LUBECA CYBER SHIELD

Schutz vor
den Folgen von
Cyberkriminalität und
anderen Angriffen aus dem Netz

Risiken im Umgang mit digitalen Daten

Unsere Infrastruktur haben wir in hohem Maß von der Verwaltung digitaler Daten abhängig gemacht - und fördern diese Abhängigkeit weiter. Der Komfort, den wir damit erreichen ist enorm, aber es ergibt sich auch ein Risiko, nämlich dann, wenn das System beschädigt wird. Unsere digitale Welt ist anfällig für Fehler, aber auch für Angriffe.
Schäden in Zusammenhang mit digitalen Daten werden als Cyberschäden bezeichnet. Sie entstehen aus unterschiedlichen Gründen:

- **Erpressungsversuche** z.B. durch Verschlüsselung
- **Hackerangriffe**
- **Datenverlust**
- **Verstöße gegen die DSGVO**
- **Phishing**
- **Malware**

Gegen wirtschaftliche Ausfälle und Schäden aus Angriffen auf die digitale Infrastruktur von Unternehmen schützt unsere Cyberversicherung. Sie ersetzt Ausfälle und begleitet die Schadenabwicklung.

Eine Cyberversicherung hilft

Das Risiko Opfer eines Angriffes oder eines anderen Cyber-Schadens im Verlauf eines Jahres zu werden, liegt für Unternehmen bei gut 50 %. Es gibt 3 Ansatzpunkte, die in ihrer Gesamtheit das Unternehmen schützen:

Prävention
Es ist kaum möglich, sich gegen jede Form von Angriffen zu schützen. Wir nutzen aber Statistiken, um die für Ihr Unternehmen relevanten Risiken zu identifizieren und so eine gezielte Vorsorge zu treffen.

Assistance
Wir helfen bei der Vorsorge aber auch im Schadenfall, sei es ein Erpressungsversuch oder der Verlust von Daten. Unser Ziel ist es, den Schaden so gering wie möglich zu halten. Damit ziehen wir gemeinsam mit Ihnen am gleichen Strang, denn jeder Cyberschaden hat erst einmal schwer vorherzusehende Konsequenzen, die es zu begrenzen gilt.

Schadenregulierung
Der Schaden, der nach aller Prävention und aller Kooperation verbleibt, mitsamt seinen Kollateralschäden, muss benannt und begründet werden. Dabei helfen wir um eine zügige Regulierung zu erreichen.

Die Cyber-Versicherung sollte heutzutage als die wichtigste Versicherung gleich nach der Haftpflichtversicherung gelten und doch hat sie nur eine geringe Verbreitung. Dabei sind nicht nur die Chancen, einen Schaden zu erleiden groß, auch die Schadenhöhe ist zuweilen existenzbedrohend. Jedes Jahr entsteht ein Schaden von 55 Mrd. €. Ein guter Grund sich abzusichern. Mehr unter www.lubeca.eu/cyber

fast **49 %** aller Unternehmen

haben ein Jahr lang **keinen** Cyberschaden

Cyber-ABC

A wie Advanced Persistent Threat (APT)

… sind zielgerichtete Cyber-Angriffe auf ausgewählte Unternehmen, Institutionen und Einrichtungen, bei denen sich der Angreifer dauerhaft Zugriff zu einem Netz verschafft und sich folgend auf weitere Systeme ausweitet.

B wie Botnet

… ist ein Verbund von Rechnern (Systemen), die von einer Malware befallen sind und mittels eines Command-and-Control-Servers kontrolliert und gesteuert werden. Cyber-Kriminelle infizieren weltweit die Systeme von Unternehmen und Privatpersonen und nutzen die Systeme für DDoS-Attacken, oder den Versand von Spam-Mails. Die Infizierung bleibt fast immer unbemerkt.

C wie Cracker

… ist das kriminelle und destruktive Gegenstück zum Hacker. Leider unterscheiden die Medien hier meist nicht.

D wie DDoS-Attacke (Distributed-Denial-of-Service-Attacke)

… ist eine künstlich herbeigeführte Überlastung eines Webservers oder Datennetzes. Tausende Systeme bombardieren die Gegenstelle mit Anfragen und sorgen für Systemausfälle, selbst bei den hochleistungsfähigsten Systemen.

