CI.Magazin

COMPUTER INSIDER – DIE SPEZIALISTEN FÜR IT IN DER ARZTPRAXIS

IT-Betreuung für Ihre Arztpraxis

Sehen wir uns auf der MEDICA 2019?

Sehr geehrte Damen und Herren, liebes Praxis-Team,

haben Sie auch aus den Medien erfahren, dass statistisch jedes zweite deutsche Unternehmen von Wirtschaftsspionage, Sabotage oder Datendiebstahl betroffen ist? Nachrichten wie diese sind es, die die IT-Security immer wieder in den Fokus rücken und zeigen, wie wichtig die Sicherheit von Unternehmensnetzwerken ist. Vielleicht haben Sie auch von GermanWiper und Ordinypt Wiper gehört? Es handelt sich dabei um ganz neue Malware-Typen, die aktuell ihr Unwesen treiben und die Daten befallener Systeme nicht nur verschlüsseln, sondern direkt unwiderruflich löschen. Stellen Sie sich das nur einmal vor!

In dieser Ausgabe unseres Kundenmagazins widmen wir uns deshalb verschiedenen Themen der IT-Sicherheit. Wir schauen, welche Rolle Ihre Mitarbeiter spielen – Stichwort IT-Security Awareness; wir berichten von den Gefahren, die durch Malware und Ransomware drohen; wir nehmen die vielen Endgeräte innerhalb von Unternehmensnetzwerken un die damit verbundene Endpoint Security in den Blic wir erklären, was das baldige Support-Ende diverse Microsoft-Produkte für die IT-Sicherheit bedeutet; wir stellen Ihnen die elektronische Archivierung vor, mit denen wichtige Unterlagen sicher hinterlegt werden können. Und zuletzt widmen wir uns noch der Zeiterfassung, denn mit diesem Thema müssen Sie sich schon bald zwangsläufig befassen.

Wir wünschen Ihnen viel Spaß beim Lesen!

Michael Olteanu
Geschäftsführender Gesellschafter
Computer Insider GmbH

IMPRESSUM

HERAUSGEBER
SYNAXON AG
Falkenstraße 31 | D-33758 Schloß Holte-Stukenbrock
Telefon 0 52 07 / 92 99 – 200 | Fax 0 52 07 / 92 99 – 296
e-mail info@synaxon.de | www.synaxon.de

REDAKTION
André Vogtschmidt (V.i.S.d.P.), Janina Kröger

LAYOUT / SATZ
Mirco Becker

ANSPRECHPARTNER
André Vogtschmidt | andre.vogtschmidt@synaxon.de

Stand 10 / 2019. Irrtümer und Druckfehler vorbehalten. Bildnachweise stock.adobe.com: # 246047493 © Thaut Images; # 175043095 © kaptn; # 207871235 © New Africa; # 243117139 © Brazhyk; # 284650614 © Monster Ztudio; # 238952467 © ASDF; # 261216495 © Pixel-Shot

Inhaltsverzeichnis

IT-Security Awareness: Erkennen Sie Gefahren?

Die „Schwachstelle Mensch“ gilt als einer der größten Risikofaktoren für die IT-Sicherheit von Unternehmen. Das Problem: Vielen Mitarbeitern mangelt es sowohl an technischem Grundwissen als auch am Gespür für mögliche Bedrohungen aus dem Internet. Was Sie tun können? Schulen Sie die IT-Security Awareness!

„Schwachstelle Mensch“

Es ist leider so: Eine gute Sicherheitsstrategie und die entsprechende technische Ausstattung reichen nicht aus, um die IT-Sicherheit eines Unternehmens zu gewährleisten. Vielmehr muss jeder einzelne Anwender innerhalb eines IT-Netzwerkes die Sicherheitsstrategie auch verinnerlichen und ein gewisses Grundwissen sowohl im Umgang mit der IT-Technik als auch in Bezug auf Cyber-Sicherheit vorweisen können.

