Leitfaden zu ARAG CyberSchutz

PDF27679 9.2017

Inhaltsverzeichnis

Auf Sicherheit programmiert – Ihr ARAG CyberSchutz

Auch kleineren Betrieben bietet die Digitalisierung von Daten große Vorteile. Dadurch steigt jedoch nicht nur die Effizienz, sondern auch das Risiko einer Online-Attacke. Gut, dass Sie mit dem ARAG CyberSchutz souverän vorgesorgt haben!

Damit ein Virus oder Hacker-Angriff idealerweise erst gar keinen Schaden in Ihrem Betrieb anrichten kann, geben wir Ihnen diesen Leitfaden an die Hand – als praktische Hilfestellung für digitale Betriebsprozesse. **Denn je besser Sie und Ihre Mitarbeiter sich und Ihre IT-Systeme schützen, desto geringer ist die Gefahr einer schädigenden Cyber-Attacke.**

Und falls es trotz der erforderlichen Sicherheitsmaßnahmen einmal dazu kommen sollte, sind wir für Sie da. Mit unserer Unterstützung **bewahren Sie Ihre Handlungsfähigkeit und schützen Ihr Betriebsvermögen.**
So können Sie sich weiter auf das Wesentliche konzentrieren: Ihr Geschäft!

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

0211 9890-1405

Fernzugriff – Kundenähe aus der Distanz

Wichtig für Sie: Im Falle eines Cyber-Schadens möchten wir Ihnen effektiv weiterhelfen. Damit Sie nach einem Virus oder Hacker-Angriff möglichst schnell wieder arbeitsfähig sind. Dafür ist es wichtig, dass auf Ihren versicherten PCs eine Software installiert ist, die das **Aufschalten per Remote (Fernzugriff)** unterstützt.

Hierfür empfehlen wir das Programm ***Teamviewer*** in seiner aktuellsten Version, das Sie hier herunterladen können:
https://www.teamviewer.com/

Maßgeblich für den Leistungsumfang sind die dem Versicherungsvertrag konkret zugrunde gelegten Allgemeinen Versicherungsbedingungen 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.

Sicher ist sicher: So schützen Sie Ihre IT-Systeme

Wir möchten, dass Sie Ihre Unabhängigkeit als Unternehmer genießen. Damit das auch nach einem Online-Angriff so bleibt, ist es wichtig, bereits im Vorfeld gut vorbereitet zu sein. Bitte befolgen Sie deshalb unbedingt sorgfältig alle nachfolgenden Sicherheitsmaßnahmen – zum Schutz Ihrer IT-Infrastruktur.

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

Überprüfen Sie Ihre Programme und IT-Systeme regelmäßig auf ihre Aktualität. Denn sobald eine Sicherheitslücke einer Software oder eines Systems bekannt geworden ist, wird diese unmittelbar von Hackern ausgenutzt. Dies geschieht meistens unter Verwendung von Schadsoftware. Informationsquellen hierzu sind zum Beispiel die Webseiten vom *Bundesamt für Sicherheit in der Informationstechnik,* kurz *BSI* (www.bsi-fuer-buerger.de, www.buerger-cert.de), oder von *heise online* (www.heise.de).

Bitte installieren Sie zeitnah die von den jeweiligen Herstellern empfohlenen und bereitgestellten Sicherheits-Updates für Betriebssystem, Büro-Anwendungen, Internet-Browser inklusive Software-Erweiterungen (Plug-Ins) und sonstiger wichtiger Applikationen. Hierzu stehen Ihnen in der Regel automatisierte Update-Funktionen zur Verfügung.

Es dürfen keine Programme zum Einsatz kommen, für die der Hersteller die weitere Wartung eingestellt hat. Zur Nutzung der Programme müssen zudem **hinreichend leistungsfähige Computersysteme und Zusatzgeräte** eingesetzt werden. Bitte folgen Sie hierbei mindestens den Empfehlungen beziehungsweise Anforderungen der Software-Anbieter. Informationen zu Leistungsdaten von IT-Systemen *(Hardware)* oder System-Anforderungen von Programmen *(Software)* finden Sie in den meisten Fällen in den Produktinformationen der Hersteller. Diese lassen sich entweder im Internet recherchieren oder liegen in gedruckter Form vor – zum Beispiel als Produktblatt oder Prospekt.

Auf betrieblich genutzten Systemen sollten nur Programme installiert sein, die Sie zur **Aufgabenbewältigung innerhalb Ihrer normalen Geschäftstätigkeit** benötigen.

Alle eingesetzten Programme müssen entsprechend ihrer Nutzung lizensiert sein. **Wichtig: Bewahren Sie die Lizenz-Schlüssel separat und sicher auf** – entweder auf Papier oder digital als Dateien.

Deinstallieren beziehungsweise deaktivieren Sie nicht benötigte Programme und Dienste. Dadurch wird die mögliche Angriffsfläche Ihres IT-Systems reduziert.

