SANOVIS CONSULTING WITH CARE.

CURACON SICHERHEIT GEBEN. LÖSUNGEN BIETEN.

NEWSLETTER DATENSCHUTZ

Liebe Leserin, lieber Leser,

der Digitalverband Bitkom berichtet von steigenden Schäden durch Datendiebstahl, Spionage und Sabotage. Mehr denn je kommt es darauf an, sich auf Datenpannen und Sicherheitsvorfälle vorzubereiten. Doch viele Unternehmen haben noch keinen IT-Notfallplan.
Umso wichtiger ist es, dass Sie wissen, was Sie bei einem IT-Vorfall tun oder lassen sollten. Diese neue Ausgabe behandelt nicht nur IT-Notfälle. Auch Datenpannen mit Papierdokumenten sind ein Thema. Diese Datenpannen kommen weitaus häufiger vor, als man in Zeiten der Digitalisierung denken mag.
Um IT-Vorfällen und Datenpannen zu begegnen, muss man sie zeitnah erkennen. Hier hilft eine datenschutzgerechte Protokollierung. Hierzu erhalten Sie ebenso wertvolle Hinweise wie zu vollständigen und sicheren Backups, die gerade in Zeiten von Ransomware-Attacken eine der wichtigsten Maßnahmen der Datensicherheit sind.

Wir wünschen Ihnen interessante Erkenntnisse beim Lesen!

Dr. Uwe Günther
Beratungsfeldleiter Datenschutz, Curacon GmbH
Geschäftsführer, Sanovis GmbH

Stefan Strüwe
Beratungsfeldleiter Datenschutz, Curacon GmbH

Dezember_2022

1 IT-NOTFALL:

DENN SIE WISSEN, WAS SIE TUN

Wenn plötzlich eine Meldung auf Ihrem Bildschirm erscheint, dass Ihre Daten verschlüsselt sind und Sie ein Lösegeld für die Entschlüsselung zahlen sollen, kommt es auf eines an: Ihr besonnenes, überlegtes Verhalten. Doch wie sieht das aus?

Panik ist ein schlechter Berater

Kaum jemand wird völlig gelassen reagieren, wenn es klare Anzeichen dafür gibt, dass der eigene Rechner und die eigenen Daten zum Ziel einer Cyberattacke geworden sind. Doch man sollte nicht überreagieren, in Panik verfallen und dann Fehler machen, die die Situation verschlimmern.

Leider besteht in vielen Unternehmen die Gefahr, dass die Beschäftigten nicht wissen, was sie im Fall eines Cyberangriffs oder eines anderen IT-Notfalls genau tun und lassen sollen. Nur gut jedes zweite Unternehmen verfügt über einen Notfallplan mit schriftlich geregelten Abläufen und Ad-hoc-Maßnahmen für den Fall von Datendiebstahl, Spionage oder Sabotage, wie der Digitalverband Bitkom berichtet.

Schnelle Reaktionen, aber keine überstürzten

Doch selbst wenn ein Notfallplan vorliegt, sind die Beschäftigten nicht immer im Bilde darüber, was in einem IT-Notfall zu tun ist. Wie ist es bei Ihnen? Kennen Sie schon das richtige Verhalten, wenn zum Beispiel ein Erpresser-Virus (Ransomware) Ihren Computer befallen hat? Dann gilt es, umgehend, aber wohlüberlegt zu reagieren.

Das Wichtigste: Die umgehende Meldung

Die wichtigste Reaktion ist, nicht selbst den Vorfall beheben zu wollen, sondern den IT-Notfall an die richtige Stelle im Unternehmen zu melden. Kennen Sie die Stelle nicht, fragen Sie bitte Ihre Vorgesetzte oder Ihren Vorgesetzten danach.

Scheuen Sie sich bitte nicht, einen IT-Vorfall zu melden. Es ist nicht Ihr Fehler, wenn Ihr Computer angegriffen wurde. Das kann jedem passieren. Aber Sie müssen den Vorfall melden, als Beobachterin oder Beobachter. Sie sind nicht etwa Verursacherin oder Verursacher, haben Sie da keine Sorge.

Wer, welches, was, wann, wo

Die Meldung eines IT-Notfalls ist einer Unfallmeldung sehr ähnlich. Die zuständige Stelle im Unternehmen braucht die Information, wer etwas meldet, um mögliche Rückfragen zu klären. Dann müssen die Expertinnen und Experten in Ihrem Unternehmen erfahren, welches IT-System betroffen ist, zum Beispiel Ihr PC oder Notebook. Im nächsten Schritt sollten Sie beschreiben, was Sie beobachtet haben, zum Beispiel die Erpresser-Meldung auf Ihrem Bildschirm.

Für die Maßnahmen zur Behebung des IT-Notfalls ist es dann noch wichtig, dass Sie sagen, wann der Vorfall aufgetreten ist und wo sich das betroffene IT-System aktuell befindet, ob Sie beispielsweise damit im Homeoffice oder im Büro gearbeitet haben.

Ansonsten gilt: Stellen Sie so lange die Arbeit an dem betroffenen IT-System ein, bis Sie die Mitteilung erhalten, dass Sie das System wieder nutzen können. Dokumentieren Sie Ihre Beobachtungen zum IT-Vorfall. Alle anderen Maßnahmen sollten nur nach Anweisung erfolgen. Damit lässt sich verhindern, dass Sie ungewollt Fehler machen, die die Lage eher verschlechtern als verbessern.

2 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

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.

