



Nr. 46 | Frühling 2024

Liebe Kunden und Geschäftsfreunde

Ist eine **Nachzahlung** in die Säule 3a sinnvoll? Wie können sich Unternehmen vor **Angriffen auf E-Mail-Konten** schützen? Dies sind die beiden Themenbereiche, welche wir für Sie auf den folgenden Seiten zusammengefasst haben.

Nachzahlung in die Säule 3a

Unser Schweizer Vorsorgesystem beruht auf einem stabilen 3-Säulen-System. Die bisherigen Reformen der zweiten Säule führen für die Versicherten nicht nur zu höheren Beiträgen, sondern auch zu einem niedrigeren überobligatorischen Leistungsbeitrag. Diese Entwicklung stärkt die Bedeutung der dritten Säule. Banken und Versicherungen erinnern ihre Kunden jeweils rechtzeitig zum Jahresende daran, Einzahlungen in die dritte Säule vorzunehmen. Damit wird die Steuerlast gesenkt und gleichzeitig das Altersguthaben geöffnet.

Wenn in einem Jahr keine Einzahlung vorgenommen wird, kann das nicht mehr nachgeholt werden. Im Gegensatz zur zweiten Säule, wo Lücken mit Einkäufen aufgefüllt werden können. Mit steuerlichen Anreizen fördert der Staat die zweite und dritte Säule. Umfragen haben ergeben, dass das Schweizer Volk am meisten Vertrauen in die dritte Säule hat. Klar, da spart man nur für sich und jeder kann das Geld individualisiert anlegen.

Motion

Basierend auf diesen Überlegungen hat der Obwaldner Ständerat Erich Ettlin im 2019 eine Motion eingereicht, die einen nachträglichen Einkauf in die Säule 3a ermöglichen soll. Es soll den Eheleuten möglich sein, die durch Erwerbsunterbrüche entstandene Lücken zu schliessen, wenn beide wieder erwerbstätig sind und über genügend Mittel für die Einzahlung verfügen. Einfach zusammengefasst sollen alle fünf Jahre und dann höchstens der Maximalbetrag für Selbständigerwerbende nachbezahlt werden können. Die Motion wurde von beiden Räten angenommen und der Bundesrat damit beauftragt, eine Vorlage zu erarbeiten und vorzulegen.

Einschränkungen beim Vorentwurf des Bundesrats

Nach etwas längerer Überlegungszeit hat sich der Bundesrat entschieden, die Verordnung BVV 3 anzupassen

und damit keine Gesetzesänderung vorzunehmen. Den Vorentwurf hat er in die Vernehmlassung geschickt.

Motion wurde nicht erfüllt

Leider beraubt die Vernehmlassungsvorlage die Motion in mehrfacher Hinsicht ihrer Substanz. Erstens beschränkt der Entwurf die Einkaufsmöglichkeiten auf Beitragsjahre, in denen die Betroffenen die Voraussetzungen für Beiträge in die Säule 3a erfüllt haben. Dies schliesst all jene aus, die ihre berufliche Laufbahn erst spät begonnen oder für eine gewisse Zeit unterbrochen haben. Genau diese hätten aber mit der Motion unterstützt werden sollen. Zudem beschränkt die Vorlage die Einkaufsmöglichkeit auf Lücken, die ab dem Inkrafttreten der Verordnung entstanden sind. Und auch nur auf die Lücken, die bis zu zehn Jahren vor dem Einkauf entstanden sind.

Es ist zwar verständlich, dass Lücken, die vor mehreren Jahrzehnten entstanden sind – die Säule 3a wurde 1987 eingeführt –, nicht berücksichtigt werden. Einerseits wären die finanziellen Einbussen für die öffentliche Hand nur schwer zu verkraften. Andererseits wäre es sowohl für Anspruchsberechtigte als auch für Behörden schwierig, die Beitragshistorie zu rekonstruieren, Beweise zu erbringen und die notwendigen Kontrollen durchzuführen. Eine solche Einschränkung würde jedoch zu einer Benachteiligung eines Grossteils der Bevölkerung führen.

Denkbarer Kompromiss

Ein Mittelweg könnte jedoch eingeschlagen werden. Es ist durchaus nachvollziehbar, nur Lücken zu berücksichtigen, welche in den letzten zehn Jahren vor Inkrafttreten der Regelung aufgetreten sind. So würden sich nicht nur die finanziellen Verluste in angemessenem Rahmen halten, dies würde auch die notwendigen Kontrollen erlauben, weil die Daten mindestens zehn Jahre lang gespeichert werden müssen. Lücken, die ab 2015 entstanden sind, könnten somit ab 2025 geschlossen werden.

