Pressemeldung

Verband der Digitalwirtschaft Berlin-Brandenburg e.V.

Hacker weg, Haftung bleibt

Warum KMU nach einem Cyberangriff vor allem rechtlich unter Druck geraten

Zum European Cybersecurity Month (ECSM) zeigt der SIBB anhand realer Fälle, was KMU nach einem Cyberangriff beachten müssen

Berlin, 19. Oktober 2026 – Der Geschäftsführer öffnet müde seinen Laptop und schreckt auf. Statt des gewohnten Startbildschirms erscheint eine Lösegeldforderung. Die zentralen Kunden-, Firmen und Bewerberdaten wurden verschlüsselt. Die Angreifer drohen, die sensiblen Daten zu veröffentlichen.

Pressekontakt
Clemens Glade
Tel. +49 171 8387225
clemens@sibb.de

Im Unternehmen klingeln ununterbrochen die Telefone. Die besorgten Mitarbeitenden können nicht arbeiten, Kunden warten verärgert auf Antworten. Niemand weiß, ob tatsächlich Daten abgeflossen sind. Es müssen sofort Entscheidungen getroffen werden: Welche Systeme müssen vom Netz? Welche Spuren dürfen nicht gelöscht werden? Müssen Behörden, Versicherer oder Kunden informiert werden?

Mit dem Angriff beginnt eine zweite Krise

Dieser anonymisierte Fall aus der anwaltlichen Praxis zeigt: Ein Cyberangriff ist nicht nur ein technischer Notfall. Während die IT um die Systeme kämpft, beginnt für die Unternehmensleitung eine zweite Krise – mit rechtlichen Fristen, Haftungsfragen und hohem Entscheidungsdruck.

Anlässlich des ECSM im Oktober rückt der SIBB e. V. deshalb die rechtliche Seite von Cyberangriffen in den Mittelpunkt. Ein unbequemes Thema, das viele Unternehmen gern aufschieben. Im Ernstfall fehlt dafür jedoch die Zeit.

„Die größte Wissenslücke liegt häufig nicht in der Prävention, sondern in der Frage: Was muss ich in den ersten 72 Stunden nach einem Vorfall konkret tun?“, sagt Daniel Schätzle, Rechtsanwalt für IT-Sicherheitsrecht bei HÄRTING Rechtsanwälte. „Die ersten 72 Stunden sind kein Zeitraum für improvisierte Einzelentscheidungen. Unternehmen brauchen einen vorher festgelegten Ablauf mit klaren Verantwortlichkeiten.“

Gerade kleine und mittlere Unternehmen stehen vor einer enormen Herausforderung: Sie müssen steigende regulatorische Anforderungen erfüllen, verfügen aber häufig weder über ein eigenes Security-Team noch über spezialisierte juristische Ressourcen.

Sind personenbezogene Daten betroffen, kann eine Meldung an die Datenschutzaufsichtsbehörde erforderlich sein. Dafür gilt grundsätzlich eine Frist von 72 Stunden, nachdem die Verletzung bekannt geworden ist. Zu diesem Zeitpunkt ist oft noch unklar, was genau

SIBB e.V.
Verband der Digitalwirtschaft Berlin-Brandenburg

www.sibb.de

Büro Berlin
Friedrichstraße 68
Mindspace im Quartier 205
10117 Berlin

Büro Brandenburg
Konrad-Zuse-Ring 12b
14469 Potsdam

Geschäftsführer: Sinan Arslan

Vereinsregister: Amtsgericht Charlottenburg Berlin, VR 15412 B

passiert ist. Umso wichtiger ist es, Erkenntnisse, Risikobewertungen und Entscheidungen von Beginn an zu dokumentieren.

Eine manipulierte Rechnung – und das Geld ist weg

Ein zweiter Praxisfall beginnt unauffälliger. Auf bislang ungeklärtem Weg gelangen Angreifer in die E-Mail-Konten eines Unternehmens und lesen mit. Als eine größere Rechnung verschickt wird, verändern sie die Bankverbindung. Das Geld landet bei den Tätern. Der Betrug fällt erst auf, als der eigentliche Empfänger nach der Zahlung fragt.

Im Nachgang geht es nicht nur um die technische Ursache: Waren Zugänge durch Mehrfaktor-Authentifizierung geschützt? Mussten neue Bankverbindungen auf einem zweiten Kommunikationsweg bestätigt werden? Und war geregelt, wie IT-Dienstleister im Ernstfall unterstützen?

