Leitfaden zum ARAG CyberSchutz

PDF27679 4.2017

Inhaltsverzeichnis

Wir kümmern uns – Ihr neuer ARAG CyberSchutz

Auch kleineren Betrieben bietet die Digitalisierung von Daten große Vorteile. Damit steigt jedoch nicht nur die Effizienz, sondern auch das Risiko eines Online-Angriffs auf die IT-Systeme. Gut, dass Sie mit ARAG CyberSchutz souverän vorgesorgt haben!

Damit Sie Ihre neu gewonnene Sicherheit genießen können, soll Ihnen dieser Leitfaden in Ihrem Betriebsalltag eine Hilfestellung sein. Denn je besser Sie und Ihre Mitarbeiter sich und Ihre IT-Systeme schützen, desto geringer ist das Risiko eines Cyber-Angriffs. Und umso mehr Freiheiten haben Sie, sich auf Ihren Betrieb zu konzentrieren.

Sie haben einen Cyber-Schadenfall und brauchen Hilfe?
Rufen Sie uns an unter

0211 9890-1405

Wichtig für Sie: Im Falle eines Cyber-Schadens (zum Beispiel nach einem Hacker-Angriff) möchten wir Ihnen schnell und effektiv weiterhelfen. Dafür ist es wichtig, dass auf Ihren versicherten PCs eine Software installiert ist, die das Aufschalten per Remote (Fernzugriff) unterstützt. Hierfür empfehlen wir die Software „Teamviewer" in seiner aktuellsten Version – die Möglichkeit zum Download finden Sie unter folgendem Link: https://www.teamviewer.com/

Auf Sicherheit programmiert

Wir möchten, dass Sie Ihre Unabhängigkeit als Unternehmer genießen. Damit das auch so bleibt, wenn Sie mal doch von einem Online-Angriff betroffen sein sollten, ist es wichtig, bereits im Vorfeld gut vorbereitet zu sein. So können wir sicherstellen, dass wir Ihnen im Fall der Fälle wirklich helfen können:

1. Aktualität, Lizensierung und Modifikation der eingesetzten Programme und Systeme

Sobald eine Sicherheitslücke eines Programms oder eines Systems bekannt geworden ist, wird diese auch unmittelbar von Hackern ausgenutzt. Dies geschieht meistens unter Verwendung von entsprechender Schadsoftware.

Daher sind die bei Ihnen zum Einsatz kommenden Programme und Computersysteme regelmäßig auf ihre Aktualität hin zu überprüfen. Informationsquellen hierfür sind zum Beispiel die Webseiten vom Bundesamt für Sicherheit in der Informationstechnik, kurz BSI, (zu finden unter www.bsi-fuer-buerger.de oder www.buerger-cert.de) oder von *heise online* unter www.heise.de.

Die von den jeweiligen Herstellern empfohlenen und zur Verfügung gestellten Sicherheitsupdates für Betriebssystem, Büro-Anwendungen, Internet-Browser inklusive Software-Erweiterungen (auch Plug-Ins genannt) und sonstiger wichtiger Applikationen sind zeitnah zu installieren. Hierzu stehen in den meisten Fällen vom Hersteller bereitgestellte automatisierte Updatefunktionen zur Verfügung.

Es dürfen keine Programme zum Einsatz kommen, für die der Hersteller die weitere Wartung eingestellt hat.

Für die Nutzung der eingesetzten Programme dürfen nur entsprechend leistungsfähige Computersysteme und Zusatzgeräte eingesetzt werden. Hierbei ist mindestens den Empfehlungen/Anforderungen der Software-Anbieter zu folgen. Informationen zu Leistungsdaten von IT-Systemen (Hardware) oder zu den System-Anforderungen von Programmen (Software) sind in den meisten Fällen aus den Produktinformationen der entsprechenden Hersteller zu ersehen. Diese liegen entweder in gedruckter Form (Produktblätter, Prospekte usw.) vor oder sind im Internet zu recherchieren.

Auf geschäftlich genutzten Systemen sollten nur Programme installiert sein, die zur Aufgabenbewältigung innerhalb der normalen Geschäftstätigkeit benötigt werden.

Die eingesetzten Programme müssen entsprechend ihrer Nutzung lizensiert sein. Wichtig für Sie: Die Lizenz-Schlüssel für die eingesetzte Software sollten separat und sicher (entweder auf Papier oder als Dateien) aufbewahrt werden.

Nicht benötigte Programme und Dienste auf Systemen sollten deinstalliert bzw. deaktiviert werden. Dadurch wird die mögliche Angriffsfläche eines IT-Systems reduziert.

