datenschutz-berater.de

45. Jahrgang

DSB 06/2021

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Editorial

Stichwort des Monats

Datenschutz im Fokus

Aktuelles aus den Aufsichtsbehörden

Rechtsprechung

ISSN 0170-7256

dfv Mediengruppe

Alexander Weidenhammer und Max Just

Die menschliche Firewall – Der Nutzer als Sicherheitsrisiko?

Die Gefährdungslage der IT-Sicherheit verzeichnet in den letzten Jahren einen stetigen Anstieg von Bedrohungsszenarien im privaten wie im betrieblichen Umfeld. Aus dem aktuellen Bericht zur Lage der IT-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik („BSI") geht hervor, dass Angreifer zunehmend Schadprogramme für Cyber-Angriffe nutzen. Ein effektiver Schutz gegen derartige Angriffe kann zwar durch den Einsatz von Antiviren-Software aufgebaut werden. Eine vollständige Sicherheit kann allein hierdurch jedoch nicht gewährleistet werden. Zunehmend wird der Nutzer zur entscheidenden Sicherheitsbarriere. Der Beitrag zeigt sowohl die Risiken als auch die Chancen hinsichtlich des „Faktors Mensch" in der IT-Sicherheit auf.

Sicherheitsrisiken durch Social Engineering

Ein Blick auf aktuelle Bedrohungslagen und -szenarien zeigt, dass Sicherheitsvorfälle in der IT-Sicherheit sowie im Datenschutz, neben technischen Fehlfunktionen, ebenso auf menschliches Fehlverhalten zurückzuführen sind. Ein Wandel ist zudem seit Beginn der Covid-19-Pandemie zu verzeichnen. Mit der zunehmenden Dezentralisierung der betrieblichen IT-Infrastruktur und dem Wechsel zahlreicher Arbeitnehmer ins „Homeoffice" ergeben sich für Cyberkriminille neue Angriffsmöglichkeiten, was wiederrum neue Sicherheitsstrategien von Unternehmen und Behörden erforderlich macht. Aber auch bei den Nutzern kommt es aufgrund der neuen Arbeitssituation zu Unsicherheiten. Zu den beliebten Angriffsvektoren zählt das sogenannte „Social Engineering", im Konkreten Phishing-E-Mails mit Bezug zur Covid-19-Pandemie wie bspw. vermeintliche Informationen durch das BMG oder die WHO, Anträge für Corona-Soforthilfen, Bestellmöglichkeiten für Masken oder Schnelltests sowie Einladungen zu Videokonferenzen. Doch auch über die aktuellen Themen hinaus stellt das „Social Engineering" nach wie vor ein beliebtes Werkzeug zur Verwirklichung krimineller Absichten über das vermeintlich schwächste Glied in der IT-Sicherheit dar: den Nutzer.

Der Nutzer als Sicherheitsrisiko?

Bereits seit längerer Zeit dürfte weitestgehend bekannt sein, dass ein hohes Maß an IT-Sicherheit nicht mehr allein durch einen baulichen Schutz vor Umwelteinflüssen oder durch Einrichtung technischer Schutzvorkehrungen erreicht werden kann. Viel mehr kommt es auf ein stimmiges Zusammenspiel solcher physischen und technischen, jedoch eben auch menschlichen Faktoren an. Dies geht insbesondere auch aus dem Aufbau der hierbei einschlägigen Managementsysteme, beispielsweise nach ISO 27001, hervor. Dem „Faktor Mensch" werden in diesem Gefüge zwei wesentliche Aufgaben zugeschrieben:

- Einerseits proaktiv mögliche Bedrohungslagen und potenzielle Gefährdungen für die IT-Sicherheit zu erkennen;
- andererseits reaktiv auf derartige Ereignisse angemessen zu reagieren, um bereits eingetretene Schäden zu minimieren. Hierbei sind entscheidend insbesondere das Bewusstsein über und die Einhaltung von definierten internen Meldeprozessen im Hinblick auf die Melde- und Benachrichtigungspflichten, bspw. gemäß Art. 33 und 34 DSGVO.