Dieses Instrument – auch wenn nur ergänzend zur beruflichen Vorsorge der zweiten Säule – ist zu begrüssen, aber nur, wenn es durch die Umsetzung nicht ausgehöhlt wird. Die weitere Entwicklung dieses Projekts gilt es zu beobachten.

Ihre axalta Treuhand AG

ANGRIFFE AUF E-MAIL-KONTEN, EINE TÄGLICHE GEFAHR UND EIN GROSSES RISIKO FÜR UNTERNEHMEN UND DEREN MITARBEITENDE

Nachfolgend möchten wir Sie über einige Tipps und Massnahmen orientieren, wie Sie sich vor Cyber-Attacken schützen können.

Jüngst erlebten Behörden in Westeuropa und in den USA einen schweren Schlag, als sie das Ziel eines umfangreichen Cyberangriffs wurden. Hacker verschafften sich Zugriff auf E-Mail-Accounts zahlreicher Mitarbeiter und legten Sicherheitslücken offen, deren Ausmasse noch nicht vollständig erfasst sind. Dies wirft drängende Fragen über den Zustand der IT-Sicherheit in öffentlichen Institutionen auf und erregt weltweit, auch bei den Unternehmen, für Aufsehen.

Die Bedrohungslandschaft verstehen

E-Mails sind ein wichtiges Ziel für Cyberangriffe, da sie eine einfache und bequeme Art der Kommunikation darstellen. E-Mail-basierte Angriffe nehmen an Zahl, Komplexität und Schwere (z.B. setzen Cyberkriminelle dazu bereits Künstliche Intelligenz «KI» ein) zu und sind immer schwieriger zu erkennen und zu verhindern.

E-Mail-basierte Angriffe sind böswillige Versuche, sich über E-Mail-Konten unbefugten Zugang zu Systemen oder Informationen zu verschaffen. Hier sind einige der häufigsten Arten:

1. *Phishing-Angriffe*: Dies geschieht in der Regel durch E-Mails mit gefälschten Links oder Anhängen, die darauf abzielen, sensible Informationen wie Passwörter und Kreditkartennummern zu erlangen.

2. *Spear-Phishing-Angriffe*: Hierbei werden personalisierte Nachrichten verschickt, die legitim erscheinen, aber Malware enthalten oder versuchen, den Empfänger zur Preisgabe vertraulicher Informationen zu verleiten.

3. *Business E-Mail Compromise (BEC) Angriffe*: Diese Angriffe verleiten Mitarbeiter dazu, Geld oder vertrauliche Informationen an das Konto des Angreifers zu senden.

4. *E-Mail-Spoofing-Angriffe*: Bei dieser Art von Angriffen werden E-Mails verschickt, die den Anschein erwecken, von einer anderen Person zu stammen, während die wahre Identität des Absenders verschleiert wird.

5. *Verbreitung von Malware und Ransomware per E-Mail*: Cyberkriminelle kapern häufig E-Mail-Konten, um Malware zu verbreiten.

6. *Man-in-the-middle-Angriffe*: Ein solcher Angriff liegt vor, wenn ein Angreifer Daten zwischen zwei Parteien abfängt und weiterleitet, ohne dass eine der Parteien davon weiss.

7. *E-Mail-Konto-Hijacking oder Takeover-Angriffe*: Bei diesem Angriff versucht ein Hacker, auf Ihr E-Mail-Konto zuzugreifen, indem er das Passwort errät oder eine andere Methode verwendet.

8. *Angriffe zum Sammeln von Zugangsdaten durch Phishing oder Social Engineering*: Hacker können sich Zugang zu E-Mail-Konten verschaffen, indem sie Sie dazu bringen, Ihre Anmeldedaten preiszugeben, z.B. indem sie sich als eine andere Person ausgeben und nach Ihren Benutzernamen und Kennwörtern fragen, als Servicetechniker verkleidet in den Geschäftsräumen Computer oder das Netzwerk direkt vor Ort mit Schadsoftware infizieren, präparierte Datenträger deponieren (Mitarbeiter findet einen USB-Stick mit Aufschrift «privat» auf dem Parkplatz und schliesst ihn aus Neugier an seinem Arbeitsplatz an) oder präparierte Dokumente schicken (Spontanbewerbung per E-Mail an die HR-Abteilung) etc.

Schutz vor E-Mail-basierten Angriffen

Eigene Kenntnisse im Bereich der IT-Sicherheit sind deshalb so entscheidend, weil viele Schutzprogramme und Anti-Viren-Software hauptsächlich reaktiv agieren. Sie sind in der Regel nur effektiv gegen bereits bekannte Bedrohungen. Da Hacker jedoch oft die Ersten sind, die Sicherheitslücken entdecken und ausnutzen, sollte man nicht ausschliesslich auf softwarebasierten Schutz setzen. Diese Vorfälle sind eine Mahnung und Hinweis darauf, dass insbesondere auch mittelständische Unternehmen sich gut schützen sollten. Die Sicherheitsstrategien der Unternehmen sollten ständig überprüft und optimiert werden unter Einbezug der künftigen Cyberbedrohungen und alle Systeme sollten stets aktuell gehalten werden (inkl. Updates).