3 PROTOKOLLIERUNG – FÜR UNSERE SICHERHEIT!

„Systeme zur Angriffserkennung“ funktionieren nur, wenn Zugriffe auf personenbezogene Daten und andere Verarbeitungsvorgänge protokolliert werden. Die Protokollierung bildet die Basis für eine sichere Datenverarbeitung!

Cyberangriffe sind in aller Munde. Sie haben schon viele Unternehmen getroffen, aber auch Krankenhäuser und sonstige Gesundheitseinrichtungen bleiben nicht verschont. Die Webseiten sämtlicher Industrie- und Handelskammern in Deutschland wurden kürzlich böswillig lahmgelegt. Die Liste der Beispiele ließe sich leicht verlängern. Jedes einzelne Beispiel ist Grund genug, die Cybersicherheit sehr ernst zu nehmen.

Systeme zur Angriffserkennung sind teils gesetzlich vorgeschrieben

Ein wichtiges Instrument für die Abwehr von Angriffen ist „Systeme zur Angriffserkennung“, kurz „SzA“ genannt. Sie sind inzwischen sogar im Gesetz über das Bundesamt für Sicherheit in der Informations-technik (kurz: BSI-Gesetz) erwähnt. In Einrichtungen der kritischen Infrastruktur ist ihr Einsatz gesetzlich vorgeschrieben.

Sie dienen der Erkennung verdächtiger Abläufe

Solche Systeme fahnden nach verdächtigen Abläufen in informationstechnischen Systemen. Konkret bedeutet das: Sie messen Abläufe in EDV-Systemen, werten sie aus und gleichen sie mit Mustern ab, die erfahrungsgemäß auf Angriffe hindeuten.

Das ist manchmal einfach, häufig jedoch nicht

So kann es zum Beispiel verdächtig sein, wenn von einem PC mitten in der Nacht Datenüber-

mittlungen ausgehen, obwohl zu dieser Zeit niemand im Unternehmen arbeitet. In der Regel sind viel kompliziertere Auswertungen und Abgleiche nötig.

Protokolldaten sind die Basis vieler Auswertungen

Um sie durchführen zu können, müssen auch Aktivitäten von Mitarbeiterinnen und Mitarbeitern erfasst und ausgewertet werden. Dies führt zum Thema der Protokollierung von Daten. Es hat gute Gründe, wenn beispielsweise protokolliert wird, wer auf welche Daten zugreift und was er dann mit den Daten tut. Möglicherweise laufen nämlich im Hintergrund ferngesteuerte Aktivitäten ab, von denen er überhaupt nichts ahnt.

Verdächtige Abläufe führen zu schnellen Reaktionen

Falls ein System zur Angriffserkennung anhand von Protokolldaten ungewöhnliche Aktivitäten erkennt, sorgt es dafür, dass umgehend Maßnahmen ergriffen werden. Sie laufen in der Regel automatisch ab. Dazu kann es etwa gehören, laufende Datenübermittlungen zunächst einmal zu stoppen oder auch betroffene Geräte vom Internet zu trennen.

Schutzrechte berücksichtigen die Interessen der Belegschaft

Manche haben die Sorge, sie würden über die Protokollierung vom eigenen Unternehmen möglicherweise unangemessen kontrolliert. Rechtliche Schutzvorschriften stellen jedoch sicher, dass dies nicht der Fall ist. Protokolldaten können je nach ihrem Inhalt zur Kontrolle des Verhaltens und der Leistung von Mitarbeiterinnen und Mitarbeitern geeignet sein. Deshalb greifen hier die Mitbestimmungsregelungen ein, die für solche Situationen gelten.

Der Grundsatz der Zweckbindung ist zu beachten

Generell gelten für Protokolldaten, die personenbezogen sind, die allgemeinen Schutzregelungen für personenbezogene Daten. Dazu gehört der Grundsatz der Zweckbindung. Protokolldaten dienen dazu, eine sichere Datenverarbeitung zu ermöglichen. Insbesondere soll ihre Auswertung böswillige Angriffe von innen oder von außen abwehren. Damit ist der Zweck definiert, für den sie bestimmt sind. Nur dafür dürfen sie verarbeitet werden.

Viele Protokolldaten werden nur kurz gespeichert

Gespeichert werden dürfen Protokolldaten nur so lange, wie es für den geschilderten Zweck erforderlich ist. Viele Protokolldaten werden schon nach wenigen Stunden wieder gelöscht. Im Rahmen eines Sicherheitskonzepts kann es aber auch erforderlich sein, manche Protokolldaten über längere Zeit hinweg zu speichern. Denn manche Angriffsmuster lassen sich nur im längerfristigen Querschnittsvergleich entdecken.

Ein Löschkonzept gehört zu jedem Sicherheitskonzept

Wann welche Protokolldaten gelöscht werden, ist Teil der unternehmensinternen Regelungen für den Einsatz von Systemen zur Angriffserkennung. Da sich Bedrohungslagen immer wieder ändern, dürfen solche Regelungen nicht zu starr sein. Vielmehr müssen sie immer wieder an neue Entwicklungen angepasst werden. Dies alles wird sorgfältig dokumentiert. Der Grundsatz der Rechenschaftspflicht erfordert dies. Er besagt, dass der Verantwortliche nachweisen können muss, dass die DSGVO stets eingehalten wurde.

4 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!

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.

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 Hinter-grund, 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

Redaktion
Dr. Uwe Günther
Sanovis GmbH
Riedenburger Straße 7
81677 München
089 9927579-22
Uwe.Guenther@Sanovis.com

Stefan Strüwe, RA
CURACON GmbH Wirtschaftsprüfungsgesellschaft
Am Mittelhafen 14
48155 Münster
0251 92208-209
Stefan.Struewe@Curacon.de