Proaktiv Sicherheitsvorfälle vermeiden

Ersichtlich wird, dass nicht die technische Endpoint-Security allein für eine entsprechende Sicherheit der Organisation ausreichend ist, sondern dem Nutzer eine tragende Rolle zu Teil wird. Der Mensch ist als letzte Sicherheitshürde Dreh- und Angelpunkt in der Sicherheitsstrategie von Unternehmen und Behörden.

Nicht wenige Angriffsmodelle zielen auf eine menschliche Interaktion ab. Immer wieder kommt es zum gezielten Ausnutzen von menschlichen Schwächen, aber auch vermeintlichen Stärken. Dadurch sollen z. B. die Preisgabe von Informationen, die Freigabe von Geschäftsprozessen, der Zugang zu technischen Systemen oder die Installation von Schadsoftware erreicht werden. Exemplarisch für kritische Situationen sind die permanent geforderte Aufmerksamkeit, ermüdende Tätigkeiten durch zahlreiche Wiederholungen oder andauernde Monotonie zu nennen. Jeder Nutzer ist in dieser Hinsicht empfänglich für psychologische Fehler. Es herrscht zuweilen eine große Vielfalt an Fehlerquellen. Bei entsprechenden Gestaltungen genügen mitunter bereits kleine visuelle Änderungen zur Täuschung des Nutzers.

Mit Blick auf das Social Engineering als bewusste Manipulation von Menschen ist erkennbar, dass sich die Angreifer zunehmend dem Werkzeug der Angst bedienen. Insbesondere mit Blick auf die Covid-19-Pandemie kommt es aufgrund der allgemeinen Unsicherheit der Nutzer zum gezielten Ausnutzen des Menschen. Die Pandemie prägt anhaltend die berufliche und private Lebensgestaltung der Menschen. Durch fortwährende Einschränkungen gelingt es Angreifern allzu häufig an die angespannte Situation anzuknüpfen. Allein das Aufzeigen von Hilfsmitteln jeglicher

Art – sei es Masken, Tests, finanzielle Unterstützungen – die zur Bekämpfung der Pandemie beitragen, kann ein willkommenes Geschenk sein. Inhaltlich nehmen Angreifer hierbei auf die medial wirksamen Themen rund um die Pandemie Bezug und bedienen bekannten Interaktionsmuster, wie z. B. Klick auf den Link einer E-Mail oder Öffnen eines Anhangs. Im Zusammenhang mit der Covid-19-Pandemie kann zudem auch ein erhöhtes Klickverhalten der Nutzer festgestellt werden. Darüber hinaus zeichnet sich derzeit als neues Phishing-Vorgehen die Versendung von Termineinladungen per E-Mail ab. Hierbei enthalten die Einladungen die Möglichkeiten diese anzunehmen oder abzulehnen sowie alternativ einen (gefälschten) Link zu aktivieren. Besondere Vorsicht ist deshalb geboten, da die E-Mails häufig einen äußeren Zusammenhang zu einem tatsächlich bestehenden Kontakt aufweisen können.

Es wäre verfehlt, leichtfertig allein auf das menschliche Fehlverhalten als Ursache für einen Sicherheitsvorfall abzustellen. Ausschlaggebend ist mitunter, ob in der Organisation entsprechende organisatorische Vorgaben für Datenschutz und IT-Sicherheit vorhanden sind und ob diese Vorgaben gelebt werden. Fehlen vergleichbare Rahmenbedingungen kann dem Nutzer durchaus schon nicht bewusst sein, dass er fehlerhaft handelt und welche Konsequenzen dieses Handeln nach sich ziehen kann.

Ein wesentlicher Beitrag zur Vermeidung bzw. Reduzierung von Sicherheitsrisiken liegt daher in der Initiierung und Implementierung von Sicherheitsrichtlinien, Anweisungen oder vergleichbaren Regelungen. Allerdings erschöpft sich die Schaffung des Sicherheitsprozesses nicht allein mit der Einführung von Sicherheitsregelungen. Zum einen ist es gleichwohl erforderlich, dass diese auf dem aktuellen Stand gehalten und bei Bedarf an veränderte Rechts- und Tatsachenlagen angepasst werden. Zum anderen genügt allein das Schaffen von rechtlichen Rahmenbedingungen nicht. Die bloße Existenz gewährleistet mit Nichten die Einhaltung durch den Nutzer. Derartige Regelungen müssen ebenso verstanden und letztlich zur Anwendung gebracht werden. Andernfalls droht ein Leerlaufen der Festlegungen.

