ITDSC UG
Data-Security-Consulting
www.itdsc.de

Informationen zum Thema Datenschutz

Liebe Leserin, lieber Leser,

In dieser Ausgabe geht es einmal nicht direkt um IT-Vorfälle.
Auch Datenpannen mit Papierdokumenten sind ein Thema. Diese Datenpannen kommen weitaus häufiger vor, als man in Zeiten der Digitalisierung denken mag.

Ein sehr wichtiger Aspekt in einem Unternehmen ist die Datensicherung oder auch Backup genannt.
Sie sollten diesem Bereich ein gr0ßes Augenmerk schenken.
Da sicheren Backups, gerade in Zeiten von Ransomware-Attacken eine der wichtigsten Maßnahmen der Datensicherheit sind.

Ich wünsche Ihnen viel Spass beim Lesen.

Detlef Riese
Datenschutzbeauftragter

Datenpannen rund um Papier

„Papier verwenden wir im Büro gar nicht mehr!“ Schön, wenn das bei Ihnen wirklich zu 100 % so ist. Denn der falsche Umgang mit Papier führt immer noch die Hitliste der Datenpannen an. Falls in Ihrem Büro zumindest noch etwas Papier vorkommt, sollten Sie also unbedingt weiterlesen.

Statistiken über Pannen sind einfach

Die gesetzlich vorgeschriebene Meldung von Datenpannen an die Datenschutzaufsicht ermöglicht recht genaue Statistiken dazu, was alles schiefgeht in den Büros. Und siehe da: „Pannen rund um Papier“ spielen immer noch eine erhebliche Rolle.

Die Anschriften „außen und innen“ müssen identisch sein

Wenn viel los ist und ein Schreiben mit der gelben Post verschickt wird, gerät es schnell in einen Umschlag, auf dem außen ein falscher Adressat steht. Das kann harmlos sein, wenn etwa nur die neueste Preisliste in die Post geht. Anders sieht es aber beispielsweise bei einem persönlich adressierten Mahnschreiben aus. Es betrifft den Adressaten sehr individuell. Und schon liegt eine ernsthafte Datenpanne vor.

Vier Augen sehen mehr als zwei

Zumindest wenn es um rechtserhebliche Schreiben geht oder um Schreiben mit medizinischen Daten, sollte deshalb vor dem Versand das Vier-Augen-Prinzip zur Anwendung kommen.

Kuvertiermaschinen brauchen Wartung

Verschickt ein Unternehmen eine größere Zahl von Schreiben, kommen nach wie vor Kuvertiermaschinen zum Einsatz. Leider werden sie oft nicht ausreichend gewartet. Dann ist es schnell geschehen, dass die Maschine mehrere Schreiben auf einmal einzieht und in denselben Briefumschlag steckt. Dagegen hilft nur, nicht an der Wartung zu sparen.

Das Faxgerät ist für viele eine Blackbox

Der Faxversand von Dokumenten erfolgt oft durch Hilfskräfte. Schließlich ist das eine scheinbar ideale Arbeit etwa für Praktikanten. Allerdings haben gerade sie meist keinerlei Erfahrung mit Faxgeräten. Der Griff zur falschen Faxnummer ist daher ebenso häufig wie das Vertippen bei der Eingabe der Faxnummer. Eine sorgfältige Einweisung in die Benutzung der Geräte ist deshalb unentbehrlich.

Nummernverzeichnisse brauchen Pflege

Auch die Aktualität von Verzeichnissen mit Faxnummern lässt häufig zu wünschen übrig – oft gerade deshalb, weil Faxgeräte immer seltener benutzt werden. Gerade die schrumpfende Bedeutung solcher Geräte führt dann im Ergebnis dazu, dass Pannen häufiger werden.

Falsch abgelegte Akten sind schwer wiederzufinden

Akten, neuerdings auch „papierbasierte Datenträger“ genannt, kommen vor allem im Personalwesen noch öfter vor. Die praktische Erfahrung zeigt, dass auch dickere Akten durchaus abhandenkommen können. Meist geht es dabei gar nicht um Diebstahl oder dergleichen. Vielmehr werden Akten immer wieder an falscher Stelle abgelegt. Die fehlende Übung gerade jüngerer Mitarbeiterinnen und Mitarbeiter im Umgang mit Akten begünstigt solche Pannen. Aufwendige Suchaktionen sind bisweilen erfolgreich, aber nicht immer. Die beste Abhilfe bietet die Umstellung auf elektronische Verarbeitung.

