Newsletter Datenschutz

Ausgabe 08 | 2022

Datenschutz-Audits stellen Standards sicher!

Ihr Datenschutz-Info-Blatt

Liebe Leserin, lieber Leser,

stellen Sie sich vor, Sie bekommen eine E-Mail, die eine Cyberattacke androht, wenn man dem Übeltäter kein Geld überweist. Wenn Sie jetzt nicht wissen, was dann zu tun wäre, lesen Sie am besten jetzt gleich den ersten Beitrag unserer neuen Datenschutz-Zeitung!

Es muss aber nicht gleich eine Cyberattacke sein, die richtiges Verhalten notwendig macht. So sollten Sie auch wissen, was bei einem Datenschutz-Audit auf Sie zukommen kann. Ebenso sollten Sie sich gut vorbereiten, wenn Telefonanrufe für Werbezwecke geplant sind. Beide Themen finden Sie ebenfalls in dieser Ausgabe.

Den Abschluss macht diesmal die bittere Erkenntnis, dass selbst ein guter Geschäftspartner zum Datenrisiko werden kann – ungewollt, weil Internetkriminelle seine IT-Systeme zu Angriffszwecken kapern und missbrauchen.

Ihr Frank Berns, Datenschutzbeauftragter

So verhalten Sie sich bei einer Online-Erpressung richtig

Internetkriminelle drohen Unternehmen mit gezielten Angriffen, die wichtige IT-Systeme zum Ausfall bringen könnten. Sicherheitsbehörden warnen davor, den Online-Erpressern nachzugeben und Lösegeld zu bezahlen. Doch was tut man stattdessen?

Cyber-Straftaten auf neuem Höchststand

Die Anzahl erfasster Cyber-Straftaten hat im Jahr 2021 einen neuen Höchstwert erreicht, so das Bundeskriminalamt (BKA) im neuen Bundeslagebild Cybercrime. Auch bei DDoS-Angriffen (Distributed Denial of Service) war im Jahr 2021 erneut ein qualitativer und quantitativer Zuwachs zu verzeichnen. Insbesondere ihre Komplexität nimmt weiter zu.

DDoS zielt darauf ab, Webpräsenzen, Server und Netzwerke zu überlasten und so eine Nichterreichbarkeit der Dienste herbeizuführen. Von dieser Art von Cyberangriffen war eine Vielzahl verschiedener Branchen betroffen. Neben Finanzdienstleistern, Hosting-Anbietern, Lern- und Impfportalen standen im letzten Jahr auch öffentliche Einrichtungen und der E-Commerce im Fokus.

Androhung: Lösegeld oder DDoS

DDoS-Angriffe, die zum Beispiel den Webserver eines Unternehmens überlasten sollen, können ganz plötzlich und ohne jede Warnung auftreten. Aber oftmals melden sich die Internetkriminellen vor einem

möglichen Angriff und verlangen Lösegeld. Zahlt das Unternehmen nicht, erfolgt der Angriff, so lautet dann die Drohung.
Es ist nicht klar, ob es sich um eine leere Drohung handelt oder ob der Angriff wirklich erfolgt, aber auch nicht, ob eine Zahlung den DDoS-Angriff überhaupt verhindern würde.

In jedem Fall sagen die Sicherheitsbehörden: „Gehen Sie nicht auf Lösegeldforderungen ein, weder bei Erpresser-Viren (Ransomware) noch bei Online-Erpressung bei einer angedrohten DDoS-Attacke!" Der Grund: Das Lösegeld würde die Kriminellen unterstützen und Anreize für weitere Straftaten setzen. Stattdessen gilt es, richtig und besonnen zu reagieren – auch im Kreis der Anwenderinnen und Anwender, nicht nur in der IT-Administration.

Das richtige Verhalten ist entscheidend

Das BKA gibt Unternehmen eine Reihe von Hinweisen, wie sich ein möglicher Schaden durch DDoS so gering wie möglich halten lässt. Dabei ist jeder im Unternehmen gefordert. Ist man selbst der Empfänger der Droh-Mail, lautet die Empfehlung des BKA: „Fotografieren Sie die Erpressungsnachricht auf Ihrem Bildschirm und erstatten Sie Anzeige bei der Polizei".

Innerhalb eines Unternehmens bedeutet das, Nachweise für die Online-Erpressung (Foto des Bildschirms mit der Nachricht) zu sammeln und alle Stellen im Unternehmen, die für einen solchen Notfall definiert sind, zu benachrichtigen. Diese Stellen werden dann unter anderem mit der Polizei in Kontakt treten. Erstattet ein Unternehmen frühzeitig Strafanzeige, ist es den Strafverfolgungsbehörden möglich, schnelle und effektive Maßnahmen gegen kriminelle Cybergruppierungen zu treffen, so das BKA.