Reaktiv Sicherheitsvorfälle minimieren

Auch unter Kenntnis und Verständnis diverser Sicherheitsregelungen kann niemals gänzlich ausgeschlossen werden, dass von Zeit zu Zeit innerhalb der Organisation Sicherheitsvorfälle eintreten. Hierbei bedarf es eines strukturierten Incident-Response-Managements. Wesentlicher Bestandteil ist die Etablierung von Melde- und Prozessketten, wobei dies nicht allein die Schaffung theoretischer Prozesse, sondern ebenfalls die Bekanntgabe gegenüber den Nutzern sowie die praktische Erprobung des Ernstfalls umfasst. Je nach Ausmaß eines Sicherheitsvorfalls können Nutzer aufgrund der (potenziellen) Auswirkungen und des damit verbundenen Zeitdrucks erneut anfälliger für Fehler sein. Eine regelmäßige Erprobung des Ernstfalls kann dem entgegenwirken und ein gesundes Maß an Routine erzeugen. Gegebenenfalls lassen sich aus einem praktischen Testlauf zudem Unstimmigkeiten in den Melde- und Prozessketten identifizieren und bereits frühzeitig beheben.

Weiterhin ist die Tragweite eingetretener Sicherheitsvorfälle zu analysieren und zu dokumentieren. Dies ermöglicht nicht nur einen noch andauernden Sicherheitsvorfall einzudämmen, sondern auch notwendige Maßnahmen technischer oder organisatorischer Natur abzuleiten, um zukünftige Ereignisse zu verhindern – unabhängig davon, ob der Sicherheitsvorfall durch ein technisches System oder durch einen bzw. mehrere Nutzer verursachte wurde. Die abgeleiteten Maßnahmen sind nach Wiederherstellung des Normalzustandes unverzüglich umzusetzen. Es gilt: Nach dem Sicherheitsvorfall ist vor dem Sicherheitsvorfall.

Maßgebliche Voraussetzungen für das proaktive und reaktive Verhalten der Nutzer sind, dass diese ein Bewusstsein für (potenzielle) Sicherheitsvorfälle entwickeln, einschließlich der Tragweite und Bedeutung für die Organisation. Um die Akzeptanz für getroffene Vorkehrungen seitens der Nutzer zu erreichen, sind außerdem Kenntnis über mögliche Meldepflichten bei Sicherheitsvorfällen und die hinreichende Sensibilisierung bezüglich etwaiger Bedrohungsszenarien erforderlich.

Meldepflichten bei Sicherheitsvorfällen

Neben der im breiten Anwendungsfeld wohl bekanntesten Meldepflicht des Art. 33 DSGVO (siehe zu den Anforderungen an eine Meldung S. 174), existieren zahlreiche weitere vergleichbare Verpflichtungen. Beispielhaft kann in diesem Zusammenhang hingewiesen werden auf § 8b Abs. 4 BSIG zur Meldepflicht für Betreiber kritischer Infrastrukturen oder § 109 Abs. 5 TKG für Telekommunikationsunternehmen. Bedeutung erlangen zudem § 11 Abs. 1c EnWG, § 44b AtG, § 329 SGB V, § 8c Abs. 3 BSIG oder länderspezifisch z. B. die §§ 15–17 SächsISichG.

Zentraler Baustein für die fristgerechte Wahrnehmung der gesetzlichen Meldepflichten ist der organisationsinterne Informationsfluss an die entscheidungsbefugten Ebenen. Um ein erfolgversprechenden Meldeprozess aufzubauen, ist es notwendig, ein grundlegendes Verständnis für die Thematik zu schaffen. Außerdem sollten mögliche Konsequenzen für festgestellte Sicherheitsvorfälle gegenüber den Nutzern transparent kommuniziert werden.