Denn: Oft sind es Mitarbeiter, die Gefahren aus dem Internet nicht erkennen und durch ihr unachtsames Verhalten dafür sorgen, dass Daten in die falschen Hände geraten oder Systeme beispielsweise durch Malware kompromittiert werden. Damit wird der Mensch zu einem der größten Risikofaktoren für die IT-Sicherheit Ihres Unternehmens. Die Rede ist hierbei von „der Schwachstelle Mensch“.

IT-Security Awareness – was ist das genau?

Mit IT-Security Awareness ist das Bewusstsein des Menschen für mögliche Bedrohungen für IT-Systeme gemeint. Und dieses Bewusstsein lässt sich durch eine Sensibilisierung schulen. Oder anders gesagt: Die Mitarbeiter eines Unternehmens entwickeln einen Riecher für potenzielle Gefahren – und werden sozusagen zur letzten Barriere in Sachen Cyber-Sicherheit. Dafür gibt es spezielle Schulungsangebote.

Wie sich Lücken im IT-Wissen schließen lassen

Das Thema IT-Sicherheit ist natürlich sehr umfassend. Entsprechend vielfältig sind auch die Themen, die in regelmäßigen Mitarbeiterschulungen aufgegriffen werden können. Zum Beispiel:

+ Informationen zur Datensicherheit
+ Sicherer Umgang mit E-Mails
+ Bedrohungspotenzial durch Malware
+ Umgang mit mobilen Geräten
+ Gefahren der Internetnutzung
+ Gefahren durch soziale Netzwerke
+ Bedrohung durch Phishing-Attacken
+ Sichere Passwörter
+ Sichere Nutzung öffentlicher Hotspots
+ Verhalten bei erkannten Gefahren
+ Gefährdung durch Social Engineering
+ Umgang mit mobilen Datenspeichern

Unser Tipp

Kontaktieren Sie uns und informieren sich über Schulungsangebote in Sachen IT-Security Awareness. Wir helfen Ihnen gern weiter.

Social Engineering nutzt „Schwachstelle Mensch“

Beim Social Engineering richten Angreifer ihre Attacke an das vermeintlich schwächste Glied der Sicherheitskette – den Menschen. Das Problem: Durch die zunehmende digitale Vernetzung eröffnen sich den Cyberkriminellen viele Möglichkeiten, innerhalb kürzester Zeit Millionen von potenziellen Opfern zu erreichen.

Aber wodurch zeichnen sich solche Cyber-Attacken aus? Und wie sind sie für Zielpersonen als solche zu erkennen?

+ Besonders perfide: Social Engineering macht sich Hilfsbereitschaft, Vertrauen, Angst oder den Respekt vor Autoritäten zunutze, um ein Opfer zu manipulieren.
+ Ziel der Angreifer ist es, mit Hilfe ihrer Attacke an vertrauliche Informationen zu gelangen, Überweisungen zu erschwindeln oder auch Sicherheitsschranken auszuhebeln, um zum Beispiel Schadsoftware in ein IT-System einschleusen zu können.
+ Zentrales Merkmal einer Attacke: Der Täter täuscht eine andere Identität vor. Vielleicht gibt er sich als Techniker oder als Mitarbeiter von PayPal, Facebook oder einem Telekommunikationsunternehmen aus, um seinem Opfer beispielsweise Anmeldedaten oder Kontoinformationen zu entlocken.
+ Bekannte Social-Engineering-Methoden sind unter anderem Phishing, Spear Fishing, Scareware und CEO-Fraud – es gibt aber noch einige weitere.

Malware und Ransomware bedrohen Existenzen

Wussten Sie, dass aktuell mehr als eine halbe Milliarde unterschiedlicher Malware-Varianten bekannt sind? Vermutlich gibt es noch viele weitere Schadprogramme, die noch gar nicht entdeckt worden sind – schließlich kommen jeden Tag hunderte Versionen hinzu. Ein wichtiges Thema für die IT-Security Ihres Unternehmens.