Interne Meldewegen kennen und nutzen

Der Schutz vor DDoS-Attacken, sei es durch die eigene IT-Abteilung oder einen spezialisierten Dienstleister, muss so schnell wie möglich reagieren, um die Angriffswellen umlenken zu können.

Dazu ist es entscheidend, dass alle Beschäftigten sowohl entsprechende Androhungen intern melden als auch auf Anzeichen für DDoS-Attacken achten, darunter die Nichterreichbarkeit der Unternehmenswebseite und Störungen in der digitalen Kommunikation.

Wer nicht genau weiß, wie intern zu melden ist, sollte sich umgehend informieren.

Datenschutz-Audit

Datenschutz-Audits sind zunehmend ein Thema. Sie verlaufen erfolgreich, wenn alle beteiligten Stellen im Unternehmen konstruktiv mitwirken.

Audits stellen Standards sicher

Audits gibt es auf vielen Gebieten. Generell soll ein Audit feststellen, ob bestimmte Standards erfüllt sind. Ein Datenschutz-Audit soll herausfinden, ob die Standards eingehalten sind, die das Datenschutzrecht vorgibt. Diese Vorgaben können sich auf rechtliche Fragen, aber auch auf technische Abläufe und Prozesse beziehen.

Ein Datenschutz-Audit ist kein Selbstzweck

„Erst haben alle viel Aufwand und am Ende steht eine Bestätigung, die dann in irgendeiner Schublade schlummert." Solche spöttischen Kommentare gibt es immer wieder einmal, wenn ein Datenschutz-Audit ansteht. Sie unterschätzen seine Bedeutung. Intern sorgt es dafür, dass Schwachstellen erkannt und behoben werden können.
Extern zeigt es Auftraggebern des Unternehmens, dass sie sich auf dessen Datenschutzbemühungen verlassen können. Das kann beim Wettbewerb um lukrative Aufträge den Ausschlag geben.

Datenschutz-Audits sind in der DSGVO verankert

Das Wort „Datenschutz-Audit" findet man in der Datenschutz-Grundverordnung (DSGVO) zwar nicht. Dafür enthält sie jedoch die Verpflichtung, die Einhaltung der Datenschutzvorschriften jederzeit nachweisen zu können. Einschlägiges Stichwort hierfür ist die „Rechenschaftspflicht", die in Art. 5 Abs. 2 DSGVO verankert ist.
Ein bewährtes Mittel, um diese Pflicht zu erfüllen, ist ein erfolgreiches Datenschutz-Audit.

Es gibt interne und externe Datenschutz-Audits

Unternehmen haben die freie Entscheidung zwischen beiden Varianten. Welche im Einzelfall sinnvoll ist, hängt von vielen Faktoren ab. Ein eher neutraler Blick von außen kann sehr wertvoll sein. Ihm entgeht aber vielleicht auch das eine oder andere, das ein Insider erkannt hätte. Manchmal kombinieren Unternehmen auch beide Formen. Dann steuert beispielsweise der Datenschutzbeauftragte den Ablauf des Audits. Für die Durchführung im Einzelnen kann er auf externe Unterstützung zurückgreifen.

Wesentlich beteiligt ist der Datenschutzbeauftragte in jedem Fall. Denn zu seinen Aufgaben gehört es, die Einhaltung datenschutzrechtlicher Vorschriften zu überwachen. Das legt Art. 39 Abs. 1 Buchstabe b DSGVO so fest.

Datenschutz-Audits setzen umfassend an

Es hilft einem Unternehmen wenig, wenn es zwar rechtlich korrekte Einwilligungen bei seinen Kunden einholt, die Daten der Kunden dann aber sicherheitstechnisch nicht ausreichend schützt. Dieses Beispiel zeigt, dass ein Datenschutz-Audit mehrere Kontrollbereiche abdecken muss:

- Im Bereich „Recht" steht die Einhaltung der „Paragrafen" im Fokus. Beispiel: Entsprechen Einwilligungserklärungen den Vorgaben der DSGVO und der Aufsichtsbehörden?
- Im Bereich „Organisation und Prozesse" geht es vor allem darum, ob die rechtlichen Anforderungen in den Abläufen korrekt abgebildet sind. Beispiel: Ist sichergestellt, dass die vorgeschriebenen Datenschutzinformationen alle Kunden auch tatsächlich erreichen?
- Im Bereich „IT" geht es um die Sicherheitsanforderungen des Datenschutzes. Beispiel: Ist durch geeignete Backup-Routinen sichergestellt, dass Kundendaten trotz eines erfolgreichen Störangriffs von außen schnell wieder verfügbar sind?