1. *Sichere Passwörter finden*: Eine Analyse der Passwortwahl im Jahr 2022 hat gezeigt, dass Kreativität offenbar Mangelware ist: «Password, 123456 und 123456789 führen die Liste der am meisten genutzten Passwörter an! Cyberkriminelle sind sich dieser Tatsache bewusst und probieren diese einfachen Kombinationen als Erstes aus. Um sich effektiv zu schützen, empfiehlt es sich, ein komplexes Passwort aus einer zufälligen Mischung Gross- und Kleinbuchstaben, Sonderzeichen und Zahlen zu wählen. Zur sicheren Aufbewahrung sollte man

dabei nicht auf den handgeschriebenen Zettel setzen. Sinnvoller ist ein Passwort-Manager, der starke, zufällige Passwörter generiert und diese intern abspeichert.

2. Mit Zwei-Faktor-Authentifizierung arbeiten: Fast alle Online-Konten bieten die Option der Zwei-Faktor-Authentifizierung, auch 2FA genannt. Diese Sicherheitsfunktion muss manuell aktiviert werden und erfordert neben dem Passwort eine zusätzliche Authentifizierung, um den Zugang zu ermöglichen. Diese zusätzliche Authentifizierung kann ein via SMS verschickter Code sein, der eingegeben werden muss, oder die Verifizierung durch einen Fingerabdruckscan. Selbst wenn Cyberkriminelle es schaffen, das Passwort zu entschlüsseln, bleibt ihnen der Zugang zum Konto durch diese zusätzliche Sicherheitsebene verwehrt.

3. Analyse der E-Mail-Absender: Nicht selten gelangen Hacker vor allem über infizierte E-Mails an private Daten. Umso wichtiger ist es, solch unseriöse E-Mails direkt zu identifizieren. Eine gute Möglichkeit dazu bieten alternative Authentifizierungen (SPF, DKIM, DMARC). Sie können unseriöse Absender und Anomalien im E-Mail-Header erkennen. Indem sie gefährliche Mails abwehren, anstatt sie in Quarantäne zu verschieben, sind Nutzer besser geschützt.

4. Phishing erkennen: Oftmals sind Phishing-Angriffe in E-Mails versteckt, die den Empfänger dazu auffordern, einem speziellen Link zu folgen, meist mit dem Vorwand, persönliche Daten zu bestätigen. Ignoriert man diese Aufforderung, wird in der Regel mit der Sperre des betroffenen Kontos gedroht. Ein Klick auf den Link führt jedoch zu einer täuschend authentischen Webseite. Wer dort seine Daten eingibt, überreicht sie unfreiwillig den Cyberkriminellen. Einen Schutz gegen Phishing-Angriffe bieten zum Beispiel Tools, die über die «Suchen und Neutralisierung»-Funktion arbeiten. Wenn Sie während der aktuellen Aktivität beispielsweise eine Änderung der Bedrohungsstufe feststellen, wird der Anwender gewarnt oder die schädliche URL direkt entfernt.

5. E-Mails richtig verschlüsseln: Es ist von grundlegender Bedeutung, dass berufliche E-Mails immer verschlüsselt versendet werden, insbesondere wenn sie sensible Informationen enthalten. Verschlüsselungs-Technologien wie S/MIME (Secure/Multipurpose Internet Mail Extensions) oder PGP (Pretty Good Privacy) bieten dabei doppelten Schutz. Sie sorgen nicht nur dafür, dass der Inhalt vertraulich bleibt, sondern erlauben auch die Ver-

wendung einer digitalen Signatur zur Bestätigung der Identität. Zudem entspricht diese Form der Verschlüsselung den Anforderungen der Datenschutzgrundverordnung (DSGVO) für sichere Kommunikation.

6. Sicherheitsfragen gut wählen: Sicherheitsfragen werden dann gestellt, wenn ein Anwender sein Passwort vergessen und sich authentifizieren soll. Viel zu oft sind die Fragen allerdings einfach gestellt. Sei es die Frage nach dem Namen des Haustiers oder dem eigenen Geburtstag – mit einigen Recherchen ist es für Hacker so ein Leichtes, die Antwort herauszufinden und das Passwort zurückzusetzen.

