service-Angriffe, Datenverlust, Sabotage, unberechtigte oder fehlerhafte Nutzung von Geräten und Systemen, Manipulationen von Geräten und Informationen, Softwareschwachstellen, Identitätsdiebstahl, Ressourcenmangel und Missbrauch von Berechtigungen. Das Kompendium enthält auch eine Liste zur Priorisierung der empfohlenen Maßnahmen. Alternativ kann auf die ISO-Norm 27001 zurückgegriffen werden. Die Erfüllung eines dieser Standards ist die erste Säule eines professionellen Cybermanagements.

Technische Vorkehrungen

Wichtig ist aber, dass neben den organisatorischen Maßnahmen auch eine Vorbereitung auf technischer Ebene erfolgt, die zweite Säule: Cyberverteidigung. Hier bieten Dienstleister mittlerweile eine externe 24/7-Überwachung der IT an. Begleitet werden muss diese Maßnahme durch ein Notfallkonzept, das vor allem die Wiederherstellung der IT für den Fall eines erfolgreichen Incidents anstrebt. Das ist auch zentrales Element für die Umsetzung der ESG-Anforderungen, die in ihrem dritten Element, der Governance, solche Vorkehrungen fordern.

Diese Aufstellung gibt dem Cybervorstand und dem Unternehmen einen optimierten Schutz. Schließlich sichert die Etablierung der IT-Compliance auch die Möglichkeit der Versicherung von Angriffen aller Art ab. Versicherer fordern meist zumindest ein etabliertes Sicherheitskonzept, das Früherkennung, Richtlinien und personelle Ressourcen beinhaltet.

Kommt es zu einem Cybervorfall, muss der erste Schritt in der technischen Verteidigung und forensischen Aufbereitung der Cyberattacke liegen. Der Cybervorstand muss schnell sein und ein Team aus IT-Sicherheitsexperten und (externen) Forensikern vorhalten.

Binnen 72 Stunden muss dann in aller Regel die Datenschutzaufsichtsbehörde über den Vorfall informiert werden: Dieser Schritt ist meist die erste offizielle Außenkommunikation. Durch sie werden die Weichen gestellt für sich potenziell anschließende Bußgeld- und Schadenersatzrisiken, die sich bereits aus der Formulierung der Schadensmeldung ergeben können. Betroffene und die Allgemeinheit sind häufig ebenfalls zu informieren. Die Krisen-Kommunikationsstrategie leitet der Cybervorstand.

Handling des Ernstfalls

Das regulatorische Umfeld zur Gewährleistung von Cybersicherheit wächst. Es nimmt Unternehmen straf- und bußgeldrechtlich in die Pflicht. Im Haftungsregime der Datenschutz-Grundverordnung folgt das direkt aus Art. 32 DSGVO. Angesichts der Komplexität technischer Systeme steuert man schnell vom Bußgeldverfahren in ein Strafverfahren. Nahezu jedes Gesetz sieht zur Pflichtensicherung Sanktionsvorschriften vor. Schnell kann dann die Grenze zur Kriminalstrafe überschritten werden.

Das besonders dann, wenn der unberechtigte Zugriff auf Daten, die Umgehung von Sicherungsmaßnahmen, die Veränderung von Daten und der Eingriff in digitale Kommunikation im Raum stehen (§§ 202a, 202b, 202c, 303a, 303b StGB). Unternehmen können sich zwar selbst nicht strafbar machen, aber sie können für Verstöße von Organen und Aufsichtspflichtverletzung gegenüber Mitarbeitern nach dem Gesetz über Ordnungswidrigkeiten (OWiG) haftbar gemacht werden. Es besteht also die Verpflichtung, die erforderlichen, zumutbaren Aufsichtsmaßnahmen zu ergreifen, um Verletzungen der Cybersicherheit gar nicht erst entstehen zu lassen.

Vorbereitung ist zwingend

Die Entwicklung zeigt: Nur wenn eine Sicherheitsstrategie und ein Maßnahmenpaket vorliegen, kann der Cybervorstand das Unternehmen wirksam schützen. Die wichtigsten Elemente sind:

1. Wissen: Cybervorstände müssen wissen, worum es geht und welche Prozesse benötigt werden. Trainings und externe Unterstützung helfen, die Pflichten aller Beteiligter angemessen zu strukturieren und zielgerichtet umzusetzen.
2. Strukturieren: Das Unternehmen muss intern auf den Notfall vorbereitet werden. Hier helfen das Know-how von Experten und als erster Schritt auch Checklisten der Behörden.
3. Handeln: Im Ernstfall muss schnell gehandelt werden. An erster Stelle stehen technische Verteidigung und forensische Aufarbeitung, um weiteren Schaden zu verhindern. Oft ist das Herunterfahren aller Systeme der Beginn einer erfolgreichen Aufbereitung. Fortgesetzt wird sie mit einer in der Gesamtstrategie abgestimmten Kommunikation gegenüber Behörden, Betroffenen und auch der Allgemeinheit.