Schwachstellen sind willkommen

Bei einem Datenschutz-Audit geht es nicht um eine Leistungsprüfung, die mit einem Zeugnis abschließt. Es soll vielmehr objektiv feststellen, wie die Lage des Datenschutzes ist. Dazu dokumentiert es die vielen Dinge, die in der Regel schon gut laufen. Zum anderen zeigt es allen Beteiligten, wo Optimierungsbedarf besteht oder wo beispielsweise ein vorgeschriebener Ablauf noch gar nicht vorhanden ist. Hier ist dann für die Zukunft anzusetzen.

Die Datenschutz-Aufsicht bleibt außen vor

Ein Datenschutz-Audit löst auch Diskussionen aus, was eigentlich vorgeschrieben ist und was nicht. Solche Diskussionen laufen manchmal kontrovers ab. Dann sind sie besonders wertvoll. Sie finden nämlich rein intern statt. Die Datenschutz-Aufsichtsbehörden sind dabei völlig außen vor. Es ist stets besser, mögliche Schwachstellen intern zu diskutieren, als dies später bei einer Kontrolle mit einer Datenschutz-Aufsichtsbehörde tun zu müssen. Der Stress und der Druck wären dann wesentlich höher.

Routine braucht Zeit

Das erste Datenschutz-Audit in einem Unternehmen verlangt allen Beteiligten einiges ab. Die Abläufe sind ungewohnt. Es gibt Diskussionen über die Maßstäbe des Audits und darüber, was seine Ergebnisse bedeuten. Das zweite Audit funktioniert dann erfahrungsgemäß schon recht „rund". Der Aufwand des Anfangs trägt dann Früchte.

Direktwerbung – das müssen Sie beachten

Für persönlich adressierte Werbekontakte, also für Direktwerbung, gibt es in vielen Unternehmen genaue Richtlinien. Lesen Sie, warum Sie diese Vorgaben genau beachten müssen und warum Werbung per Telefon besondere Tücken aufweist.

Der Begriff „Werbung" geht sehr weit

Im alltäglichen Sprachgebrauch versteht man unter „Werbung" Angebote von Waren oder Dienstleistungen. Direktes Ziel ist dabei, die angesprochene Person zum Abschluss eines Vertrags zu bringen. Rechtlich gesehen reicht der Begriff „Werbung" aber deutlich weiter. Das sollte man beachten.

Geburtstags- und Weihnachtsgrüße gehören dazu

So besteht Einigkeit darüber, dass auch Geburtstagsanrufe oder Weihnachtsmails an Kunden als Werbung anzusehen sind. Dasselbe gilt auch für die Nachfrage bei einem Kunden, ob er mit einer Lieferung zufrieden ist („Zufriedenheitsnachfrage").

Entscheidend ist das Ziel der Absatzförderung

Dieses weite Verständnis des Begriffs „Werbung" hat seine Berechtigung. Denn natürlich soll etwa auch ein Geburtstagsgruß dazu beitragen, dass der Kunde dem Unternehmen gewogen bleibt. So gesehen dienen Geburtstagswünsche der Förderung des Geschäfts. Dies wiederum ist das entscheidende Merkmal, das eine Handlung oder eine Äußerung zu einer Werbemaßnahme macht.

Eine Einwilligung wäre ein guter Weg

Für persönliche Werbung („Direktwerbung") braucht man personenbezogene Daten wie Namen und Telefonnummer. Festhalten und verwenden darf man solche Daten nur, wenn die DSGVO dafür eine Rechtsgrundlage bereithält. Die Einwilligung der betroffenen Person wäre eine Möglichkeit. Sie genügt immer – jedenfalls wenn sie ordnungsgemäß eingeholt wurde. Oft fehlt eine Einwilligung jedoch völlig. Auch Zweifel, ob eine vorhandene Einwilligung wirklich passt, sind häufig.

Die Interessenabwägung ist eine denkbare Alternative

Schön wäre es deshalb, wenn die DSGVO die Direktwerbung unter bestimmten Voraussetzungen generell erlauben würde. Der eigentliche Text der DSGVO sagt speziell dazu nichts. Hoffnung weckt aber Erwägungsgrund 47 zur DSGVO. Dort heißt es: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden." Die Erwägungsgründe bilden einen Teil der DSGVO und sollen es erleichtern, ihren Sinn zu verstehen.

