FAQ IT-Datenverlust

Leitfaden für Gebäudedienstleister

Ausgabe 1 | Juni 2021

Herausgeber:
Bundesinnungsverband des Gebäudereiniger-Handwerks
Dottendorfer Straße 86
53129 Bonn
www.die-gebaeudedienstleister.de
T: +49-228-917750
Mail: biv@die-gebaeudedienstleister.de

Die Gebäudedienstleister
Bundesinnungsverband

Einleitung

Der vorliegende Leitfaden setzt die BIV-Informationsreihe zur IT-Sicherheit fort, die im Mai 2021 mit dem Leitfaden „FAQ IT-Sicherheit“ startete. Er enthielt Hinweise zu den wesentlichen präventiven Maßnahmen zum größtmöglichen Schutz von IT und Daten im Betrieb. Doch auch bei hohem Schutzniveau besteht die latente Gefahr eines erfolgreichen Angriffs auf die betriebliche IT-Infrastruktur und damit des Verlustes wichtiger und wesentlicher Daten. Diesen Verlust im Schadensfall so gering wie möglich zu halten, sollte das Ziel eines IT-Notfallplans sein. Dessen Bausteine stellen wir nun in diesem Leitfaden „FAQ IT-Datenverlust“ vor.

Die, nicht zuletzt durch den Digitalisierungsschub aufgrund der Corona-Pandemie, enorm steigende Anzahl von Angriffen auf Computer und betriebliche Netzwerke führt zu erheblichen direkten und indirekten Schäden bei den Betroffenen. Cyberkriminalität hat die Weltwirtschaft laut einer Studie des Security-Anbieters McAfee im Jahr 2019 über eine Billion US-Dollar gekostet – das entsprach bereits ungefähr einem Prozent des weltweiten BIP zum damaligen Zeitpunkt. Eine viel beachtete Umfrage des Spezialversicherers Hiscox kommt aktuell zu dem Ergebnis, dass fast jedes zweite befragte Unternehmen in Deutschland mindestens einmal von einer Cyberattacke betroffen war. Zunehmend werden auch mittelständische Unternehmen attackiert, denn der Markt wächst auf Seiten der Cyberkriminellen rasant:

Es hat sich bereits eine regelrechte Infrastruktur von unterschiedlichen Anbietern diverser Bausteine etabliert, die unabhängig voneinander und in der Regel im Darknet agieren, weshalb die Rückverfolgbarkeit auch extrem schwierig ist. Das „Portfolio“ im Netzt reicht von Schadsoftware über die Lieferung von Adressdaten potentieller Opfer, Internet-Hosting, Daten-Codierung und Verschlüsselung, so dass selbst Antiviren-Software oft nicht reagiert, bis hin zu „Dienstleistern“, die stellvertretend die Abwicklung des Lösegeldtransfers übernehmen. Das Bundeskriminalamt spricht bereits von „Crime as a Service“, also „Verbrechen als Dienstleistung“.

Durch eine Cyberattacke droht der vollständige Verlust betrieblicher Daten, wie es auch aktuelle Beispiele aus der Branche gezeigt haben. Und dies selbst bei Gebäudedienstleistern, die bereits zahlreiche und sicher weit überdurchschnittliche Sicherungsmaßnahmen installiert hatten. Der resultierende materielle wie immaterielle Schaden, nicht zuletzt durch den erzwungenen Stillstand der Verwaltung und ggfs. sämtlicher betrieblicher Kommunikation via Computern und mobiler IT-Geräte, kann immens sein, so dass die vorbeugenden Maßnahmen in ihrer Bedeutung nicht unterschätzt werden dürfen und natürlich an erster Stelle stehen.

Kommt es jedoch aller präventiven Maßnahmen zum Trotz zu einem Angriff mit entsprechendem Datenverlust, sollten alle notwendigen und sinnvollen Schritte ergriffen werden, den resultierenden Schaden so gering wie möglich zu halten. Im vorliegenden Leitfaden haben die Experten der BIV-Arbeitsgruppe IT-Sicherheit_Cybercrime deshalb zusammengetragen, was im Falle eines Falles zu beachten und zu tun ist und welche Lehren für die Zukunft aus einem solchen Vorfall zu ziehen sind.

Auch hier gilt: das Thema ist derart komplex, facettenreich und anspruchsvoll, dass die dringende Empfehlung lautet, die Maßnahmen unbedingt mit Hilfe der eigenen IT-Experten und ggfs. auch externen Fachleuten abzustimmen und durchzuführen.

