Cybersicher ist sicher: praktische Tipps zur Cybersicherheit

Im Jahr 2019 wurden **81%** aller Unternehmen von Betrügern im Zahlungsverkehr attackiert. Das ist die höchste Rate seit 2009.[1]

Sie spielen eine entscheidende Rolle für die Cybersicherheit Ihres Unternehmens. Zeit, diese Rolle zum Wohle des gesamten Finanzbereichs aktiv anzugehen. Dabei geht es um viel mehr als um Lösungen für einzelne Schwachstellen im Treasury. Überzeugen Sie Ihr Unternehmen von den richtigen, ganzheitlichen Sicherheitsmaßnahmen.

Fragen Sie sich, wie genau Treasury Cybersicherheit beeinflussen kann? Sind Sie auf der Suche nach Maßnahmen, die Sie sofort umsetzen können? Dann sind Sie hier richtig. Wir geben Ihnen Tipps, was Sie jetzt direkt tun können, um die „Schätze" Ihres Unternehmens zu bewahren. Lesen Sie außerdem, wie wichtig die Unterstützung eines Systemanbieters sein kann.

[1] https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/paymentsfraud-2019. Zuletzt abgerufen am 10. September 2020

Ihre Herausforderung: **sicheres Arbeiten trotz verschiedenster Systeme**

10-15% mehr Kosten jährlich allein für die Wartung alter Systeme.[2]

Wo liegt das Problem?

In vielen Unternehmensbereichen gleicht die IT-Infrastruktur einem wahren Flickenteppich an veralteten Systemen. Da ist auch das Treasury keine Ausnahme. Auch wenn diese Systeme Ergebnisse liefern, sind sie umständlich zu bedienen und zu warten. Vielleicht ist es auch in Ihrem Unternehmen so, dass in der IT-Abteilung niemand speziell für Treasury-Belange zuständig ist. Da lässt sich das Thema Cybersicherheit kaum bewältigen. Entsprechend ist die Versuchung groß, alles beim Alten zu lassen und auf das Beste zu hoffen.

Welche Maßnahmen können Sie sofort treffen?

Informieren Sie sich, welche Vorteile technologische Fortschritte beim Thema Sicherheit liefern.

- Erarbeiten Sie sich einen Business Case für eine Cloud-Lösung und erfassen Sie, wie viel Zeit systemübergreifend für sicherheitsrelevante Aufgaben draufgeht (z.B. das Hin- und Herspringen zwischen Systemen oder die Suche nach den richtigen Unterschriften).
- Lassen Sie sich von einem Versicherungsanbieter bzw. Ihrem derzeitigen oder gewünschten Treasury-Management-Systemanbieter klar und prägnant erklären, wie eine Konsolidierung von Systemen sowie eine Migration in die Cloud dazu beitragen können, Cyberbetrug zu verhindern (z.B. in Form von E-Mail-Betrug oder gefälschten Zahlungen).

Wie kann der richtige Anbieter helfen?

Erschließen Sie sich in der Cloud eine einheitliche, sichere Umgebung. So können Sie sich auf Ihre Kernaufgaben konzentrieren und sich für sichere Methoden und Prozesse einsetzen, während Sie das Hosting Ihrer webbasierten Treasury-Management-Lösung einem Expertenteam überlassen können.

Treasury-Management-Experten übernehmen folgende Aufgaben für Sie:

- Migration und Implementierung sowie den Betrieb, Support und Updates. Sie als Treasurer arbeiten schnell, sicher und verlässlich mit einer einzigen sicheren Plattform in einer einheitlichen Umgebung.
- Entwicklung und Integration von Protokollen, die immer wieder neue Betrugsmaschen berücksichtigen. Sie verhindern und entschärfen Cyberbetrug dank eingebauter Prozesse.
- Analyse von Workflows, um diese effizienter und sicherer zu machen. Sie als Treasurer können sich ganz auf die Analyse korrekter Echtzeitdaten konzentrieren und entsprechende Empfehlungen aussprechen.

[2] https://gcn.com/blogs/cybereye/2015/06/legacysystems.aspx. Zuletzt abgerufen am 9. September 2020

Ihre doppelte Herausforderung: **Sicherheit gewährleisten und sich gleichzeitig auf wertstiftende Treasury-Aufgaben konzentrieren**

87% aller Treasurer sind der Meinung, dass Treasury mittlerweile eine strategische Rolle in Unternehmen einnimmt.[3]

Wo liegt das Problem?

Wenn Sie als Treasurer in Echtzeit Zugriff auf unternehmensweite und vollständige Daten haben, können Sie Ihre kostenbare Zeit in die Analyse dieser Daten stecken, statt sie mühsam zusammentragen zu müssen. Echtzeitzugang zu Daten bringt eine gewisse zusätzliche Komplexität mit sich, wenn man bedenkt, dass Unternehmen sensible Daten schützen und sich an Auflagen und Best Practices halten müssen. Im 21. Jahrhundert gilt es, die Wechselwirkungen zwischen Menschen, Technik und Prozessoptimierung mit Blick auf sicheres Treasury Management zu verstehen. Manche Treasurer befürchten, dadurch von anderen strategischen Aufgaben abgehalten zu werden.

Welche Maßnahmen können Sie sofort treffen?

Gehen Sie den ersten Schritt und treffen Sie einige ebenso einfache wie essenzielle interne bzw. externe Maßnahmen. Sorgen Sie für einen regelmäßigen Austausch mit Banken und erkundigen Sie sich, ob diese Informationen zu Cyberkriminalität und Prävention veröffentlichen. Setzen Sie Kontrollen um und nehmen Sie sich die Zeit für die Benutzerverwaltung. So stärken Sie Ihre Datengrundlage und den Systemzugang.