Was ist Malware?

Der Begriff „Malware" ist ein inzwischen gängiges Kunstwort, das sich vom englischen Terminus „malicious software" ableitet. Das heißt: Es handelt sich dabei um eine Software, die mit böswilliger Absicht entwickelt wurde und das Ziel hat, unerwünschte und meist schädliche Funktionen in einem fremden System auszuführen. Computerviren, Würmer und Trojaner sind Beispiele solcher Schadsoftware. Es geht den Angreifern vor allem darum, mit Hilfe von Cyber-Attacken vertrauliche Daten abzugreifen und damit Schabernack zu treiben – zum Beispiel indem Adressdaten verkauft oder Kontodaten abgegriffen werden.

Wie kommt Malware ins System?

Malware lauert leider überall. Sie kann sich in einem E-Mail-Anhang verstecken, sich hinter einem Link verbergen, durch einen Download mit heruntergeladen oder auch auf einem USB-Stick eingeschleust werden. Und ohne einen guten Anti-Viren-Schutz und eben auch einem gewissen Gespür für Gefahren aus dem Internet seitens der Mitarbeiter bleibt das leider oftmals unbemerkt.

Ramsomware verschlüsselt Daten

Unter den vielen verschiedenen Malware-Varianten ist die Ransomware eine besonders fiese Sorte. Einmal im System, verschlüsseln diese Schadprogramme sämtliche Daten und legen dadurch das gesamte System lahm. Es folgt die Aufforderung zur Zahlung eines Lösegeldes – auf Englisch „ransom". Erst danach werden die Daten wieder freigegeben.

GermanWiper und Ordinypt Wiper

In so einem Fall haben Sie sogar noch Glück. Warum? In diesem Sommer sind mit GermanWiper und Ordinypt Wiper zwei neue Bedrohungen aufgetaucht, die sich zwar als Erpressertrojaner tarnen, de facto aber keine sind. Denn: Sie verschlüsseln Daten nicht nur, sondern überschreiben sie direkt. Ob Sie das geforderte Lösegeld zahlen oder nicht – die Daten sind weg. Sofern Sie kein gutes Backup haben, steht dann unter Umständen die Existenz des gesamten Unternehmens auf dem Spiel. Bislang sind GermanWiper und Ordinypt Wiper ausschließlich im deutschsprachigen Raum aktiv. Besonders fies: Die Ransomware verbirgt sich im Anhang von Bewerbungen, die sich auf reale Stellenangebote beziehen.

Tipps zum Malware-Schutz

Natürlich gibt es Mittel und Wege, mit denen Sie Ihr Unternehmen vor Malware und Ransomware – so gut es eben möglich ist – schützen können. Wir geben Ihnen folgende Tipps mit auf den Weg:

+ Nutzen Sie eine professionelle Sicherheitssoftware und denken auch über Endpoint-Security nach. Wir helfen Ihnen gern bei der Auswahl und Einrichtung einer Lösung und übernehmen auch das Patch-Management für Sie.
+ Firewalls mit integriertem Malware-Schutz, E-Mail-Spam-Filter und Sandboxing-Systeme sorgen für zusätzliche Sicherheit. Informieren Sie sich bei uns zu den Möglichkeiten.
+ Sorgen Sie für ein gutes Backup Ihrer Daten – den Hintermännern eines Erpressertrojaners nehmen Sie damit den Wind aus den Segeln. Sie können uns als Ihren zuverlässigen IT-Dienstleister auch gern mit dem Backup-Management beauftragen.
+ Stichwort: IT-Security Awareness. Schulen und sensibilisieren Sie Ihre Mitarbeiter zum Umgang mit verdächtigen E-Mails, Anhängen, Links und Downloads.