E wie Exploit

… man spricht von einem Exploit, wenn eine Schwachstelle in einer Software zur Infektion des Computers mit Malware missbraucht wird.

F wie Fake President

… ist eine Betrugsmethode („Enkeltrick“), bei welcher E-Mails mit angeblichen Transaktionsanordnungen bzw. Aufforderungen zu bestimmten Handlungen im Namen des Firmenchefs an Mitarbeiter des Unternehmens geschickt werden.

G wie Grey Hat

… ist der Typus eines Hackers, bei dem nicht trennscharf zwischen gutartigen und kriminellen beziehungsweise destruktiven Aktionen unterschieden werden kann. Im Gegensatz zu White Hats nutzen Grey Hats ihr Talent mitunter auch für Angriffe.

H wie Hacker

… sind Technikenthusiasten, die mit ihren Fachkenntnissen beliebige Techniken abseits des eigentlich gedachten Zweckes verwenden. Per se keine Online-Kriminellen, anders als Cracker. Wohlmeinende Hacker weisen auf Sicherheitslücken in Software oder Systemen wie dem elektronischen Personalausweis hin und verwenden die Informationen nicht für Angriffe oder andere kriminelle Aktivitäten.

I wie IT-Forensik

… befasst sich mit der Untersuchung, Analyse und Aufklärung von Sicherheitsvorfällen im Zusammenhang mit IT-Systemen.

J wie Junk Mail

… dient beispielsweise zum Verkauf gefälschter Pharmazeutika (zumeist Viagra und Co.) und auch zum Abgreifen von Login-Daten per Phishing-Attacke.

K wie Keylogger

… wird Hard- oder Software zum Mitschneiden von Tastatureingaben bezeichnet. Sie zeichnen alle Tastatureingaben auf, um sie möglichst unbemerkt an einen Angreifer zu übermitteln. Dieser kann dann aus diesen Informationen für ihn wichtige Daten, wie z. B. Anmeldeinformationen oder Kreditkartennummern filtern.

L wie Linux

… ist der vermeintliche heilige Gral aller IT-Sicherheitsspezialisten und gilt im Vergleich zu Windows als deutlich sicherer. Das ist aber nicht unbedingt korrekt: Auch in Linux und seinen Komponenten finden sich reichlich Lücken, und es gibt nicht weniger Patches als im Microsoft-Umfeld. Aber mangels Marktanteil schreiben die Online-Kriminellen keine Exploits für Linux.

M wie Man-in-the-Middle-Angriff

… ist ein Angriff mit dem Ziel, sich unbemerkt in eine Kommunikation zwischen zwei oder mehreren Partnern einzuschleichen, beispielsweise um Informationen mitzulesen oder zu manipulieren. Hierbei begibt sich der Angreifer „in die Mitte“ der Kommunikation, indem er sich gegenüber dem Sender als Empfänger und gegenüber dem Empfänger als Sender ausgibt.

N wie Nicknapping

… bezeichnet einen Cyberangriff, bei dem der Angreifer unter einem bekannten Namen oder Pseudonym auftritt. Dadurch versucht der Angreifer, gegenüber Dritten den Eindruck zu erwecken, er sei der eigentliche/ursprüngliche Inhaber des Namens oder des Pseudonyms. Gelingt dies, kann der Angreifer in begrenztem Maße als der eigentliche/ursprüngliche Inhaber agieren.

P wie Phishing

… hierbei wird z. B. mittels gefälschter E-Mails und/oder Webseiten versucht, Zugangsdaten für einen Dienst oder eine Webseite zu erlangen. Wird diese Manipulation vom Opfer nicht erkannt und die Authentizität einer Nachricht oder Webseite nicht hinterfragt, gibt das Opfer seine Zugangsdaten u. U. selbst unwissentlich in unberechtigte Hände.

R wie Replay-Angriff

… beschreiben allgemein Angriffe, bei denen ein Informationsaustausch zuerst aufgezeichnet wird und die gewonnenen Informationen im Anschluss daran missbräuchlich wiederverwendet werden. Anhand eines aufgezeichneten Login-Vorgangs kann ein Angreifer beispielsweise versuchen, sich selbst unberechtigt Zugang zu dem jeweiligen System zu verschaffen.