Auch vorschnelles Handeln kann den Schaden vergrößern. Werden Systeme sofort gelöscht oder neu aufgesetzt, gehen möglicherweise wichtige Spuren für Aufklärung, Versicherung und rechtliche Schritte verloren. „Ein Unternehmen muss in den ersten Stunden nicht alles wissen“, erklärt Schätzle. „Es muss aber zeigen können, dass es strukturiert, risikobasiert und nachvollziehbar gehandelt hat.“

„Den Ernstfall sollte man regelmäßig mit Mitarbeitenden und Dienstleistern durchspielen“, ergänzt Andrea Hornung, Director Cybersecurity & Innovation beim SIBB e. V. „Erst in der Übung zeigt sich, wo es hakt: eine fehlende Telefonnummer, eine unklare Freigabe, ein Plan, der nur auf dem Firmenserver liegt. Diese Lücken lassen sich dann in Ruhe schließen und nicht erst nach dem Angriff unter Druck. Im Krisenmodus funktioniert nur, was vorher trainiert wurde.“

Der SIBB unterstützt Unternehmen gemeinsam mit seinem Netzwerk und als Partner des **EDIH pro_digital** u.a. dabei, Sicherheitsrisiken zu bewerten und ihre digitale Resilienz zu stärken.
https://www.edihprodigital.eu/de

Über den SIBB e.V.

Der SIBB e. V. ist seit 35 Jahren der Verband der digitalen Wirtschaft in Berlin und Brandenburg. Rund 200 Mitglieder mit über 10.500 Beschäftigten stehen für technologischen Fortschritt und engagieren sich für eine lebenswerte digitale Zukunft. Bereits seit 1992 vernetzt der Verband Tech-Unternehmen, Startups und Forschung, fördert Innovationen und begleitet Gründerinnen und Gründer.
www.sibb.de

Hilfe im Cybernotfall

- notfallhilfe.transferstelle-cybersicherheit.de/
  Kostenlose digitale Ersteinschätzung mit allgemeinen Handlungsempfehlungen sowie Suche nach Fachleuten für Incident Response, Datenrettung, Datenschutz und

Verband der Digitalwirtschaft Berlin-Brandenburg e.V.

Krisenkommunikation. Die anschließenden Dienstleistungen können kostenpflichtig sein.

- digitalagentur.berlin
  Kostenlose und auf Wunsch anonyme Ersthilfe für Berliner Unternehmen unter **0800 360 30 60**, Montag bis Freitag von 9 bis 17 Uhr. Sie vermittelt bei Bedarf spezialisierte IT-Sicherheitsunternehmen.
- www.bsi.bund.de
  Organisatorische und technische Checklisten, Ransomware-Erste-Hilfe, IT-Notfallkarte, Hinweise zu Meldepflichten und qualifizierten Dienstleistern.

Mitglieder des SIBB, die sich mit Cybersecurity beschäftigen

- **O&O Software:** https://www.oo-software.com
- **Office Company:** https://www.office-company.de
- **M&H IT-Security (Berlin):** https://mh-it-security.de
- **Pÿur Business:** https://www.pyur.com/en/business/solutions/it-security.html
- **SHD System-Haus-Dresden:** https://www.shd-online.de
- **Xopero:** https://www.xopero.com
- **CCVossel:** https://www.ccvossel.de
- **Quirso:** https://www.quirso.de
- **PID1:** https://www.pid1.tech
- **Digital Trust Analytics:** https://www.digitaltrust.de
- **e*message:** https://www.emessage.de
- **Kroker Legal:** https://kroker.legal
- **Härting:** https://haerting.de
- **Derdack:** https://www.derdack.com/
- **NordSecurity:** https://nordsecurity.com
- **nenna.ai:** https://www.nenna.ai

Netzwerk, Managed IT und sichere Architektur: Pÿur Business, Office Company, SHD, PID1
Detection, Response und Pentests: CCVossel, Quirso
Beratung, Compliance und Training: M&H IT-Security, Digital Trust Analytics, CCVossel, Office Company
Recht und Datenschutz (inkl. KI-Datenschutz): Härting, Kroker Legal, nenna.ai
Datensicherung und Recovery: Xopero, O&O Software
Privacy- und Zugriffs-Tools: NordSecurity
Randbereiche (Alarmierung, sichere Entwicklung): e*message, Derdack.

Wünschen Sie ausführliche Informationen zu den genannten Fällen, schreiben Sie gern eine Mail an clemens@sibb.de