Inhalt

Feststellung der betroffenen Systeme und Daten

Schadensbegrenzung (schnell Maßnahmen einleiten)

Frage: Welche Systeme sind von dem Angriff betroffen?

Im Ernstfall ist schnell herauszufinden, welche Systeme von dem Angriff betroffen sind: Wurde möglicherweise nur ein einzelner Computer befallen? Wütet der Virus bereits auf einem oder allen Servern? Ist die gesamte Infrastruktur betroffen? Die Erkenntnis, was gerade passiert oder passiert ist, ist essentiell für die Einleitung der nachfolgenden Schritte zur Schadensbegrenzung.

„Stecker ziehen“?

Frage: Kann ein Angriff unterbrochen werden, wenn ich einfach den Stecker ziehe?

Ja und nein. Grundsätzlich empfiehlt es sich natürlich, primär noch nicht befallene Rechner und Server schnell herunterzufahren und anschließend vom Strom und insbesondere vom Netzwerk abzutrennen. Das unverzügliche Trennen der Netzwerkverbindung von noch unbefallenen Geräten kann gerade bei einem laufenden Ransomware-Befall wichtige Daten und Systeme vor der vernichtenden Verschlüsselung retten. Diese Maßnahmen sollten aber von einem Ihrer IT-Mitarbeiter durchgeführt werden – das einfache, unbedachte Abziehen des Strom-Steckers einer zum Beispiel virtualisierten Serverlandschaft kann ähnlich schlimme Folgen haben, wie der eigentliche Virenbefall.

Isolation

Frage: Kann man Computer, die von Viren befallen sind, nicht einfach isolieren?

Ja, eine erste Isolation erreichen Sie, indem Sie den betroffenen Rechner umgehend aus dem Netzwerk entfernen. Dies sollte serverseitig über Ihren Domänen-Controller passieren, aber auch physikalisch durch die Unterbrechung der Netzwerkverbindung über das Entfernen des Netzwerkkabels oder die Unterbrechung der WLAN-Verbindung. Befallene Systeme sollten auch nach der Beseitigung des Virus nicht ohne vorherige Prüfung durch einen Spezialisten wieder in das Netzwerk eingebunden werden! Die sicherste Variante ist es, den Rechner komplett durch ein neues Gerät zu ersetzen.

Offline-arbeiten?

Frage: Was heißt „offline Arbeiten“ und warum sollte ich mich damit beschäftigen?

Im Ernstfall ist die eingeschränkte Arbeit ohne digitale Daten, also auf Papier, besser, als den Verlust der gesamten IT-Infrastruktur zu riskieren. Halten Sie für diesen Fall wichtige Daten, beispielsweise Kundenstammdaten, Mitarbeiterstammdaten, Daten aus dem Controlling, Leistungsverzeichnisse und Zeitvorgaben in Papierform vor und aktualisieren Sie diese zum Beispiel halbjährlich. Wenn Sie einen Befall Ihrer Systeme bemerken, können Sie ihre wichtigsten betrieblichen Abläufe dadurch einige Tage auch ohne Zugriff auf Ihre digitalen Systeme aufrechterhalten.

Ausfallzeit so gering wie möglich halten (finanziellen Schaden minimieren)

Frage: Warum ist es so wichtig, schnell zu agieren und keine Zeit zu verlieren?

Jeder Tag, an welchem Ihr alltäglicher Betriebsablauf durch einen Ausfall der IT-Systeme gestört ist, kostet Sie auf verschiedensten Ebenen viel Geld. Von dem Verlust wichtiger Kunden, deren Reklamationen Sie nicht mehr bearbeiten können, weil Ihnen wichtige Eckdaten über die

Dienstleistung und das Objekt fehlen, bis hin zu unproduktiven Mitarbeitern, die Sie nach Hause schicken müssen, weil ihre Computer unbrauchbar geworden sind. Jede Stunde, die der Befall länger anhält, kostet Sie eine Menge Geld. Je kürzer Sie den Ausfall durch gute Präventionsmaßnahmen und Soforthilfen wie das Thema „Offline arbeiten“ halten, desto weniger wird Sie der ungeplante (temporäre) Verlust Ihrer IT-Systeme kosten.

IT-Dienstleister umgehend informieren

Frage: Wen sollte ich informieren, wenn ich einen Virenbefall bemerke?