Bestehende Schutzfunktionen eines Systems dürfen nicht durch Manipulation am Betriebssystem und an Programmen (zum Beispiel durch das Einspielen von sogenannten Patches[1]) oder durch zusätzliche Installation von Programmen (zum Beispiel durch sogenannte Jailbreaks[2]) umgangen oder gänzlich außer Kraft gesetzt werden.

2. Einsatz von Virenschutzmaßnahmen

Zum Schutz vor Malware (zum Beispiel Viren, Trojaner) sind entsprechende Virenschutz-Programme einzusetzen.

Diese sind regelmäßig zu aktualisieren (Virenschutz-Software und Malware-Signaturen).

Wichtig ist, dass die Virenschutz-Programme Funktionen wie Heuristik (Analyse und Schlussfolgerung) und Anomalie-Erkennung (Entdecken von Unregelmäßigkeiten im Netzwerk oder auf Systemen) enthalten. Aufgrund der zunehmenden Gefährdungslage sollten außerdem bevorzugt Programme mit Sandbox-Funktionen (Analyse in einer gekapselten Umgebung) zum Einsatz kommen.[3] Hierbei wird unbekannte Software in einer gekapselten Umgebung (Sandbox) zur Ausführung gebracht und auf schädlichen Inhalt überprüft. Sollte die Software schädliche Inhalte enthalten, wird sie automatisch beendet und gelöscht. Dabei werden die übrigen im Betrieb befindlichen Programme nicht berührt bzw. infiziert.

Ob die eingesetzten Virenschutz-Produkte die genannten Funktionen enthalten, ist bei Bedarf den Produktinformationen der Hersteller zu entnehmen. Bei kostenfreien Produkten sind diese Funktionen meistens nicht enthalten oder werden nach Ablauf einer Testperiode (meistens 30 Tage) wieder deaktiviert.

Neben der regelmäßigen Funktionskontrolle bei der Echtzeiterkennung sollten auf den System-Festplatten regelmäßig sogenannte Full-Scans (vollständige Virensuchläufe) durchgeführt werden.

Sollten innerhalb von lokalen Netzwerken[4] zentrale Virenschutzlösungen zum Einsatz kommen, ist darauf zu achten, dass verschlüsselter Datenverkehr vor der Überprüfung auf Malware entschlüsselt wird. Verschlüsselte Daten können nicht auf Malware untersucht werden. Sollte eine Entschlüsselung vorab nicht möglich sein, ist ein zusätzlicher Virenschutz auf den Endgeräten durchzuführen, auf denen die Daten entschlüsselt vorliegen.

1 Ein Patch ist eine Korrektur für eine Software, um Sicherheitslücken zu schließen, Fehler zu beheben oder bislang nicht vorhandene Funktionen nachzurüsten.
2 Als Jailbreak bezeichnet man das Entfernen von Nutzungsbeschränkungen auf IT-Systemen (z.B. Smartphones), die vom Hersteller serienmäßig vorgegeben sind. Mit der Installation eines Jailbreaks durchbricht man die Beschränkungen.
3 Mögliche Anbieter solcher Produkte sind ESET, Antivir oder Symantec.
4 LAN = Local Area Network = internes Netzwerk

3. Einsatz von Firewalls und VPN[5]-Zugängen

Die Kommunikation im Netzwerk oder zwischen Netzwerken (zum Beispiel zwischen lokalem Netzwerk und Internet) muss durch geeignete Firewalls abgesichert werden. Firewalls kontrollieren alle Verbindungen von und zu internen Rechnern und überprüfen sowohl Anfragen ins Internet als auch Daten, die aus dem Internet an die internen Systeme gesendet werden. Sie schützen so vor Angriffen (zum Beispiel unerlaubte Verbindungsversuche) von außen.

Firewalls sind bereits integraler Bestandteil in den meisten modernen Betriebssystemen bzw. installierbaren Virenschutzlösungen. In diesem Fall spricht man von sogenannten „Personal Firewalls". Bei lokalen Netzwerken können auch separate, eigenständige Firewall-Systeme zum Einsatz kommen.

Bei der Nutzung von elektronischen Zugängen von außen auf das lokale Netzwerk bzw. auf interne Systeme sind diese durch entsprechende VPN-Technologien abzusichern, das heißt über eine verschlüsselte Verbindung zu nutzen.[6] Solche Zugänge dürfen nur von vertrauenswürdigen Partnern und Mitarbeitern verwendet werden. VPN-Technologien umfassen Verfahren der Benutzeridentifizierung und -autorisierung (zum Beispiel durch Benutzername und Kennwort) sowie eine Verschlüsselung der übertragenen Daten zwischen den Kommunikationspartnern. Zusätzlich sollten VPN-Zugänge auf die notwendige Nutzungszeit beschränkt werden.