Diese Alternative hat aber ihre Tücken

Erwägungsgrund 47 verlangt genaue Lektüre. Er gibt keinen Freibrief dafür, personenbezogene Daten für die Direktwerbung zu verwenden. Er sagt nämlich nicht, dass die Direktwerbung immer ein berechtigtes Interesse darstellt. Er hält lediglich fest, dass dies prinzipiell so sein „kann". Das führt zu der Frage, was die genauen Voraussetzungen dafür sind. Wann hat die Direktwerbung als berechtigtes Interesse den Vorrang und wann sind Interessen der betroffenen Person wichtiger?

Die Bildung von Fallgruppen hilft weiter

Die Datenschutz-Aufsichtsbehörden und die Rechtsprechung sind sich über die Bewertung bestimmter Fallgruppen einig. Beispiele hierfür:

- Ein Unternehmen sendet allen Kunden, die bei ihm etwas bestellt haben, später noch einen Werbekatalog oder ein Werbeschreiben zu. Das soll weitere Bestellungen auslösen. Es besteht Einigkeit, dass das erlaubt ist.
- Es ist auch o.k., wenn dabei nur Kunden aus bestimmten Postleitzahlbereichen so angesprochen werden. Das hat beispielsweise Sinn, wenn sich das Unternehmen auf bestimmte räumliche Bereiche konzentrieren will.
- Anders sieht es aus, wenn die Kunden mittels zusätzlicher individueller Merkmale (wie etwa Alter oder Angaben zu Immobilienbesitz) in Gruppen sortiert werden. Eine solche individuelle Profilbildung („Profiling") ist nur mit individueller Einwilligung des jeweiligen Kunden zulässig. Sie greift so tief in seine Belange ein, dass eine Interessenabwägung das nicht mehr legitimieren kann.

Datenschutz und Wettbewerbsrecht laufen parallel

Telefonanrufe für Werbezwecke sind im Gesetz gegen unlauteren Wettbewerb (UWG) streng reglementiert:

- Gegenüber Endverbrauchern sind sie nur zulässig, wenn der Verbraucher darin ausdrücklich eingewilligt hat (§ 7 Abs.2 Nr. 2 UWG).
- Gegenüber Unternehmen sind sie erlaubt, wenn zumindest mutmaßlich davon ausgegangen werden kann, dass das andere Unternehmen damit einverstanden ist. Typisches Beispiel dafür: Es bestand schon einmal früher geschäftlicher Kontakt.

Das Datenschutzrecht übernimmt diese Maßstäbe. Wer also darauf hofft, über eine Interessenabwägung im Datenschutz den Vorgaben des UWG zu entkommen, würde Schiffbruch erleiden.

Der Geschäftspartner als Datenrisiko?

Mit Lieferanten und anderen Geschäftspartnern verbindet einen oftmals eine lange, vertrauensvolle Zusammenarbeit. Genau das nutzen nun Cyberkriminelle aus und greifen über die Partner an. Diese Angriffe über die Lieferkette sind besonders gefährlich.

Vertrauen ist ein hohes Gut

Marktforscher wie das Analystenhaus IDC betonen, dass in Zeiten der Digitalen Transformation das Vertrauen noch wichtiger geworden ist. Das sollte nicht verwundern. Denn so praktisch die digitale Kommunikation auch ist, sie ersetzt nicht den persönlichen Kontakt, der so wichtig ist, um eine Geschäftsbeziehung aufzubauen. Man muss bei digitalen Kontakten mehr als bisher dem Gegenüber Vertrauen schenken.

Die Vertrauensbeziehung gibt es zu Kunden, aber auch zu Lieferanten und anderen Geschäftspartnern. Kommt zum Beispiel eine E-Mail von einem Lieferanten, der seit Langem bekannt ist, wird ihr mehr Vertrauen geschenkt. Denn man kennt sich ja und hat gute Erfahrungen miteinander gesammelt.
Leider wissen die Internetkriminellen um die Vertrauensstellung von Geschäftspartnern und Lieferanten und missbrauchen sie auf vielfältige Weise.

Social Engineering ist nicht alles

Schon seit Jahren nutzen Cyberattacken das Vorspielen einer dem Opfer bekannten Identität, zum Beispiel bei Phishing-Mails, um Passwörter und andere vertrauliche Daten zu stehlen. Doch es sind nicht nur psychologische Tricks der Cyberkriminellen, wie sie beim Social Engineering zum Einsatz kommen, die das Vertrauen zu Lieferanten ausnutzen.