Verständnis schaffen

Mit Blick auf vorbezeichneten Normen wird deutlich, dass der Gesetzgeber bei der Bestimmung der gesetzlichen Meldefristen zuweilen auf starre Fristen verzichtet und stattdessen auf die „Unverzüglichkeit“ der Handlung abstellt. Im Fall des Art. 33 DSGVO ist eine Meldung an die zustän-

dige Aufsichtsbehörde „unverzüglich und möglichst binnen 72 Stunden, nachdem […] die Verletzung [des Schutzes personenbezogener Daten] bekannt wurde," vorzunehmen. Zwar ist der Begriff „unverzüglich" grundsätzlich europäisch und nicht nach Maßgaben des deutschen Zivilrechts zu interpretieren. Im Ergebnis wird es jedoch bei einem Handeln „ohne schuldhaftes Zögern" verbleiben. Die englische Textfassung – „without undue delay" – verdeutlicht, dass sich dieses Begriffsverständnis mit jenem des deutschen Zivilrechtes und im konkreten § 121 Abs. 1 Satz 1 BGB („ohne schuldhaftes Zögern") deckt. Unter Zugrundelegung dieser Grundsätze tritt erkennbar hervor, dass zur Einhaltung gesetzlicher Meldefristen eine funktionierende interne Organisation zur Bekanntgabe und Meldung von Sicherheitsvorfällen notwendig ist. Die Brisanz für Organisationen liegt hierbei zudem in den möglichen folgenden Sanktionen bei Verletzungen der Meldefristen wie bspw. i.R.d. Art. 83 Abs. 4 lit. a DSGVO (siehe zu weiteren Fehlern bei der Meldung nach Art. 33 DSGVO S. 174).

Bezogen auf die unterschiedlichen Angriffsszenarien drängt sich zudem auf, dass im Hinblick auf mögliche Schadensszenarien der Zeitraum zwischen dem Erkennen einer Gefährdung und der (internen) Meldung so kurz wie möglich gehalten werden muss. Neben der Erfüllung regulatorischen Anforderungen und daran anknüpfenden Konsequenzen rücken für Organisationen ebenso mögliche Schäden aufgrund des Sicherheitsvorfalls sowie die Kosten zu dessen Beseitigung und Imageschäden bei Kunden, Interessenten und Beschäftigten auf die Agenda.

Unabdingbar für die Einhaltung von zunächst internen Meldepflichten und -fristen ist, dass den Nutzern bewusst ist, was unter einem IT-Sicherheits- oder Datenschutzvorfall zu verstehen ist. Hilfreich aber nicht ausreichend sind beispielhafte Aufzählungen von möglichen Fallkonstellationen in internen Dokumentationen. Hand in Hand mit derartigen Festlegungen gehen stets daran anknüpfende Sensibilisierungsmaßnahmen. Bestenfalls fallen hierunter auf die konkreten Tätigkeitsfelder der Nutzer zugeschnittenen Besprechungen von Anwendungsfällen. Nur der verständige Nutzer steigert die Möglichkeit zur frühzeitigen Erkennung und Behandlung von Sicherheitsvorfällen.

Transparenter Umgang mit Sanktionen

Die zuvor beschriebene Sensibilisierung der Nutzer löst häufig zugleich die Befürchtungen vor möglichen persönlichen Konsequenzen aus. Dies tritt insbesondere dann ein, wenn der Vorfall aufgrund von (fahrlässigen) Verstößen gegen interne Sicherheitsvorgaben oder -richtlinien hervorgerufen wurde. Organisationen müssen verhindern, dass die betroffenen Nutzer deshalb nicht gehemmt sind, intern Informationen weiterzuleiten. Häufig mangelt es aufgrund von emotionalen Einflüssen an einer sachgerechten Entscheidungsgrundlage und der Nutzer schätzt zu erwartende Risiken falsch oder unzutreffend ein. Dieser Gefahrenquelle kann mit einem entsprechenden transparenten Umgang mit möglichen Konsequenzen vorgebeugt werden.

Die Sensibilisierung ist der Schlüssel

Die vorstehenden Ausführungen verdeutlichen, dass neben den technischen Vorkehrungen und den rechtlichen Maßnahmen – der Implementierung von Sicherheitsrichtlinien – die organisatorische Maßnahme der Sensibilisierung der Nutzer unabdingbar ist. Dies geht beispielsweise auch aus dem Baustein „ORP.3: Sensibilisierung und Schulung zur Informationssicherheit" des BSI IT-Grundschutzes hervor.