Weitere Details sind den Kapiteln „Betrieb und Nutzung von drahtlosen Netzwerken (WLANs)" und „Benutzerindividuelle Kennungen und Passwörter" zu entnehmen.

4. Regelmäßige Datensicherungen

Die Daten auf den eingesetzten Systemen müssen regelmäßig (mindestens wöchentlich) gesichert werden. Es empfiehlt sich bei unregelmäßiger Systemnutzung (zum Beispiel keine tägliche Nutzung) mindestens nach Abschluss der Tätigkeiten an einem System die durchgeführten Änderungen an den Daten zu sichern.

Durch das regelmäßige Erstellen von Sicherheitskopien Ihrer Daten (Backup) sind diese weitestgehend vor Verlust geschützt (Minimierung des Datenverlustes).

Während der normalen Geschäftstätigkeit ist eine physische Trennung der Backup-Systeme bzw. Datenträger (zum Beispiel externe Festplatte) von den Systemen, an denen normal gearbeitet wird, zu gewährleisten. Diese Trennung wird auch als Air-Gap bezeichnet und verhindert, dass bei einem Virenbefall die Daten auf den Sicherungsmedien nicht auch infiziert werden.

Externe Backup-Medien sind eindeutig (zum Beispiel mit Datum und Inhalt) zu kennzeichnen und separat und sicher aufzubewahren (zum Beispiel anderes Gebäude oder Sicherungsschrank).

In regelmäßigen Abständen ist die korrekte Funktion der Datensicherung durch das Zurückspielen von gesicherten Daten (Restore) zu überprüfen. Backup-Programme enthalten grundsätzlich Funktionen zum Zurückspielen der Daten.[7]

5. Betrieb und Nutzung von drahtlosen Netzwerken (WLANs)

Beim Betrieb von drahtlosen Netzwerken, sogenannten WLANs[8], wird zwischen internen (geschlossenen) und externen (offenen) WLANs unterschieden.

Interne WLANs sollten grundsätzlich von externen Netzwerken getrennt werden. Hier müssen entsprechende Sicherungsmaßnahmen wie Zugangskontrolle (zum Beispiel durch SSID[9] und Kennwort) und sichere Verschlüsselungsstandards bei der Datenübertragung (zum Beispiel WPA2[10]) zum Einsatz kommen.

Gastzugänge im internen WLAN sind nach Möglichkeit zu vermeiden oder müssen physisch vom internen Netzwerk getrennt werden. Eine Ausnahme bilden hier die Zugänge für vertrauenswürdige externe Dienstleister (zum Beispiel für Wartungsarbeiten).

Beim Betrieb von Hybrid-Lösungen (zum Beispiel offenes und geschlossenes WLAN in einem Internet-Café) ist auf eine strikte Trennung zwischen internen und externen WLANs zu achten. Weitere Details hierzu sind auch im Kapitel „Einsatz von Firewalls und VPN-Zugängen" zu finden.

Bei der Nutzung von offenen WLANs (zum Beispiel über Hotspots) sollte grundsätzlich bei der Übertragung von sensiblen Daten darauf geachtet werden, dass die Übertragung verschlüsselt erfolgt. Ansonsten könnte ein Angreifer sämtlichen Datenverkehr mitschneiden und entsprechend ausnutzen (zum Beispiel für Identitätsmissbrauch).

Bei offenen WLANs ist zwischen kostenpflichtigen und freien WLANs zu unterscheiden. Bei kostenpflichtigen WLANs sind zum Schutz vor finanziellem Schaden durch Fremdmissbrauch für den Zugang sichere Benutzerkonten und Kennworte zu verwenden.
Weitere Details sind den Kapiteln „Einsatz von Firewalls und VPN-Zugängen" und „Benutzerindividuelle Kennungen und Passwörter" zu entnehmen.