Die IT-Systeme der Lieferanten und anderer Geschäftspartner sind meist eng verknüpft mit den IT-Anwendungen eines Unternehmens. Mitunter haben Lieferanten bestimmte Berechtigungen für Fernzugriffe auf Unternehmensdaten, es gibt definierte Schnittstellen untereinander.

Eine Besonderheit bilden IT-Lieferanten, deren Software und Hardware beim Unternehmen zum Einsatz kommen. Auch ihnen und ihren IT-Lösungen wird Vertrauen geschenkt. Das aber kann zunehmend zu einem Datenrisiko werden.

Angriffe über die Lieferkette

Erfolgt über die Datenverbindung, die zu einem Lieferanten aufgebaut wird, plötzlich eine Cyberattacke, wird also zum Beispiel Malware übertragen, dann steckt in aller Regel nicht der langjährige Lieferant selbst hinter dem Angriff.
Vielmehr nutzen externe Angreifer Schwachstellen beim Lieferanten und missbrauchen dann die vertrauensvolle Verbindung zu weiteren Unternehmen, um noch mehr Attacken zu starten. Das kann auch eine Update-Datei eines Softwarelieferanten sein, die heimlich eine Schadsoftware in sich trägt. Angreifer haben dazu die Update-Dateien des Lieferanten manipuliert und greifen über das Update an.

Supply-Chain-Attacken greifen um sich

Solche Angriffe über Lieferanten und Geschäftspartner werden auch als Attacken über die Lieferkette oder Supply-Chain-Attacken bezeichnet. Leider gibt es dafür immer mehr gefährliche Beispiele. So berichtet das Bundesamt für Sicherheit in der Informationstechnik (BSI): „Immer öfter sind auch ganze Lieferketten von Angriffen beeinträchtigt, mit Folgen nicht nur für die Opfer, sondern auch für deren Kunden oder für andere unbeteiligte Dritte".

Diese Entwicklung macht es notwendig, das Vertrauen selbst in Geschäftspartner neu zu bewerten. Nicht weil man den Lieferanten misstraut, sondern weil es Angriffe gibt, die die Vertrauensstellung ausnutzen. Geschäftspartner sind entscheidend für den Unternehmenserfolg, doch sie können auch ein Datenrisiko werden und müssen genauso sorgfältig von der IT-Sicherheit geprüft werden wie andere Externe.

Wissen Sie, was Supply-Chain-Attacken sind? Machen Sie den Test!

Frage: Greifen Geschäftspartner auf die für sie freigegebenen Unternehmensdaten zu, stellt dies kein Risiko dar. Stimmt das?

1. **Nein, denn Cyberkriminelle könnten die Berechtigungen des Geschäftspartners für Attacken missbrauchen.**
2. **Ja, solange sie nur auf die Daten zugreifen, die für sie bestimmt sind.**

Lösung: Die Antwort 1. ist richtig. Natürlich stellen die erlaubten Datenzugriffe durch einen Geschäftspartner an sich kein Risiko dar. Doch Cyberkriminelle nutzen Schwachstellen bei den Geschäftspartnern, um dann deren Zugriffsberechtigungen für weitere Angriffe zu missbrauchen.

Frage: Über Updates eines Softwarelieferanten kommen neue Funktionen und keine möglichen Attacken. Ist das so richtig?

1. **Ja, denn der Softwarelieferant prüft seine Updates, damit sie keine Schadsoftware enthalten.**
2. **Nein, auch in Updates können Attacken versteckt sein. Diese Dateien müssen immer zuerst überprüft werden.**

Lösung: Die Antwort 2. ist richtig. Gute Softwarelieferanten prüfen natürlich ihre Updates vor der Verteilung. Doch Internetkriminelle unterwandern auch Lieferanten und verteilen über die Lieferkette ihre Schadpro-gramme. Hierfür hat es schon viele Beispiele gegeben, die zeigen, dass es inzwischen gezielte Angriffe über die Lieferkette gibt, sogenannte Supply-Chain-Attacken. Deshalb müssen auch Softwarelieferungen und jede Form der digitalen Kommunikation mit den Lieferanten und anderen Geschäftspartnern so behandelt werden, als wären unbekannte Dritte die Absender.

Impressum

Redaktion:
Frank Berns, Datenschutzbeauftragter, Geschäftsführer

Anschrift:
Konzept 17 GmbH
Westring 3
24850 Schuby
Amtsgericht Flensburg: HRB 12329
Telefon: 0049 4621 5 30 40 50
E-Mail: mail@konzept17.de