*) **Dr. Kristina Schreiber ist Partnerin von Loschelder Rechtsanwälte in Köln und Dr. Eren Basar Partner von Wessing & Partner Rechtsanwälte in Düsseldorf.**

IM INTERVIEW: HANS-MICHAEL WOLFFGANG

Anti-Dumping-Zölle können die Kalkulation von Importeuren zum Platzen bringen

Der AWB-Partner zu den Risiken eines Schutzmechanismus für europäische Unternehmen

Börsen-Zeitung, 22.4.2023


Hans-Michael Wolffgang

▪ Herr Wolffgang, mit Anti-Dumping-Zöllen will die EU europäische Unternehmen vor unfairen Wettbewerbern schützen, die ihre Produkte zu künstlich niedrigen Preisen anbieten, etwa weil sie stark subventioniert sind. Welche Auswirkungen ergeben sich für Firmen, die solche Waren beziehen?

Der Import von Waren, die unter die Anti-Dumping-Regelungen der EU fallen, kann für Unternehmen sehr teuer werden. Ein großes Risiko sind dabei die immensen Preisspannen von 4 bis existenzbedrohlichen 100 Prozentpunkten oder mehr über den regulären Zöllen. Das bringt die Kalkulation von Importeuren zum Platzen. Dazu kommt die Gefahr von sogenannten Nacherhebungen, die Firmen noch bis zu drei Jahre nach der Einfuhr entsprechender Waren treffen können. Bei Fehlern in der Warenbezeichnung, der Zolltarifposition, dem Ursprung oder bei Umgehungstransporten sind in schweren Fällen Millionensummen zu zahlen. Neben den finanziellen Risiken kommen dann die Vorwürfe eines möglicherweise strafbaren Verhaltens hinzu, neben strafrechtlichen Ermittlungen und Anklagen sind dann Nachforderungen bis zu zehn Jahre lang zulässig.

▪ Wie werden die Anti-Dumping-Zölle festgelegt?

Anti-Dumping-Zölle werden zusätzlich zu den regulären Einfuhrabgaben erhoben. Die Höhe von Anti-Dumping-Zöllen richtet sich nach einer Vielzahl von einzelnen Verordnungen der EU, die anhand von Warenbeschreibungen, tariflichen Codenummern, Ursprungsland und Hersteller die Zollsätze nach Gewicht, Stück oder Prozentsatz des Warenwerts festlegen. Richtig teuer wird es beispielsweise gerade bei Importen aus China mit Zollsätzen von knapp 70% bei Keramikfliesen oder 90% bei Eisen- und Stahlrohren. Keramikfliesen aus Indien sind mit Zollsätzen unter 10% im Vergleich günstig.

▪ Welche Warengruppen sind betroffen?

Von Anti-Dumping-Zöllen werden Produkte quer durch den Warenkatalog betroffen. Das beginnt bei A wie Aluminium und reicht bis Z wie Zuckermais. Dazwischen sind Erzeugnisse aus Glasfasern, Garne aus Polyester, Luftreifen für Lkw, Stahlerzeugnisse oder Windkraftanlagen. Die Maßnahmen sind immer gegen Produkte mit Ursprung in bestimmten Ländern gerichtet, sehr häufig ist es China. Aktuell unterliegen viele Fahrradteile aus verschiedensten Ländern den Zöllen.

▪ Ist die Zollfestsetzung für Außenstehende transparent?

Grundsätzlich ja, da die Anti-Dumping-Zollsätze im elektronischen Zolltarif auf der Homepage der Zollverwaltung frei zugänglich sind. Allerdings können sich Unternehmen nicht abschließend auf die Zolltarifposition verlassen, denn laut EuGH-Rechtsprechung kommt es auf die Beschreibung der Ware in der Anti-Dumping-Verordnung an. Diese kann von der im Zolltarif erfassten Ware abweichen - sowohl zum Vorteil des Einführers als auch zum Nachteil.

▪ Wie sollten Unternehmen mit der Unsicherheit im Importgeschäft umgehen?