5 VPN = Virtual Private Network
6 Mögliche Programme (VPN-Tools) wären z.B. TunnelBear, Hotspot Shield, Cyberghost VPN oder PC-WELT Anonym Surfen VPN.
7 Mögliche Produkte für Sicherheitskopien Ihrer Daten und deren Zurückspielen sind z. B. „Personal Backup" und „Acronis True Image"
8 WLAN = Wireless Local Area Network = drahtloses lokales Netzwerk
9 SSID = Service Set Identifier = Name eines einzelnen WLAN's
10 WPA2 = Wi-Fi Protected Access 2 = Implementierung eines Sicherheitsstandards für Funknetzwerke nach bestimmten WLAN-Standards und Nachfolger von WPA

6. Benutzerindividuelle Kennungen und Passwörter

Bei der Arbeit mit IT-Systemen müssen Benutzerkonten mit verschiedenen (abgestuften) Berechtigungen verwendet werden, das heißt es muss ein stufiges Rechtekonzept mit normalen und administrativen Benutzerkonten geben. Alle gängigen Betriebssysteme bieten die Möglichkeit, sich als normaler Nutzer oder als Administrator anzumelden.

Für die tägliche Bürotätigkeit sollten ausschließlich einfache Benutzerkonten mit eingeschränkten Rechten verwendet werden.

Auf keinen Fall dürfen für den Zugriff auf das Internet Konten mit Administrator-Rechten verwendet werden. Wenn ein Angreifer nämlich Kenntnis über administrative Zugangsdaten mit erweiterten Rechten erlangen sollte, könnte er diese bei seinen Angriffen auf interne Netzwerke ausnutzen und einen vergleichsweise großen Schaden verursachen.

Alle Benutzerkonten müssen durch die Verwendung von sicheren Passwörtern (zum Beispiel 10 Stellen, Groß- und Klein-Buchstaben, Ziffern, Sonderzeichen) geschützt werden.

Außerdem sollten bei der Nutzung von Online-Diensten (zum Beispiel E-Mail, Online Shops, Online Banking, Foren, Soziale Netzwerke) unterschiedliche Passwörter je genutztem Dienst verwendet werden.

Passwörter müssen regelmäßig (zum Beispiel alle 60 Tage) geändert werden. Es macht Sinn, die Mitarbeiter auf die Notwendigkeit der regelmäßigen Passwort-Änderung hinzuweisen und dies ggf. regelmäßig zu hinterfragen. Moderne Netzwerk-Zugangssysteme (zum Beispiel Windows-Server) bieten Möglichkeiten, die regelmäßige Änderung und die Nutzung von komplexen Passwörtern automatisiert zu erzwingen.

Bei der Inbetriebnahme von neuen Systemen sollten vom Anbieter oder Hersteller voreingestellte Standard-Passwörter (zum Beispiel Administrator, Guest, User, System, Default) sofort geändert werden.

7. Einsatz von Verschlüsselungstechniken

Verschlüsselungstechniken bieten die Möglichkeit, die Erfordernisse des Bundesdatenschutz-Gesetzes (kurz: BDSG) nach Zugangskontrolle, Zugriffskontrolle, Ü bertragungskontrolle usw. bei der Arbeit mit personenbezogenen o der s onstigen s ensiblen Daten zu gewährleisten.

Bei der Übertragung solcher Daten im Internet (zum Beispiel beim Online Banking oder Online Shopping) sollten diese ausschließlich über eine verschlüsselte Verbindung erfolgen. Durch die verschlüsselte Übertragung werden Daten vor dem Ausspähen durch Dritte und ggf. vor Missbrauch geschützt.

Jeder seriöse Online-Dienst bietet eine Möglichkeit zur verschlüsselten Datenübertragung an, beispielsweise im Internetbrowser durch die Nutzung des sicheren Kommunikationsprotokolls "HTTPS".

Sensible Daten (zum Beispiel personenbezogene Daten, Bankdaten, Benutzerkennungen und Passwörter) sollten ausschließlich verschlüsselt gespeichert werden. Sollte dies nur mit einem größeren Aufwand möglich sein, sind diese Daten durch entsprechende Passwörter zu schützen.[11]

8. PCI Standards

Der PCI DSS (Payment Card Industry Data Security Standard) ist ein Sicherheitsstandard mit strengen Vorgaben, der den sorgfältigen und geschützten Umgang mit Kreditkartendaten sicherstellen soll. Dieser Standard wurde von den fünf wichtigsten Kreditkartenunternehmen (Visa, MasterCard, American Express, JCB, und Discover Financial Services) ins Leben gerufen und umfasst zwölf technische und organisatorische Anforderungen, die in unterschiedlichem Maße erfüllt sein müssen.

Jedes Unternehmen, das Kreditkartenzahlungen in irgendeiner Form akzeptiert, muss sich an die Sicherheitsvorgaben des PCI DSS halten. Hierbei sind die Größe und das Geschäft des Unternehmens und der Umfang der Kartentransaktionen unerheblich. Die PCI DSS Richtlinien betreffen sowohl Daten in digitaler Form, als auch jene, die nur papierhaft vorliegen. Das Unternehmen muss den Nachweis erbringen, dass es PCI compliant (PCI konform) ist.