Grundsätzlich sollten Sie sofort ihre eigenen IT-Mitarbeiter informieren, sofern Sie nicht von diesen auf den Angriff aufmerksam gemacht wurden. Die zweite Nummer, die Sie anrufen, ist die Ihres IT-Dienstleisters. Holen Sie sich umgehend Ihre internen und externen Fachleute dazu. Tipp: Notieren Sie sich den Ablauf bzw. eine Kontaktkette im Rahmen Ihres EDV-Notfallplans. Bricht erst einmal Panik aus, werden Sie froh sein, sich an einem schriftlichen Ablauf orientieren zu können.

EDV-Notfallplan strikt verfolgen (Ruhe bewahren)

Auf „Grunddaten“ zurückgreifen (Basics)

Frage: Was sind Grunddaten und woher weiß ich, was ich im Ernstfall benötige?

Um die Frage zu klären, möchten wir Sie auffordern, sich das Szenario vorzustellen, dass Sie plötzlich keinen Zugriff mehr auf jegliche EDV-Systeme haben. Für welche Daten wären Sie in dem Moment dankbar, wenn alles nicht mehr zur Verfügung stünde? Lohndaten, Stammdaten der Kunden, Leistungsbeschreibungen der Kunden, Telefonnummern von Mitarbeitern, Handelsregisterauszüge, Arbeitsverträge, Bankverbindungen, Rechnungen der letzten 12 Monate – das alles sind heute Selbstverständlichkeiten für Sie, die Sie in einem solchen Szenario zu schätzen lernen. Speichern Sie diese Grunddaten regelmäßig auf zum Beispiel externen Festplatten oder drucken Sie gewisse Zusammenfassungen aus, so dass die wesentlichsten Informationen auf Papier, also als „analoges Backup“ vorliegen.

Frage: Was ist ein EDV-Notfallplan?

Ein EDV-Notfallplan ist ein Dokument, welches die wichtigsten Systemeigenschaften Ihrer IT-Landschaft beschreibt und auch einen Ablaufplan für ein Worst-Case-Szenario beinhaltet. Notieren Sie sich Handlungsreihenfolgen und Kontaktlisten, welche die Kontaktdaten Ihrer IT-Dienstleister beinhalten. Skizzieren Sie einen Ablaufplan, was Sie machen würden, wenn ein Virenbefall Ihre Systeme betrifft oder auch ein Feuer den Serverraum vernichtet.

Wiederherstellung grundlegend notwendiger Daten – Geschäftsbetrieb aufrechterhalten

Prüfung – was kann wiederhergestellt werden?

Frage: Wie finde ich heraus, welche Daten wiederhergestellt werden können?

Die Antwort auf diese Frage ist von der IT-Landschaft, dem Virus oder Angriff, dem Sie ausgesetzt waren und in ganz entscheidender Rolle auch von den vorher getroffenen Präventionsmaßnahmen abhängig. Der Verlauf einer Attacke ist immer individuell und wird durch viele Faktoren beeinflusst. Versuchen Sie, sich gemeinsam mit Ihren IT-Mitarbeitern und Ihren IT-Dienstleistern einen Blick aus

der Vogelperspektive zu verschaffen – möglicherweise finden Sie Datensicherungen oder einzelne Dateien, die von dem Angriff verschont geblieben und noch brauchbar sind.

Prüfung, wie schwerwiegend der Vorfall ist (Meldepflicht)

Meldung der zuständigen Aufsichtsbehörde (falls zutreffend)

Frage: Wer prüft, ob ein meldepflichtiger Vorfall vorliegt?

Grundsätzlich ist bei dem Verdacht, dass personenbezogene Daten abhandengekommen sein könnten, Ihr (interner oder externer) Datenschutzbeauftragter zu Rate zu ziehen. Er kann beurteilen, ob durch den Vorfall eine Meldepflicht gegenüber der Aufsichtsbehörde besteht.

72-Stunden-Regel zur Prüfung des Vorfalls einhalten

Frage: Gibt es eine Frist, in welcher der Vorfall der Aufsichtsbehörde gemeldet werden muss?

Ja, wenn ein möglicher Datenschutzverstoß erkannt wurde, beginnt die 72-stündige Frist zur Bearbeitung der Meldung an die zuständige Aufsichtsbehörde. Zusätzlich muss das Risiko der Betroffenen (die Personen, deren Daten von dem Vorfall betroffen sind) abgeschätzt werden. Auch dies wird Ihr Datenschutzbeauftragter übernehmen. Wird das Risiko der Betroffenen als nicht gering eingeschätzt, sind diese über den Vorfall zu informieren (Artikel 34 Abs. 2 DSGVO).