Papiervernichtung erfordert klare Vorgaben

Papierunterlagen, die nicht mehr benötigt werden, sind zu vernichten. Damit dies in jedem Fall datenschutzkonform erfolgt, sind relativ umfangreiche organisatorische Vorgaben notwendig. Sie sind weitaus wichtiger als beispielsweise die Frage, wie klein die Schnipsel nach dem Schreddern von Papier sein müssen.

Was seltener vorkommt, geht häufiger schief

Auch hier gilt: Gerade weil die Verwendung von Papier tendenziell abnimmt, nehmen die Pannen rund um die Vernichtung von Papier zu. Denn oft sind die organisatorischen Vorgaben schon sehr in die Jahre gekommen. Die Praxis im Unternehmen sieht dann ganz anders aus als in den einschlägigen Checklisten beschrieben. Dagegen hilft nur, diese Checklisten zu aktualisieren und dafür zu sorgen, dass sie auch beachtet werden.

Die Zugriffsprotokollierung funktioniert nur bei elektronischen Daten

Zu beachten ist auch, dass unberechtigte Zugriffe von Mitarbeiterinnen und Mitarbeitern bei Daten auf Papier oft viel einfacher sind als bei elektronischen Daten. Dies liegt daran, dass es keine Spuren hinterlässt, wenn jemand auf „Papier-Daten“ zugreift. Zugriffe auf elektronische Daten werden dagegen in der Regel protokolliert. Solche Zugriffsprotokolle lassen sich auswerten und liefern bisweilen aufschlussreiche Erkenntnisse über Datenschutzverstöße.

Papier ist eine unterschätzte Gefahrenquelle

Über das papierlose Büro wird zwar viel geredet. Zur Realität wird es dadurch allein aber nicht. Es stellt ein sehr richtiges Ziel dar. Solange es aber noch nicht erreicht ist, braucht die „Gefahrenquelle Papier“ die Aufmerksamkeit, die ihr gebührt.

Was bei Backups oft falsch gemacht wird

Hat man ein vollständiges, sicheres Backup, kann man trotz Ransomware-Attacke bald wieder den Betrieb aufnehmen. Leider sind viele Backups aber lückenhaft und unsicher. Erfahren Sie, was Sie zu einer erfolgreichen Datensicherung beitragen können.

Backups sind das Gegenmittel gegen Online-Erpressungen

IT-Sicherheitsbehörden sehen in den Online-Erpressungen mit Ransomware eine der größten Cyberbedrohungen. Das Risiko durch Erpresser-Schadprogramme steigt so stark, dass man vermuten könnte, es gibt keine Gegenwehr.

Doch das „Gegengift“ bei Ransomware-Attacken existiert, es ist wohlbekannt und eigentlich ein alter Bekannter in der IT: ein vollständiges, aktuelles und geschütztes Backup. Hat man seine Daten gesichert, kann man trotz der kriminellen Datenverschlüsselung seine Daten wiederherstellen und bald weiterarbeiten.

Leider sind Backups oft lückenhaft

Die scheinbar einfache Lösung gegen die Ransomware-Folgen ist offensichtlich komplizierter, als viele Unternehmen denken. Versuchen die Unternehmen, ihre Backups wieder einzuspielen, stellen sie fest, dass die Datenbestände unvollständig und veraltet sind. Im schlimmsten Fall müssen die Unternehmen erkennen, dass die Backups nicht geschützt waren und ebenfalls kriminell verschlüsselt wurden.

Laut einer Umfrage des GDV (Gesamtverband der Versicherer e.V.) unter kleinen und mittleren Unternehmen in Deutschland hapert es bei 80 Prozent bereits an den Basisschutzmaßnehmen gegen Cyberattacken. Zu diesen Basisschutzmaßnahmen zählen auch die regelmäßigen und geschützten Datensicherungen.

Zu den Backup-Lücken kommt es zum einen, weil in der zentralen Backup-Verwaltung nicht an alles gedacht wurde. Zum anderen sind aber auch Sie als Nutzerin oder Nutzer gefragt, damit die Backups wirklich zu einer erfolgreichen Datensicherung werden.