Alle Endgeräte schützen – eine Mammutaufgabe

Arbeitsrechner, Firmenlaptops, Businesshandys, Barcode-Scanner und POS-Terminals – all diese Geräte stellen Endpunkte innerhalb des Unternehmensnetzwerks dar und müssen vor Angriffen von außen geschützt werden. Ein einfacher Virenscanner reicht da nicht mehr aus. Auftritt für die Endpoint Security!

Vorteile der Endpoint Security:

+ Nahtlose Überwachung zu jeder Zeit
+ Minimierung des Risikos von Datenverlust
+ Proaktive Abwehr aller Angriffsarten

Endgeräte ohne Ende

Ihre Mitarbeiter arbeiten nicht ausschließlich stationär am Rechner, sondern nehmen auf Geschäftsreisen einen Firmenlaptop mit? Nutzen Sie selbst für Geschäftskontakte vielleicht ein vom Unternehmen zur Verfügung gestelltes Smartphone? Oder verwenden Sie eventuell ein Tablet Ihres Arbeitgebers für Präsentationen bei auswärtigen Geschäftsterminen? In all diesen Fällen benutzen Sie eines von vielen Endgeräten innerhalb des Unternehmensnetzwerkes. Damit dieses vor Zugriffen und Angriffen sicher ist, muss jedes einzelne Endgerät gut geschützt sein.

Endgeräte sind ein leichtes Ziel

Cyberattacken zielen vermehrt auf einzelne Endgeräte ab, um sich darüber Zugang zu Unternehmensnetzwerken zu verschaffen. Mal sollen sie Ransomware in das System einschleusen, sodass Daten verschlüsselt und anschließend Lösegeld-Forderungen gestellt werden können; in anderen Fällen geht es dagegen um Wirtschaftsspionage und Datendiebstahl. Das Problem dabei ist, dass sich Schadsoftware heutzutage gut zu verstecken und auch Hintertürchen zu nutzen weiß. So können ein manipuliertes Werbebanner, eine Sicherheitslücke im Browser oder eine heruntergeladene pdf-Datei schnell ein größeres Desaster auslösen. Da können Mitarbeiter im Sinne von IT-Security Awareness schon so vorsichtig wie möglich agieren.

Warum Endpoint Security?

Endpoint-Security-Systeme nehmen sich der Mammutaufgabe an, alle Endgeräte zu schützen. Sie verwenden dabei ein Client-/Server-Modell. Das bedeutet, dass ein Sicherheitsprogramm auf einem zentral verwalteten Server läuft, während auf allen Endgeräten zusätzlich eine passende Client-Software installiert wird. Alternativ gibt es SaaS-Lösungen (Software as a Service), bei denen Server und Sicherheitssoftware aus der Ferne oder in einer Cloud verwaltet werden. In beiden Fällen werden die Aktivitäten an allen Endpunkten überwacht. Versucht ein Endgerät, sich mit dem Netzwerk zu verbinden, prüft das Programm auf dem Server die zugewiesenen Rechte und stellt auf diese Weise fest, ob die Firmenrichtlinien zur IT-Sicherheit auf diesem Gerät eingehalten werden. Potenziell gefährliche Aktionen können dementsprechend direkt verhindert werden, indem das fragwürdige Gerät keinen Zugang erhält.

Schutz wird immer wichtiger

Mit der fortschreitenden Digitalisierung und der zunehmenden Vernetzung im Internet of Things wird der Schutz jeder einzelnen Komponente innerhalb eines Netzwerks immer wichtiger. Eine besondere Schwierigkeit dabei ist, dass sich den Cyber-Kriminellen gleich drei potenzielle Angriffsflächen bieten: die (End-)Geräte, die Kommunikationskanäle und die Software-Lösungen. Schäden gehen in die Millionen, wenn in einem Industriebetrieb beispielsweise eine Maschine vollkommen lahmgelegt wird. Oder stellen Sie sich vor, ein Virus verschlüsselt oder zerstört sämtliche Dateien – von heute auf morgen steht Ihre Existenz auf dem Spiel.