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

2. Einsatz von Virenschutzmaßnahmen

Setzen Sie zum Schutz vor Malware (zum Beispiel Viren und Trojaner) entsprechende Virenschutz-Programme ein. Aktualisieren Sie diese regelmäßig (Virenschutz-Software und Malware-Signaturen). Wichtig: Ihr Virenschutz sollte über Funktionen wie Heuristik (Analyse und Schlussfolgerung) und Anomalie-Erkennung (Entdecken von Unregelmäßigkeiten im Netzwerk oder auf Systemen) verfügen.

Aufgrund des stetig wachsenden Risikos einer Cyber-Attacke sollten außerdem bevorzugt Programme mit ***Sandbox*-Funktionen** zum Einsatz kommen.[3] Hierbei wird unbekannte Software in einer **gekapselten Umgebung *(Sandbox)*** zur Ausführung gebracht und analysiert. Sollte sie schädliche Inhalte enthalten, wird sie automatisch beendet und gelöscht – ohne dass die übrigen sich im Betrieb befindlichen Programme davon berührt oder infiziert werden.

Ob ein Virenschutz-Produkt die genannten Funktionen umfasst, können Sie den Produktinformationen des Herstellers entnehmen. Bei kostenfreien Produkten sind sie meistens nicht enthalten oder werden nach Ablauf einer Testperiode (meistens 30 Tage) deaktiviert.

Auf Ihren System-Festplatten sollten Sie nicht nur regelmäßig eine Funktionskontrolle bei der Echtzeiterkennung durchführen, sondern auch **vollständige Virensuchläufe –** sogenannte *Full-Scans.*

Sie setzen innerhalb lokaler Netzwerke[4] zentrale Virenschutzlösungen ein? Achten Sie in diesem Fall bitte darauf, dass verschlüsselter Datenverkehr **vor der Überprüfung auf Malware entschlüsselt** wird: Verschlüsselte Daten können nicht darauf untersucht werden. (Sollte eine Entschlüsselung vorab nicht möglich sein, muss ein **zusätzlicher Virenscan** auf den Endgeräten durchgeführt werden, auf denen die Daten entschlüsselt abgelegt sind.)

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 (zum Beispiel 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 von außen – zum Beispiel unerlaubte Verbindungsversuche.

Firewalls sind bereits integraler Bestandteil der meisten modernen Betriebssysteme beziehungsweise installierbaren Virenschutzlösungen. In diesem Fall spricht man von sogenannten *Personal Firewalls*. Bei lokalen Netzwerken können auch separate, eigenständige Firewall-Systeme zum Einsatz kommen.

Bei Nutzung elektronischer Zugänge von außen auf das lokale Netzwerk beziehungsweise auf interne Systeme sind diese durch entsprechende VPN-Technologien abzusichern, das heißt über eine verschlüsselte Verbindung zu nutzen.[6] Solche Zugänge dürfen ausschließlich von vertrauenswürdigen Partnern und Mitarbeitern verwendet werden. VPN-Technologien umfassen Verfahren der Benutzeridentifizierung und -autorisierung (zum Beispiel durch Benutzernamen und Kennwort) sowie eine Verschlüsselung der zwischen den Kommunikationspartnern übertragenen Daten. **Zusätzlich sollten VPN-Zugänge auf die notwendige Nutzungszeit beschränkt werden.** (Weitere Details: siehe Kapitel „Betrieb und Nutzung von drahtlosen Netzwerken (WLANs)" und „Benutzerindividuelle Kennungen und Passwörter".)

4. Regelmäßige Datensicherungen

Die Daten auf Ihren Systemen müssen regelmäßig (mindestens wöchentlich) gesichert werden. Sie nutzen Ihr System nur unregelmäßig (zum Beispiel nicht täglich)? Dann empfiehlt es sich, mindestens nach Abschluss der Tätigkeiten die an den Daten durchgeführten Änderungen zu sichern.

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

Während der normalen Geschäftstätigkeit muss eine **physische Trennung** der Backup-Systeme beziehungsweise Datenträger (zum Beispiel externe Festplatte) von den Systemen, an denen gearbeitet wird, gewährleistet sein. Diese Trennung wird auch als *Air Gap* bezeichnet: Sie verhindert, dass bei einem Virenbefall die Daten auf den Sicherungsmedien infiziert werden.

Externe Backup-Medien müssen eindeutig gekennzeichnet (beispielsweise mit Datum und Inhalt) sowie separat und sicher aufbewahrt werden, zum Beispiel in einem anderen Gebäude oder im Sicherungsschrank.

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

Vermeiden Sie Gastzugänge im internen WLAN nach Möglichkeit oder trennen Sie diese physisch vom internen Netzwerk. Eine Ausnahme bilden hier die Zugänge für vertrauenswürdige externe Dienstleister, beispielsweise für Wartungsarbeiten.

Bei der Übertragung sensibler Daten über offene WLANs (zum Beispiel Hotspots) sollten Sie immer sicherstellen, dass diese verschlüsselt erfolgt. Denn sonst könnte ein Hacker sämtlichen Datenverkehr mitschneiden und missbräuchlich verwenden, zum Beispiel für Identitätsdiebstahl.