7. Sich nicht im öffentlichen WLAN einloggen: Öffentliche WLAN-Netzwerke, die in Cafés, Flughäfen oder anderen öffentlichen Orten kostenlos zur Verfügung stehen, sind für viele verlockend. Das Problem ist, dass diese Netzwerke oft mangelhaft gesichert sind und so eine einfache Angriffsfläche für Hacker darstellen. Aus diesem Grund ist es ratsam, sich nicht über solche Netzwerke in E-Mail-Konten einzuloggen, insbesondere wenn es um berufliche E-Mails geht. Möglich ist auch eine VPN-Verbindung, die das E-Mail-Konto schützt.

8. Meldungen zur Kontoaktivität ernst nehmen: Nahezu alle Online-Konten benachrichtigen den Nutzer über ungewöhnliche Aktivitäten, etwa gescheiterte Anmeldeversuche. Diese Warnungen können per E-Mail kommen oder direkt auf der Website angezeigt werden. In jedem Fall ist es entscheidend, solche Hinweise ernst zu nehmen und schnell die Sicherheitseinstellungen zu überprüfen oder zu verstärken, um potenzielle Risiken abzuwehren.

Der Faktor Mensch ist in Bezug auf Cyber-Sicherheit zentral. Sehr viele Sicherheitsvorfälle in Unternehmen sind auf die Unwissenheit oder Unachtsamkeit der Mitarbeitenden zurückzuführen. Gemäss Studien werden 30 % der verseuchten Mails binnen zehn Minuten nach dem Eingang angeklickt. Weitere 52 % werden in einem Zeitraum von einer Stunde geöffnet. Der Mensch ist eine derart eklatante Schwachstelle, dass die Cyberkriminalität dazu mit «Social Engineering» eine eigene Angriffskategorie entwickelt hat.

Was, wenn ein Angriff stattgefunden hat?

Dann gilt, schnell handeln: Cyberkriminelle operieren international, eine forensische Spurensicherung muss sofort erfolgen, sowohl um den Angriff zu identifizieren sowie wirksam zu beenden und das Ausmass zu erkennen, als auch, um überhaupt eine Strafverfolgung zu ermöglichen.

Jedes Unternehmen muss im Voraus über definierte Prozesse und Verantwortlichkeiten verfügen, damit im Angriffsfall klar ist, wer was bis wann zu erledigen hat und wie das Unternehmen kommunizieren will (wann und wen informieren? Kunden, Partner, Medien, Eidg. Datenschutzbeauftragter «EDÖB»? etc.).

Es ist umgehend Strafanzeige bei der **Kantonspolizei am Geschäftssitz** zu erstatten und den Vorfall dem Bundesamt für Cybersicherheit (BASC) zu melden.

Weiter ist damit zu rechnen, dass der Geschäftsbetrieb während einiger Zeit stillsteht (IT-forensische Spurensicherung, Ermittlung der Polizei, allenfalls haben die Angreifer ihr System verschlüsselt etc.). Eine entsprechende Betriebsauffall-/Cyberversicherung ist (zwingend) zu empfehlen.

Gemäss dem seit dem 1. September 2023 geltenden Datenschutzgesetz besteht eine umgehende Meldepflicht an den EDÖB wenn ein Cyberangriff Personendaten (Kunden, Partner etc.) tangiert und dadurch ein hohes Risiko einer Beeinträchtigung der Persönlichkeit oder Grundrechte schafft. Je nachdem sind zudem die Bestimmungen der DSGVO der Europäischen Union zu befolgen.

Grundsätzlich dürfte eine rasche und aktive Kommunikation vorzuziehen sein, denn der Angriff lässt sich auch durch Geheimhaltung nicht rückgängig machen und oft nutzen die Angreifer das Schweigen als zusätzliches Nötigungsmittel, indem sie drohen, die Kunden, Partner etc. gleich selbst zu informieren.

Fazit

Aus heutiger Sicht ist die Cyberkriminalität eine der höchsten und somit auch wichtigsten Risiken für Firmen. Wird die IT-Sicherheit von Firmen und deren Mitarbeiter nicht ernst genommen und die entsprechenden Massnahmen nicht umgesetzt, so können die Auswirkungen eines erfolgreichen Angriffs existenziell werden. Im schlimmsten Fall kann es zum Verlust aller relevanten Daten einer Firma führen. Wir empfehlen Ihnen, **regelmässig** Updates und Checks durch Ihren IT-Betreuer vornehmen zu lassen und sowohl **die Geschäftsleitung als auch das Personal** dafür zu sensibilisieren und zu schulen. Als Unternehmerin/Unternehmer müssen Sie im Rahmen Ihres Risikomanagements ihre eigene IT-Infrastruktur im Detail kennen und über Konzepte und Instrumente verfügen, wie diese zu schützen ist und wer im Falle eines Angriffs was zu tun hat. Sie müssen davon ausgehen, dass es nur eine Frage der Zeit ist, bis Sie oder Ihr Unternehmen Ziel eines Cyberangriffs werden und dann wäre ein unzureichender Schutz und fehlende Vorbereitung fatal.