Holen Sie sich Hilfe!

Deshalb können wir Ihnen nur dringlichst empfehlen: Holen Sie sich Rat bezüglich Endpoint Security und sorgen Sie dafür, dass mit der richtigen Software-Lösung sämtliche Endgeräte in Ihrem Unternehmen bestens geschützt sind. Wir helfen Ihnen bei der Wahl des richtigen Tools, kümmern uns um die individuelle Anpassung an Ihr Unternehmenssystem und übernehmen selbstverständlich auch die Einrichtung.

Support-Ende – jetzt wird es unsicher!

In wenigen Wochen und Monaten stellt Microsoft den Support für einige seiner Produkte ein. Auch danach können Windows 7, Windows Server 2008, Office 2010 und Exchange Server 2010 zwar wie gewohnt genutzt werden, aber es wird keine Sicherheitsupdates mehr geben – eine Gefahr für Ihre IT-Security!

Microsoft-Produkte haben festen Lebenszyklus

Die meisten Microsoft-Produkte unterliegen einem von vornherein definierten Lebenszyklus. Er beginnt mit der ersten Veröffentlichung des Produkts und endet zehn Jahre später mit dem offiziellen „Dienstende". Vor allem Windows 7, Windows Server 2008 und Exchange Server 2010 rücken unaufhaltsam auf den Tag zu, an dem sie von Microsoft in Rente geschickt werden – Stichtag ist der 14. Januar 2020. Office 2010 hat noch etwas Schonfrist, denn erst der 13. Oktober 2020 läutet hier das Dienstende ein.

Keine Updates, keine Sicherheit

Auch nach dem Dienstende werden diese Produkte weiterhin funktionieren. Das heißt aber nicht, dass Sie sich zurücklehnen können.

Denn: Es werden, beginnend an den Stichtagen, von Microsoft keine weiteren Updates gegen Fehler, für mehr Sicherheit und für interne Microsoft-Anwendungen zur Verfügung gestellt. Zudem wird Microsoft künftig keine technische Unterstützung bei auftretenden Problemen mehr bieten, und mit dem technischen Support ist ebenfalls Schluss.

Gefahr von Sicherheitslücken

Der Knackpunkt: Sollte es nach dem jeweiligen Dienstende der einzelnen Produkte zu Sicherheitslücken kommen, werden diese also nicht mehr geschlossen. Angriffe, Datenverluste und eine Unterbrechung der geschäftlichen Abläufe drohen. Deshalb sollten Sie unbedingt rechtzeitig handeln und auf neuere Microsoft-Produkte umsteigen. Hier eine Übersicht der Migrationsmöglichkeiten:

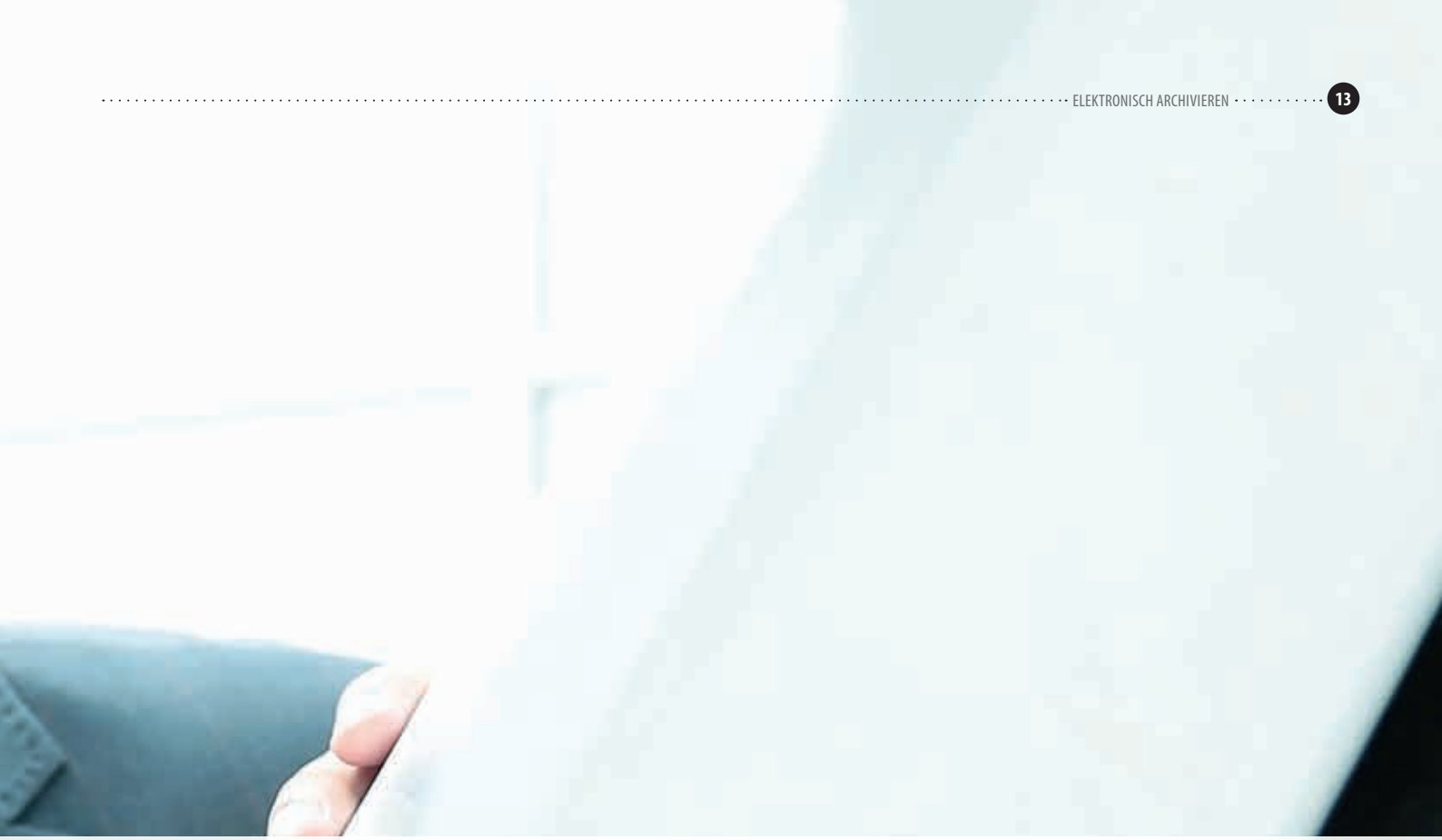
+ Windows 7 > Windows 10
+ Windows Server 2008 > Windows Server 2019
+ Exchange Server 2010 > Exchange Server 2016 > Exchange Server 2019
+ Exchange Server 2010 > Office 365
+ Office 2010 > Office 2019 / Office 365

Achtung: DSGVO

Übrigens: Mit dem Einsatz von veralteten Microsoft-Produkten gefährden Sie nicht nur Ihre sensiblen Daten und Systeme, sondern verstoßen auch gegen die gesetzlichen Vorschriften – Stichwort DSGVO. Daher der dringende Appell: Werden Sie am besten umgehend aktiv! Unsere IT-Fachleute beraten Sie gern zu den verschiedenen Möglichkeiten und übernehmen den Migrationsprozess. Sprechen Sie uns einfach an!

Elektronisch archivieren – einfach und schnell

Rechnungen, Belege, Handelsbriefe, Bücher und Schriftverkehr – laut Gesetzgebung besteht für solche Dokumente und Unterlagen eine Aufbewahrungspflicht. Da ein Großteil der Geschäftskorrespondenz heute digital in Form von E-Mails stattfindet, steigen Unternehmen vermehrt auf die elektronische Archivierung um.