Das Schaffen von „Awareness" – also das Umsetzen von Sensibilisierungsmaßnahmen – sollte stets frühzeitig und iterativ etabliert werden: Empfehlenswert ist es etwa bereits im Stadium des Onboardings darauf zu achten, dass Nutzer mit grundlegenden Anforderungen vertraut werden. Häufig wird die Übergabe und Unterzeichnung von gültigen Sicherheitsleitlinien in einer Vielzahl von Organisationen bereits etabliert sein. Immer häufiger enthalten die Anstellungsverträge neben den „üblichen" Verschwiegenheitsklauseln zusätzliche sicherheitsrelevante Regelungen. Insbesondere aufgrund der Fülle von Informationen, mit der neue Nutzer bei Beginn der Tätigkeit konfrontiert werden, ist es wichtig, dass es nicht bei einer reinen Kenntnisnahme der relevanten Regelungen verbleibt.

In Betracht gezogen werden sollte, in einem engen zeitlichen Zusammenhang zur Einstellung die Durchführung erster Schulungsmaßnahmen, um die Thematik gegenwärtig und präsent zu halten. Anschließend empfiehlt sich zu aktuellen oder besonders sensiblen Schwerpunkten weitere Maßnahmen zu ergreifen. So können Informationsschreiben zu bestehenden Bedrohungslagen durch Cyberangriff oder zu stets relevante Themen wie Passwortsicherheit und Umgang mit mobilen Datenträgern gut in den Berufsalltag eingeflochten werden. Insbesondere im Bereich der Cybersicherheit ist darauf zu achten, dass Angriffsmodelle fortlaufend einem Wandel unterliegen und sich stetig fortentwickeln. Aus diesem Grund ist ebenfalls eine kontinuierliche Sensibilisierung erforderlich, damit Nutzer auf die neuen Bedrohungsszenarien reagieren können und anderes nicht in Vergessenheit gerät.

Ein gesundes Mittelmaß finden

Von entscheidender Bedeutung ist dabei auch, ein gutes Maß an Sensibilisierungsmaßnahmen zu finden. Während eine unzureichende Sensibilisierung die Wirksamkeit der übrigen getroffenen technischen und organisatorischen Maßnahmen erheblich abschwächt, kann eine Übersensibilisierung aufgrund der Informationsfülle ebenfalls zu einer Abschwächung des Schutzniveaus führen: Den Nutzern fällt es zunehmend schwerer, die für ihren Verantwortungsbereich relevanten Informationen herauszufiltern und im

Rahmen ihrer täglichen Arbeit angemessen zu berücksichtigen. Weiterhin kann ein zu hohes Maß an Sensibilisierung als „Überregulierung“ oder potenzielle Einschränkung praxisnaher Arbeitsweisen missverstanden werden, sodass im Zweifel zukünftige Sensibilisierungsmaßnahmen auf immer weniger Akzeptanz oder – im schlimmsten Fall – Nichtbeachtung seitens der Nutzer stoßen.

Abhilfe kann hierbei ein auf die jeweils aktuellen Anforderungen angepasstes Sensibilisierungskonzept schaffen. Ein solches sollte dabei nicht nur die aktuell potenziellen Bedrohungsszenarien berücksichtigen, sondern auch auf die spezifischen Anforderungen, z. B. rechtliche oder organisatorische Besonderheiten, der Organisation eingehen. Dabei kann je nach Risikoabschätzung auch eine Unterscheidung hinsichtlich einzelner Organisationseinheiten erfolgen. Ziel sollte in jedem Fall ein auf die im Rahmen ihrer täglichen Arbeit relevanten Themen der Nutzer zugeschnittenes Sensibilisierungsangebot sein. Hierbei ist ein ausgewogenes Verhältnis zwischen den Sicherheitsanforderungen der Organisation und den Umsetzungsmöglichkeiten der Nutzer zu schaffen. Erforderlich ist in gleichem Maße die Bereitschaft des Nutzers zur Umsetzung.