Bei offenen WLANs unterscheidet man zwischen kostenpflichtigen und freien WLANs. **Verwenden Sie bei kostenpflichtigen WLANs für den Zugang sichere Benutzerkonten und Kennworte –** zum Schutz vor finanziellem Schaden durch Fremdmissbrauch. (Weitere Details: siehe Kapitel „Einsatz von Firewalls und VPN-Zugängen" und „Benutzerindividuelle Kennungen und Passwörter".)

Beim Betrieb von **Hybrid-Lösungen** – zum Beispiel offenes und geschlossenes WLAN in einem Internet-Café – muss auf eine strikte Trennung geachtet werden. (Weitere Details: siehe Kapitel „Einsatz von Firewalls und VPN-Zugängen".)

5 VPN = Virtual Private Network
6 Mögliche Programme (VPN-Tools) wären zum Beispiel *TunnelBear, Hotspot Shield, Cyberghost VPN* oder *PC-WELT Anonym Surfen VPN*.
7 Mögliche Produkte für Sicherheitskopien Ihrer Daten und deren Zurückspielen sind zum Beispiel *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 Berechtigungen verwendet werden. Richten Sie dazu bitte unbedingt ein **stufiges Rechtekonzept** mit normalen und administrativen Benutzerkonten ein.

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 darf der Zugriff auf das Internet über Konten mit Administrator-Rechten erfolgen! Denn wenn ein Online-Angreifer Kenntnis über administrative Zugangsdaten mit erweiterten Rechten erlangen sollte, könnte er damit bei seinen Attacken auf interne Netzwerke einen vergleichsweise großen Schaden verursachen.

Alle Benutzerkonten müssen durch die Verwendung von **sicheren Passwörtern** (zum Beispiel mit zehn Stellen, Groß- und Kleinbuchstaben, Ziffern sowie Sonderzeichen) geschützt sein. Außerdem sollten Sie bei der Nutzung von Online-Diensten (E-Mail, Online Shops, Online Banking, Foren, Soziale Netzwerke etc.) **jeweils ein anderes Passwort** nutzen.

Es ist wichtig, Passwörter **regelmäßig zu ändern**, zum Beispiel alle 60 Tage. Unser Tipp: Weisen Sie Ihr Team auf diese Notwendigkeit hin und fragen Sie gegebenenfalls nach, ob Ihre Mitarbeiter die Passwörter tatsächlich neu vergeben haben. Moderne Netzwerk-Zugangssysteme (zum Beispiel Windows-Server) bieten zudem Möglichkeiten, die regelmäßige Änderung und die Nutzung von komplexen Passwörtern automatisiert zu erzwingen.

Sie nehmen ein neues System in Betrieb? Dann sollten Sie vom Anbieter oder Hersteller **voreingestellte Standard-Passwörter** (zum Beispiel *Administrator, Guest, User, System* oder *Default*) unbedingt **sofort ändern**.

7. Einsatz von Verschlüsselungstechniken

Sie arbeiten mit personenbezogenen oder sonstigen sensiblen Daten? Moderne Verschlüsselungstechniken ermöglichen es Ihnen, die Erfordernisse des *Bundesdatenschutz-Gesetzes (BDSG)* zu gewährleisten – unter anderem hinsichtlich Zugangs-, Zugriffs- und Übertragungskontrolle.

Bei der Übertragung solcher Daten im Internet sollten diese ausschließlich über eine verschlüsselte Verbindung erfolgen. Zum Beispiel beim Online Banking oder Online Shopping. Dadurch werden die Daten vor dem Ausspähen durch Dritte und gegebenenfalls vor Missbrauch geschützt. Jeder seriöse Online-Dienst bietet eine Möglichkeit zur verschlüsselten Datenübertragung. Beispielsweise über das sichere Kommunikationsprotokoll ***HTTPS*** im Internet-Browser.

Ob personenbezogene Daten, Bankdaten, Benutzerkennungen oder Passwörter: **Speichern Sie sensible Daten ausschließlich verschlüsselt!** Sollte dies nur mit größerem 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. Er 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 sowie der Umfang der Kartentransaktionen unerheblich. Die Richtlinien betreffen sowohl Daten in digitaler Form als auch in Papierform. Das Unternehmen muss den Nachweis erbringen, dass es *PCI compliant (PCI konform)* ist.

Weitere Informationen hierzu finden Sie bei Ihrem Payment-Dienstleister, der von Ihnen eingebundenen Hausbank oder unter: https://www.pcisecuritystandards.org/

11 Anwendungen zur Verarbeitung sensibler Daten (zum Beispiel Abrechnungssysteme im Personalbereich) bieten meistens eine automatische Verschlüsselung bei der Speicherung. Ansonsten sollten separate Lösungen zur Verschlüsselung von Speicherbereichen auf Servern zum Einsatz kommen (zum Beispiel *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 zu 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