Intensive Vorbereitungen sind für Unternehmen bares Geld wert. Bei Importgeschäften mit sensiblen Gütern oder Ländern sollten die Anti-Dumping-Maßnahmen früh geprüft und laufend überwacht werden. Verbindliche Auskünfte über die tarifliche Codenummer oder den Waren-Ursprung sind bereits vor der Einfuhr einzuholen. Auch über die eigene Lieferkette sollten Firmen bestens Bescheid wissen, hier helfen Zertifikate aus unabhängigen Prüfbüros. Die EU-Kommission muss ein umfangreiches Untersuchungsverfahren durchführen, bevor sie Anti-Dumping-Zölle erhebt. Eine Beteiligung hieran kann sich für betroffene Unternehmen lohnen, denn für die freiwillige Mitwirkung sind günstigere Zollsätze für manche Hersteller möglich.

▪ Wie können sich Betriebe vor Überraschungen schützen?

Die große Tücke bei Anti-Dumping-Zöllen ist, dass sie verschuldensunabhängig erhoben werden. Selbst Unternehmen, die alle Sorgfaltspflichten einhalten und Opfer eines Betrugsfalls werden, beispielsweise in der Lieferkette, müssen zahlen. Ein 100-Prozent-Schutz ist nicht möglich. Allerdings können die Importeure die Risiken minimieren, indem sie Eigenschaften und Ursprung der Waren eindeutig bestimmen, Lieferquellen mit Bedacht auswählen, diese genau dokumentieren und unabhängige Prüfungsstellen beauftragen.

Prof. Dr. Hans-Michael Wolffgang ist Gründungspartner und Steuerberater von AWB. Die Fragen stellte Helmut Kipp.

MANDATE UND MANDANTEN

Gleiss Lutz unterstützt den Modediscounter Takko Fashion bei der finanziellen Restrukturierung mit Dr. Andreas Spahlinger, Dr. Christian Hàlasz und Friedrich Schlott.

Luther steht dem Windturbinenhersteller Nordex bei einer grünen Wandelanleihe über 333 Mill. Euro mit Dr. Jörgen Tielmann zur Seite. Für das Bankenkonsortium ist **Clifford Chance** mit Dr. George Hacket und Dr. Dominik Heß in die Emission eingebunden.

Taylor Wessing berät den Insolvenzverwalter bei der Veräußerung des Flughafens Frankfurt-Hahn an den Trierer Immobilienentwickler Triwo mit Hendrik Boss.

Freshfields Bruckhaus Deringer ist vom E-Commerce-Aggregator Razor Group für den Erwerb von The Stryze Group sowie für eine Series-C-Finanzierungsrunde mit Dr. Lars Meyer und Dr. Michael Josenhans mandatiert.

Reed Smith begleitet den Anbieter von Kommunikations- und Informationssystemen Frequentis bei der Akquisition von Frafos mit Constantin Conrads.

Allen & Overy arbeitet für Bencis Capital Partners beim Erwerb der Heytex-Gruppe mit Dr. Alexander Veith, Linda Mayer und Thomas Neubaum.

Hengeler Mueller ist für den Europipe-Gesellschafter Salzgitter in den Verkauf der US-Tochter Berg Pipe, einen Hersteller von Stahlrohren, an Borusan Mannesmann mit Dr. Simon Patrick Link und Alexander Bekier involviert.

Gibson, Dunn & Crutcher berät den Finanzinvestor Triton beim Erwerb von Arrowhead Industries mit Dr. Wilhelm Reinhardt und Dr. Dennis Seifarth.

Heuking Kühn Lüer Wojtek ist für HL Display bei der Übernahme der Displayunternehmen Oechsle und Werba mit Dr. Pär Johansson und Dr. Philipp Jansen tätig.

Dentons unterstützt das Food-Start-up KoRo bei einer Finanzierung mit Thomas Schubert. **SZA Schilling, Zutt & Anschütz** steht dem Investor SevenVentures mit Dr. Oliver Schröder zur Seite.

Rödl & Partner arbeitet für Viessmann bei der strategischen Partnerschaft mit der spanischen Industriegruppe Keyter Technologies mit Jochen Reis.

Willkie Farr & Gallagher begleitet Adiuva Capital bei einer strategischen Kapitalerhöhung für die Sanecum Gruppe mit Dr. Maximilian Schwab und Miriam Steets.

Latham & Watkins berät das Pharmaunternehmen Grünenthal bei der Emission einer Anleihe über 300 Mill. Euro mit Dr. Rüdiger Malaun und Dr. Alexander Lentz.

Oppenhoff unterstützt EIC Fund, den Sonderfonds des Europäischen Innovationsrates, beim Investment in das Startup Enote mit Dr. Peter Etzbach.

Weiterer Beiträge zu Recht & Kapitalmarkt unter www.boersen-zeitung.de/recht-kapitalmarkt

Redaktion:
Sabine Wadewitz (069/2732-212)
Helmut Kipp (069/2732-213)
recht@boersen-zeitung.de