Weitere Informationen hierzu können Sie bei Ihrem Payment-Dienstleister, der von Ihnen eingebundenen Hausbank oder unter folgendem Link finden:

https://www.pcisecuritystandards.org/

Maßgeblich für den Leistungsumfang sind die dem Versicherungsvertrag konkret zugrunde gelegten Allgemeinen Versicherungs-bedingungen zu ARAG Business Aktiv CyberSchutz 2017 (Stand 1.2017), insbesondere Ziffer 1.8 Teil D. Die Obliegenheiten aus dem Bedingungswerk finden Sie auch als Anlage zu diesem Dokument.

11 Anwendungen zur Verarbeitung sensibler Daten (z.B. Abrechnungssysteme im Personalbereich) bieten meistens eine automatische Verschlüsselung bei der Speicherung an. Ansonsten sollten separate Lösungen zur Verschlüsselung von Speicherbereichen auf Servern zum Einsatz kommen (z.B. Microsoft BitLocker).

Anlage: Auszug aus dem Bedingungswerk (ARAG Business Aktiv CyberSchutz 2017, Stand 1.2017, Ziffer 1.8 Teil D)

Der Versicherungsnehmer hat angemessene, branchenübliche, dem Stand der Technik entsprechende technische sowie organisatorische Schutzmaßnahmen zu ergreifen. Hierzu gehören insbesondere:

- Datensicherung. Der Versicherungsnehmer hat eine angemessene, jedoch mindestens einmal wöchentliche Datensicherung vorzunehmen, das heißt Duplikate der versicherten Daten und Programme anzufertigen. Diese sind so aufzubewahren, dass bei einer Beschädigung der Originale voraussichtlich nicht gleichzeitig auch die Daten der Datensicherung betroffen sind. Die technischen Einrichtungen zur Datensicherung müssen dem Stand der Technik entsprechen;
- Der Versicherungsnehmer stellt sicher, dass Form und Struktur der Daten auf dem Sicherungsdatenträger so beschaffen sind, dass deren Rücksicherung technisch möglich ist. Zum Beispiel durch Sicherung mit Prüfoption (Verify) und regelmäßiger Durchführung von Rücksicherungstests;
- Der Versicherungsnehmer stellt sicher, dass die eingesetzten Programme aktuell vom Hersteller unterstützt werden. Die Vorschriften und Hinweise des Herstellers zur Installation, Wartung und Pflege der Hard- und Software sind zu beachten. Aktualisierungen müssen nach Bereitstellung durch den Hersteller unverzüglich installiert werden;
- Der Versicherungsnehmer nimmt übliche, ständig aktualisierte Schutzmaßnahmen gegen den bestimmungswidrigen Zugriff auf gespeicherte Daten vor. Zum Beispiel durch Anti-Viren-Programme, Firewalls, Autorisierung, Verschlüsselung. Bestehende Schutzfunktionen werden nicht durch Manipulation an oder durch zusätzliche Installation von Programmen (zum Beispiel Jailbreaks) umgangen oder gänzlich außer Kraft gesetzt;
- Es liegt ein Berechtigungsmanagement mit abgestuften Befugnissen vor. Passwörter und Accounts eines Mitarbeiters werden nach Beendigung des Arbeitsverhältnisses unverzüglich gesperrt;
- Personenbezogene Daten und andere sensible Daten werden bei der Datenspeicherung, beim Datenversand und bei der Datenübertragung geschützt, zum Beispiel durch Verschlüsselung und/oder durch passwortgeschützten Zugang;
- Sofern die Bezahlung mit Kreditkarten erlaubt ist, ist mindestens der Sicherheitsstandard der Kreditkartenindustrie (Payment Card Industry Data Security Standards – PCI-DSS) anzuwenden.
- Vor der Veröffentlichung von digitalen Medieninhalten sind die Inhalte fachgerecht zu überprüfen.

Auf die Obliegenheiten bei und nach Eintritt eines Versicherungsfalls gemäß Ziffer 12.2 der Allgemeinen Bedingungen zum ARAG Business Aktiv CyberSchutz und CyberSchutz Plus wird hingewiesen. Auf die Rechtsfolgen im Falle der Verletzung von Obliegenheiten gemäß Ziffer 12 der Allgemeinen Bedingungen zum ARAG Business Aktiv CyberSchutz und CyberSchutz Plus wird ausdrücklich hingewiesen.

Herausgeber:

ARAG Allgemeine Versicherungs-AG
ARAG Platz 1
40472 Düsseldorf