S wie Spyware

… bezeichnet Programme, die heimlich, also ohne darauf hinzuweisen, Informationen über einen Benutzer bzw. die Nutzung eines Rechners sammeln und an den Urheber der Spyware weiterleiten. Spyware gilt häufig nur als lästig, es sollte aber nicht übersehen werden, dass durch Spyware auch sicherheitsrelevante Informationen wie Passwörter ausgeforscht werden können.

T wie Trojanisches Pferd

… wird oft auch (fälschlicherweise) kurz „Trojaner“ genannt, ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Ein trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogramms für seine Installation durch den Benutzer.

U wie UAC (User Access Control)

… ist die Benutzerkontensteuerung und führte Microsoft mit Windows Vista ein. Die mitunter nervigen Pop-ups sollen den Anwender darauf aufmerksam machen, dass eine Aktion Administratorrechte verlangt. Malware-Infektionen sollen so ausbleiben.

V wie Viren

… ist die klassische Form von Schadsoftware, die sich selbst verbreitet und unterschiedliches Schadpotenzial in sich tragen kann (keine Schadfunktion bis hin zum Löschen der Daten auf einer Festplatte). „Viren“ treten in Kombination mit einem Wirt auf, z.B. einem infizierten Dokument oder Programm.

W wie White Hat

… in Anlehnung an die Helden aus der Zeit der Schwarz-Weiß-Western werden wohlmeinende Hacker auch als „White Hats“ bezeichnet. Sie wollen niemandem schaden und halten sich – anders als Black Hats – an die Regeln. Grey Hats sitzen zwischen den Stühlen und handeln mal verantwortlich, mal gefährlich.

X wie XSS (Cross Site Scripting)

… hier wird eine Schwachstelle in einer Webanwendung missbraucht, um mit Hilfe des Browsers auf dem PC des Anwenders eine andere Anwendung anzugreifen. Konkret: Ist ein Webmail-Dienst wie Hotmail oder Google Mail anfällig für eine XSS-Attacke. Hier könnte eine bösartige Webanwendung aus einem anderen Browser-Fenster heraus die Login-Daten für den Maildienst stehlen.

Y wie Yahoo-Angriff

… Praxisbeispiel bei dem Daten (Namen, E-Mail-Adressen, Telefonnummern und auch Passwörter) von 3 Milliarden Nutzerkonten abgegriffen wurden. Opfer von weiteren erfolgreichen Cyber-Angriffen wurden u.A.:
Sony, Adobe Systems, Snapchat, Ebay Inc., J.P. Morgan Chase und viele mehr.

Z wie Zero Day

… sind Schwachstellen in Software, für die es noch keinen Patch vom betroffenen Hersteller gibt. Taucht also ein Exploit für die betreffende Lücke auf, gibt es keinen Schutz, und die Rechner können ohne Gegenwehr mit Malware infiziert werden.

Cyber-Angriffe nehmen zu, obwohl Softwareentwickler sich zunehmend dem Thema Daten- und Funktionssicherheit widmen. Die größte Schwachstelle bleibt der User und es ist kaum möglich an der Stelle alle Risiken zu erkennen und zu begrenzen, ohne den täglichen Arbeitsfluss zu stören. So bleibt Datensicherheit immer auch ein Kompromiss, den man am besten über den Schutz vor wirtschaftlichem Schaden durch eine Cyberversicherung absichert.

LUBECA

Wir nehmen das Risiko

LUBECA CYBER SHIELD ist eine Beratungsdienstleistung und Erstellung eines professionellen Versicherungskonzeptes zum Schutz vor den Folgen von Angriffen gegen Computer und digitale Daten von Unternehmen.
Mehr über den CYBER SHIELD unter

lubeca.eu/cyber

LUBECA

Wir nehmen das Risiko

LUBECA Versicherungskontor GmbH | Beckergrube 38-52 | 23552 Lübeck | Geschäftsführer: Dirk Beyer
Tel. +49 **451 148 260** | eMail: **mail@lubeca.eu**

www.lubeca.eu