Mittels des Sensibilisierungskonzeptes lässt sich zudem unter Zuweisung von Verantwortlichkeiten ein zeitlich und inhaltlich koordiniertes Awareness-Management dokumentiert nachweisen. Ergänzt werden sollte ein solches Konzept durch Überprüfungen hinsichtlich der Wirksamkeit der durchgeführten Maßnahmen. Etwaige sich hieraus ergebende Schwachstellen können dann im Rahmen zukünftiger Sensibilisierungsmaßnahmen vertieft thematisiert werden.

Fortwährende Sensibilisierung

Ebenso wie die bloße Existenz von Sicherheitsleitlinien und -konzepten nicht automatisch zu einem Mehr an Sicherheit führt, ist es auch mit einer einmaligen Durchführung von Sensibilisierungsmaßnahmen nicht getan. Insbesondere Awareness-Schulungen sollten regelmäßig und spätestens innerhalb eines Zeitraums von 24 Monaten – besser 12 Monaten – wiederholt werden. Die Berücksichtigung aktueller Bedrohungsszenarien und Angriffsmodelle vermeidet repetitive Inhalte.

Durch eine Ergänzung von Schulungsangeboten durch Trainings, beispielsweise simulierter Phishing-Attacken oder Social-Engineering-Anrufen, kann eine fortwährende und zugleich realitätsnahe Sensibilisierung der Nutzer erreicht werden.

Handlungsempfehlungen

Für eine aktive Vermeidung von IT-Sicherheits- und Datenschutzvorfällen obliegt es in aller erster Linie der Leitungsebene von Organisationen unter Einbeziehung der Sicherheitsbeauftragten einen transparenten Prozess zum Umgang mit derartigen Vorfällen zu schaffen. Dieser Prozess erschöpft sich keines Falles in der bloßen Festlegung, Verschriftlichung und Bekanntgabe von Sicherheitsleitlinien. Vielmehr sind eine aktive Ansprache und Sensibilisierung der Nutzer essenziell für eine erfolgreiche Implementierung des Prozesses.

Der Nutzer als entscheidender Faktor im vielfältigen Gefüge der IT-Sicherheit sollte dabei nicht weiter als mögliches Sicherheitsrisiko, sondern als „Sicherheitschance“ gesehen werden. Der Nutzer ist als wichtiger Erfolgsfaktor für die IT-Sicherheit zu verstehen. Durch einen hohen Grad an Sicherheitsbewusstsein kann mithilfe der Nutzer ein effektiver Schutz vor verschiedensten Bedrohungsszenarien erreicht werden. Dies ist nur dann möglich, wenn Sensibilisierungsmaßnahmen auf die konkreten Anforderungen der Organisation zugeschnitten sind und diese die Nutzer inhaltlich erreichen. Generische Schulungs- und Sensibilisierungsmaßnahmen verbieten sich daher. Andernfalls entsteht das Risiko, dass der Nutzer seine Handlungsnotwendigkeit verkennt. Zur Umsetzung eines zeitlich und inhaltlich koordinierten Awareness-Managements empfiehlt sich die Etablierung eines Sensibilisierungskonzeptes, welches sowohl die Sicherheitsanforderungen der Organisation als auch die Umsetzungsmöglichkeiten der Nutzer angemessen berücksichtigt und die Wirksamkeit der Sensibilisierungsmaßnahmen betrachtet.

Die Umsetzung umfasst im Wesentlichen:

- die Implementierung von organisationsbezogenen Sicherheitsrichtlinien bzw. -anweisungen,
- die Bekanntgabe gegenüber den Nutzern und praktische Erprobung der Vorgaben,
- die Analyse und Dokumentation konkreter Sicherheitsvorfälle,
- die fortlaufende Aktualisierung der Regelungen und
- die dokumentierte Sensibilisierung der Nutzer anhand eines festgelegten Sensibilisierungskonzeptes.

Autoren: **Alexander Weidenhammer ist Rechtsanwalt im Dresdner Institut für Datenschutz, spezialisiert im IT-Sicherheits- und Datenschutzrecht und als externer Datenschutz- und Informationssicherheitsbeauftragter tätig.**

Max Just, LL.M. ist Wirtschaftsjurist und im Dresdner Institut für Datenschutz für öffentliche Stellen sowie mittelständische Unternehmen als externer Datenschutzbeauftragter tätig.