Tatsächlich schaffen es nur IT-Administration und Nutzende zusammen, für gute und sichere Backups zu sorgen.

Vermeiden Sie diese Backup-Fehler

So manche Nutzerin und so mancher Nutzer glaubt, wenn ein Backup-Vorgang läuft, dann verlangsamt dies ihre Arbeit und behindert sie. Deshalb neigen diese Nutzenden dazu, wenn möglich die Backup-Funktion zu unterbrechen oder die Backups zu verschieben. Tun Sie das bitte nicht! Damit würde der Backup-Plan unterbrochen, und Ihre Daten sind dann womöglich nicht in der Datensicherung vollständig enthalten, wenn die Sicherung zurückgespielt werden muss.

Ein weiteres Problem: So mancher Fachbereich schafft zum Beispiel Cloud-Dienste an und spricht dies nicht mit der IT ab, man spricht hier auch von Schatten-IT. Wenn aber die IT nichts von der Cloud-Anwendung weiß, kann sie diese auch nicht im Backup-Prozess vorsehen. Gerade durch die Entwicklung hin zu mehr „Hybrid Work“, also dem flexiblen Wechsel zwischen Büro, Homeoffice und mobiler Arbeit, kommt es zur Nutzung von privater IT zu dienstlichen Zwecken, ohne dass die IT darüber informiert wird. Dann fehlen die entsprechenden Daten im Backup. Unvollständige Backups bedeuten aber, dass sich nicht alle Daten wiederherstellen lassen.

Deshalb sollte der Umfang des Backups immer mit der IT abgestimmt werden, damit sie auch wirklich alle Daten sichern kann. Nur dann kann ein Backup auch gegen die Risiken einer Ransomware-Attacke helfen. Vermeiden Sie deshalb Schatten-IT, also Geräte, Speicher, Anwendungen oder Clouds ohne Kenntnis der IT-Administration.

Wissen Sie, was zu einem vollständigen Backup gehört? Machen Sie den Test!

Frage: Ein zentrales Backup erkennt alle Daten und ist immer vollständig. Stimmt das?

1. Nein, wenn Geräte, Anwendungen und Dienste ohne Kenntnis der IT-Administration genutzt werden, werden diese Daten in aller Regel nicht gesichert.
2. Ja, Backup-Programme scannen die IT und sichern alle Daten.

Lösung: Die Antwort 1. ist richtig. Wenn „Schatten-IT“ ohne Kenntnis der IT-Abteilung genutzt wird, fehlen diese Geräte, Dienste und Applikationen oftmals auch in den Backup-Regeln. Generell gilt: Man kann nur schützen und sichern, was man auch kennt. Informieren Sie deshalb immer Ihre Vorgesetzten und die IT, wenn Sie eine neue Anwendung, einen neuen Cloud-Dienst oder ein neues Gerät einsetzen wollen.

Frage: Wenn der Rechner langsam ist, läuft wohl ein Backup, so denken manche Nutzenden. Dann unterbrechen sie den Backup-Vorgang. Ist das so in Ordnung?

1. Ja, denn die aktuelle Arbeit ist dringender als die Backups.
2. Nein, die Backups stören in aller Regel nicht. Zudem sind sie entscheidend wichtig und dürfen nicht gestoppt werden.

Lösung: Die Antwort 2. ist richtig. Backup-Prozesse laufen in der Regel sehr ressourcensparend ab, im Hintergrund, und stören die tägliche Arbeit nicht. Zudem sind Backups kein überflüssiger Ballast, sie können die Rettung in der Not sein bei Datenverlust und insbesondere auch bei den gefürchteten Ransomware-Attacken. Wenn man die Backups unterbrechen würde, tut man genau das, was die Internetkriminellen wollen: Man nimmt sich die Chance auf eine Wiederherstellung, ohne Lösegeld zu zahlen. Wobei man auch generell kein Lösegeld zahlen sollte.

Impressum

Detlef Riese (ITDSC UG)
Datenschutzbeauftragter
Anschrift:
ITDSC UG • Bethanienstrasse 8 • 03172 Guben
Telefon: 03561 5595574 • E-Mail: d.riese@itdsc.de