»AR1431382

Cybersicherheit 2023 – Schwachstelle bleibt der Mensch

Philipp von Bülow

In ihrer Verantwortung, Schaden vom Unternehmen abzuwenden, werden Aufsichtsräte immer öfter mit dem Thema IT-Sicherheit konfrontiert. Sie sollten Impulse geben, um für das Thema zu sensibilisieren und eine IT-Security-Strategie zu etablieren, die mit der Weiterbildung der Mitarbeitenden beginnt.

Laut „Bericht zur Lage der IT-Sicherheit in Deutschland 2022", herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik (BSI), ist die aktuelle Bedrohung durch Cyber-Angriffe für Unternehmen so hoch wie nie zuvor. Der Branchenverband der deutschen Informations- und Telekommunikationsbranche (Bitkom e.V.) stellt fest, dass im letzten Jahr in mehr als jedem zweiten Unternehmen sensible Daten gestohlen, digitale Kommunikation ausgespäht oder Systeme und Betriebsabläufe sabotiert wurden. Den durch Angriffe auf die IT-Infrastruktur entstehenden Schaden beziffert Bitkom auf mehr als 200 Mrd. € pro Jahr.

In rechtlich fundierten Online-Schulungen lernen Mitarbeitende, Cyber-Angriffe frühzeitig zu erkennen – sowohl den Versuch, Malware zu übertragen als auch Symptome einer Infizierung des Systems. Idealerweise verstehen sie so, wie Cyber-Kriminelle denken und handeln, erkennen Social Engineering, Phishing und andere Methoden und wissen, wie sie präventiv und kurativ handeln müssen. In diesem Sinne schlussfolgert auch das BSI: „Für alle Institutionen sollten die umfassende und kontinuierliche Schulung aller Mitarbeiter zum Thema Informationssicherheit (Erhöhung der Aufmerksamkeit) […] selbstverständlich sein."

Als Hauptbedrohung erachten Experten des BSI Ransomware: Schadsoftware, die in ein Netzwerk eindringt, dort gespeicherte Daten verschlüsselt und erst nach Zahlung eines Lösegelds wieder freigibt. Beim „Big Game Hunting" nehmen professionell organisierte Cyber-Kriminelle umsatzstarke Unternehmen ins Visier. Neben der Lösegeldsteht hier die Schweigegeldforderung: Betroffenen wird angedroht, bei Bekanntwerden des Angriffs sensible Daten zu veröffentlichen. Laut BSI erzielen die Angreifer mit der Kombination beider Methoden inzwischen Zahlungen im sechsstelligen Bereich.

Für Betroffene nicht weniger dramatisch ist die Gefahr durch Cyber-Sabotage-Angriffe oder neue Formen wie den Hacktivismus, bei dem politisch oder ideologisch motivierte Akteure mit Distributed Denial-of-Service-Angriffen (DDoS-Angriffe) den Zugriff auf Internetdienste unterbrechen.

Dass Schadprogramme wie Ransomware, Bots oder Trojaner eindringen und oftmals über längere Zeit unbemerkt arbeiten können, ist in der überwiegenden Mehrheit aller Fälle ein Resultat menschlichen Fehlverhaltens. Cyber-Kriminelle verbreiten Malware über vermeintlich harmlose E-Mail-Anhänge, über Links zu infizierten oder gefälschten Websites oder durch manipulierte Software. Beim Phishing gelangen Cyber-Kriminelle durch auf den ersten Blick vertrauenswürdige Mails, Webseiten oder Instant Messages an Login-Daten. Hierdurch können Kriminelle auf Unternehmensdaten zugreifen, Malware im Netzwerk verbreiten oder die so erbeuteten Daten für weitere, noch glaubwürdigere Phishing-Attacken einsetzen. Diese Schadprogramme ändern sich in immer höherer Geschwindigkeit und machen es selbst professioneller Anti-Viren-Software schwer, sie auf Anhieb zu erkennen. Laut BSI gibt es pro Tag mehr als 300.000 neue Varianten. Die einzige Möglichkeit, sich zu schützen, ist der Aufbau von Cyber-Resilienz, also der Widerstandsfähigkeit gegenüber Cyber-Attacken und ihren Auswirkungen.

Technische Systeme müssen durch Updates dauerhaft auf dem neuesten Stand sein. Wo dies nicht in der Verantwortung einer eigenen IT-Abteilung oder eines Dienstleisters steht, müssen Mitarbeitende dringend sensibilisiert werden. Gleiches gilt für die Gefahren durch E-Mail-Anhänge, Links und Social Engineering: Nur wenn auf allen Unternehmensebenen ein Bewusstsein für die Gefahren existiert, können Maßnahmen umgesetzt werden, die vor ihnen schützen. Laut der Umfrage einer deutschen Personalberatung sehen Entscheider in Unternehmen zu 71% das größte Risiko in der Unaufmerksamkeit ihrer Mitarbeitenden. Für Mitarbeitende als „einfache" Anwender sollte aber auch die erforderliche Kompetenz nicht immer vorausgesetzt werden.

Für den Aufsichtsrat ist es eine zentrale Aufgabe, im Rahmen der Mitwirkung an der Entwicklung einer IT-Sicherheitsstrategie den Faktor Mensch einzubeziehen, zu betonen und beide Seiten – Geschäftsleitung und Belegschaft – von der dringenden Notwendigkeit der intensiven Schulung aller Mitarbeitenden zu überzeugen.

Literaturhinweise:

- BSI, Lage der IT-Sicherheit in Deutschland 2022, s.u. https://fmos.link/19097.
- Bitkom, PM vom 31.08.2022, s.u. https://fmos.link/19098.
- Rochus Mummert, PM vom 09.04.2019, s.u. https://fmos.link/19099.

Autor:
Philipp von Bülow ist Geschäftsführer bei lawpilots GmbH in Berlin.

METATAGS: zeitschrift_AR; ressort_STI; doctype_au; SiriusID_1431382; RawID_0; angelegt_20230223;