Information der betroffenen Personen (und möglicherweise betroffene Personen)

Je nach Ausmaß: Information der Öffentlichkeit

Frage: Warum muss die Öffentlichkeit über den Vorfall informiert werden?

Diese Frage lässt sich nicht pauschal beantworten. Je sensibler und weitreichender der Datenverlust ist, desto transparenter wäre eine Veröffentlichung des Vorfalls. Als Adressaten der Information stehen Kunden und Mitarbeiterinnen / Mitarbeiter als direkt vom Vorfall Betroffene an erster Stelle. Hier gilt es, zeitnah eine Kommunikation mit den jeweiligen IT-Sicherheitsexperten von Unternehmen und Kundenseite zu ermöglichen sowie darüber hinaus auch die Schäden soweit möglich kommunizieren und damit auch die daraus resultierenden Verspätungen: Lohn, Faktur, Berichtswesen etc.

Bei einer breiteren öffentlichen Information muss jedoch abgewogen werden, ob der Nutzen der Transparenz größer ist als der mögliche Imageschaden durch die Veröffentlichung. Insofern muss jeder betroffene Betrieb diese Frage individuell beantworten, wenngleich eine Meldung gegenüber den Behörden u.U. verpflichtend ist (s. vorheriger Punkt).

Textform

Frage: Wie müssen die Betroffenen informiert werden?

Zur Information der Betroffenen über den Vorfall empfiehlt sich definitiv die Schriftform. Sie können somit nachweisen, dass Sie den Betroffenen über das Geschehene informiert, das Risiko abgeschätzt und ihn über die möglichen Folgen aufgeklärt haben. Verzichten Sie, in Ihrem eigenen Interesse, auf telefonische Bekanntgaben.

Motiv des Angriffs herausfinden?

Frage: Kann ich herausfinden, warum gerade ich angegriffen wurde?

Auch diese Frage ist immer individuell zu beantworten. In den meisten Fällen werden Sie mit Hilfe von Spezialisten herausfinden, wie der Virus in Ihre IT-Landschaft gelangt ist. Hingegen wird in den wenigsten Fällen aufgeklärt, wer es mit dem Virus auf Sie abgesehen hat. Leider ist das Internet zur Nachverfolgung der Täter zu groß und zu anonym. Es gelingt selten, diese zu identifizieren.

Ggfs. Versicherer informieren

Frage: Warum sollte ich meine Versicherung informieren?

Es gibt verschiedene Policen, welche die Kosten, die anfallen, wenn Sie einer Cyberattacke zum Opfer gefallen sind, übernehmen. Wenn Sie eine solche Versicherung abgeschlossen haben, sollten Sie auch daran denken, Ihren Versicherer umgehend über den Vorfall zu informieren, um eine entsprechende Übernahme anfallender Kosten zu gewährleisten. Die Versicherer haben häufig auch hilfreiche Kontakte und Spezialisten, die Ihnen möglicherweise beistehen können. Ein erst „am Ende“ gemeldeter Fall könnte von der Versicherung abgelehnt werden und Ihre Schadensersatzansprüche minimieren.

Gründliche Nachbereitung der Ursache (inkl. Einfallstore)

Identifikation der Ursache

Frage: Weiß man, was passiert ist, wenn alles wieder funktioniert?

Das Motiv und die Ursache des Angriffs werden häufig in der Phase der Nachbereitung identifiziert. Sie sollten, wenn Sie das Schlimmste überstanden haben, aus dem Vorfall lernen und die Sicherheitslücke nachhaltig sowie weitere Einfallstore schließen.

Strafanzeige?

Frage: Kann man nach einem Vorfall eine Strafanzeige erstatten?

Ja, man kann und sollte eine Strafanzeige aufgeben. Die Täter werden leider häufig nicht gefasst, dennoch ist es ratsam, dies zu tun. Das Erstatten einer Strafanzeige kann auch eine verpflichtende Klausel im Rahmen Ihrer Cyberversicherungspolice sein (wenn vorhanden).

In einigen Bundesländern, z.B. aktuell per Presseaufruf in Hamburg, ist auch der Verfassungsschutz an einer Meldung, ggfs. anonym, im Rahmen seiner Maßnahmen zum Wirtschaftsschutz interessiert.

Herausgeber:

Bundesinnungsverband des Gebäudereiniger-Handwerks
Dottendorfer Straße 86
53129 Bonn
www.die-gebaeudedienstleister.de
T: +49-228-917750
Mail: biv@die-gebaeudedienstleister.de