Ordner um Ordner in den Archiven

Archivieren meint generell das Aufbewahren von Dokumenten und Schriftstücken in einem Archiv. Früher mussten dafür eine Menge von Regalen und Ordnern herhalten – schließlich galt es, die zahlreichen Papiere sinnhaft abzuheften und irgendwo sicher unterzubringen. Heute findet die geschäftliche Kommunikation allerdings hauptsächlich per E-Mail statt. Das bedeutet, dass Unternehmen zwangsläufig umdenken müssen. Das Stichwort lautet in diesem Zusammenhang: elektronische Archivierung.

Aufbewahrung ist Pflicht

Bei der elektronischen Archivierung geht es in erster Linie um die unveränderbare, dauerhafte Ablage und Aufbewahrung steuerlich relevanter Belege und Geschäftsunterlagen in elektronischer Form für das Finanzamt. Dazu hat das Bundesfinanzministerium ein ziemlich umfassendes Regelwerk aufgestellt – die GoBD (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff). Darin ist genau festgehalten, welche Papiere wie lange aufzubewahren sind. Konkrete Anweisungen können natürlich hilfreich sein. Aber: Sie müssen auch befolgt werden.

Fit für die Buchführung

Das Ziel ist es, dass jeder Geschäftsvorfall innerhalb des Unternehmens in der Buchführung oder in den Aufzeichnungen erfasst werden muss. Wichtig wird die sogenannte revisionssichere Aufbewahrung dann, wenn zum Beispiel eine Betriebsprüfung ins Haus steht. Stellt sich nämlich heraus, dass Vorgänge nicht nachvollzogen werden können, drohen Bußgelder und sogar Haftstrafen.

Software hilft bei Archivierung

Das klingt zuerst einmal kompliziert und dementsprechend nach sehr viel Arbeit. Zum Glück gibt es mittlerweile eine Vielzahl von verschiedenen GoBD-konformen Archivierungsprogrammen, die Sie bei dieser Herausforderung unterstützen. Das Gute an der Sache: Führen Sie die elektronische Archivierung genau nach den Vorgaben dieser Software aus, wird die Angst vor einer Steuer- oder Betriebsprüfung überflüssig.

Vorteile der elektronischen Archivierung

Es ergeben sich durch die elektronische Archivierung sogar noch weitere Vorteile für Unternehmen:

+ Sie sparen durch das „papierlose Büro" Kosten für Porto, Papier und Drucker.
+ Sie benötigen für die Suche nach bestimmten Dokumenten weniger Zeit, denn durch eine sinnvolle Ablage und Suchfunktion lassen sich Papiere schnell und einfach finden.
+ Sie sparen Platz und eventuell auch Lagerkosten, denn lange Regalreihen für unzählige Aktenordner fallen weg.

Profi-Hilfe bei Implementierung

Viele verschiedene Software-Lösungen stehen heute für die elektronische Archivierung zur Verfügung. Aber welche ist für Ihr Unternehmen die Richtige? Wir stellen Ihnen die verschiedenen Lösungen vor und helfen Ihnen auf Grundlage Ihrer individuellen Anforderungen auch gern bei der Entscheidung. Die Implementierung macht Ihnen Sorge? Kein Problem, denn auch diese nehmen Ihnen unsere Profis gerne ab!

Tipp

Die elektronische Archivierung lässt sich perfekt durch ein Dokumenten-Management-System ergänzen – lassen Sie sich dazu von Ihrem IT-Dienstleister beraten!

Zurück zur Stempeluhr?

Der Europäische Gerichtshof hat im Mai 2019 beschlossen: Unternehmen müssen künftig die Arbeitszeit aller Mitarbeiter erfassen. Einen genauen Stichtag gibt es zwar noch nicht, dennoch sollten Sie sich frühzeitig darum kümmern, ein System zur Arbeitszeiterfassung in Ihrem Unternehmen zu implementieren.

EuGh hat entschieden

Im ersten Moment mag das Urteil des Europäischen Gerichtshofs (EuGh) bei Ihnen viele Fragezeichen hervorgerufen haben. Erlebt die längst ausrangierte Stempeluhr etwa ein Comeback? Können Sie weiterhin an den flexiblen Arbeitszeitregelungen in Ihrem Unternehmen festhalten? Wie lassen sich Home-Office-Möglichkeiten mit der neuen Bestimmung vereinbaren? Oder steht das moderne Arbeiten mit dieser Entscheidung vielleicht sogar vollständig auf dem Spiel?

Schutz der Arbeitnehmer

Der EuGh hat mit seiner Entscheidung die Gesundheit der Arbeitnehmer im Blick. Durch die Aufzeichnungspflicht der Arbeitszeit soll nämlich sichergestellt werden, dass Angestellte pro Woche nicht mehr als 48 Stunden arbeiten und jeden Tag mindestens elf Stunden am Stück frei haben. Grundsätzlich werden Sie als Unternehmer das Urteil, das europaweit gelten wird, also durchaus unterstützen – schließlich ist es auch Ihr Anliegen, dass Ihre Mitarbeiter dauerhaft fit bleiben und Ihr Unternehmen mit Ihrer Expertise voranbringen.

Keine Panik vor der Aufzeichnungspflicht

Die gute Nachricht: Wir können Ihnen die Angst vor der Implementierung eines Systems zur Arbeitszeiterfassung nehmen. Es gibt mittlerweile nämlich viele Software-Lösungen am Markt, mit denen Sie alle Aspekte rund um das neue Arbeitszeitgesetz und die Anforderungen der Arbeitswelt 4.0 unter einen Hut bekommen. Nach der Implementierung und ersten Eingewöhnungszeit bei den Mitarbeitern zeigt sich vielleicht sogar recht schnell: So ein Zeiterfassungstool kann große Vorteile haben.

Tools sind echte Wundertüten

Moderne Systeme zur digitalen Zeiterfassung sind meistens gut durchdacht. Hier einige Vorteile:

+ Mit Expertenhilfe lassen sich die meisten Tools einfach in bestehende Systeme integrieren.
+ Die speziellen Anwendungen lassen sich in elektronischer Form am Arbeitsrechner oder mittels App auf dem Smartphone bedienen – und sind entsprechend mit PC, Mac, Smartphone, Tablet und Terminal kompatibel.
+ Mitarbeiter können mit wenigen Klicks ihre Arbeitszeiten erfassen und ihre restliche Arbeitszeit berechnen – egal wo sie sind.
+ Die Tools erfassen Urlaub, Krankenstand, Zeitausgleich und Überstunden.
+ Die meisten Systeme ermöglichen individuelle und flexible Arbeitszeitmodelle.
+ Internationale Arbeitsgesetze werden von vielen Programmen berücksichtigt.
+ Viele Tools spucken am Monatsende per Knopfdruck einen digitalen Stundenzettel für die Lohnabrechnung aus.

Hilfe gefällig?

Unsere Experten beraten Sie gern zu den verschiedenen Software-Lösungen und unterstützen Sie bei der Wahl des für Ihr Unternehmen perfekten Tools – und zwar unabhängig von Hersteller und Art der Lösung. Verschiedene Faktoren gilt es dabei zu berücksichtigen, beispielsweise Unternehmensgröße und Wirtschaftsbranche. Ist das System einmal ausgewählt, übernehmen wir auch die Implementierung und Schulung Ihrer Mitarbeiter – und schon sind Sie für das neue Gesetz zur Arbeitszeiterfassung gerüstet!

Auch in Ihrer Nähe!

Computer Insider GmbH

Die Spezialisten für IT in der Arztpraxis

Weseler Str. 162 | 45721 Haltern am See
Tel. 02364 5089517 | info@computer-insider.de
www.computer-insider.de