Der Faktor Mensch	Der Faktor Technologie	Prozessoptimierung
☑ Überprüfen Sie einmal im Monat, alle sechs Monate oder einmal im Jahr Nutzerprofile und Bankkonten	☑ Lassen Sie sich von Drittanbietern und Banken Zertifikate vorlegen (mindestens SSAE16/ SOC1 oder ein vergleichbarer Nachweis)	☑ Abonnieren Sie E-Mail-Benachrichtigungen von Banken zu sicherheitsrelevanten Themen und aktuellen Bedrohungen
☑ Implementieren Sie komplexe Parameter für Passwörter und Nutzerkennungen	☑ Fragen Sie Ihren Cybersicherheitsversicherer nach einer ersten Analyse des Sicherheitsstatus Ihres derzeitigen Treasury Management Systems und dokumentieren Sie mögliche Lücken	☑ Bleiben Sie mit wichtigen Drittanbietern und Banken in Kontakt
☑ Machen Sie regelmäßige Passwortänderung verpflichtend		☑ Lassen Sie sich von einem Treasury-Experten beraten, inwieweit Ihre derzeitigen Treasury-Prozesse Cybersicherheit-Best-Practices entsprechen

Wie kann der richtige Anbieter helfen?

Suchen Sie einen Partner, der versteht, wie die Faktoren Mensch, Technologie und Prozessoptimierung zusammenhängen und wie diese gemeinsam eine einheitliche, sichere Arbeitsumgebung schaffen können. Holen Sie sich Unterstützung bei der Umsetzung transparenter Zahlungsverkehrsprozesse, z.B. in Form einer unternehmensweiten Richtlinie oder von Kontrollmaßnahmen. Vernetzen Sie sich mit anderen, um Prozesse zu analysieren und neu zu strukturieren und sich so auf mehrwertstiftende Aufgaben konzentrieren zu können, die von regel- und gesetzeskonformen und effizienten Methoden getragen werden.

Der Faktor Mensch

- ☑ Arbeiten Sie mit einem Vier-Augen-Prinzip, das selbst für das Neuhinzufügen von Nutzern oder die Unterschriften einzelner Mitarbeiter gilt
- ☑ Erarbeiten Sie ein ausgeklügeltes Rechte- und Rollenkonzept, im Rahmen dessen jeder Nutzer nur die Rechte und Befugnisse hat, die er oder sie zur Erledigung bestimmter Aufgaben in einer bestimmten Gesellschaft benötigt
- ☑ Führen Sie strenge Zugriffskontrollen ein, z.B. Single-Sign-On oder IP-Restriktionen
- ☑ Setzen Sie Zwei-Faktor-Authentifizierung um und machen Sie den Einsatz zweier unterschiedlicher Geräte verpflichtend, um Zugriff zu erlangen

Der Faktor Technologie

- ☑ Sorgen Sie für eine klare Aufgabenteilung in allen Bereichen
- ☑ Nutzen Sie die systemintegrierte Überprüfung von Zahlungsempfängern und Konten (z.B. durch Allow- und Block-Listen und den entsprechenden Echtzeit-Abgleich), um Risiken wie Betrug im Rahmen der Beschaffungskette oder Lieferantenbetrug vorzubeugen
- ☑ Machen Sie sich maschinelles Lernen zunutze, um fehlerhafte Transfers oder Betrugsversuche zu reduzieren

Prozessoptimierung

- ☑ Bringen Sie Ordnung in Ihre Banklandschaft und senken Sie so das Betrugsrisiko
- ☑ Setzen Sie sich für eine unternehmensweite Standardisierung und die Nutzung einer einheitlichen Plattform ein
- ☑ Führen Sie Prozessautomatisierung ein und sorgen Sie für Compliance bzw. beugen Sie Manipulation vor
- ☑ Digitalisieren Sie Ihre Prozesse und verbessern Sie Ihre Datenqualität, um u.a. Audits zu vereinfachen
- ☑ Profitieren Sie von ausgefeilten Freigabeprozessen (Vier- bis Zwölf-Augen- Prinzip)

[3] https://www.treasurers.org/hub/treasurer-magazine/key-insights-business-treasury-2018-report. Zuletzt abgerufen am 9. September 2020.

Ihre Herausforderung: **Standardmaßnahmen finden, die Cyberbetrug verhindern und entschärfen**

45% aller Mitarbeiter erhalten von Ihrem Arbeitgeber keine Schulung zum Thema Cybersicherheit.[4]

Wo liegt das Problem?

Heutzutage sind Cyberangriffe nicht nur hartnäckiger, sondern auch gefährlicher. Das macht es wahrscheinlicher, dass auch Ihr Unternehmen angegriffen werden könnte. Wenn Mitarbeiter, darunter auch Neueinstellungen, nicht wissen, welche Präventionsmaßnahmen sie treffen können, wird es zu Zwischenfällen kommen. Wer nicht weiß, wie er auf einen Angriff reagieren soll, tut unter Umständen gar nichts oder das Falsche und macht die Situation dadurch noch schlimmer.

Welche Maßnahmen können Sie sofort treffen?

Genau deshalb sind Schulung und Unterstützung wichtiger denn je.

- Setzen Sie sich mit den Sicherheitsrichtlinien und Prozessvorgaben für Ihr Treasury auseinander.
- Wenn Sie derzeit noch kein Treasury Management System im Einsatz haben, dann lassen Sie sich von Ihrer IT-Abteilung das Daten-Backup, Notfallpläne sowie Prozesse im Falle eines Systemausfalls oder Angriffs erklären.
- Wenn Sie gerade auf der Suche nach einer Treasury-Management-Lösung sind, lassen Sie sich von möglichen Anbietern deren Vorschläge für Sicherheitsschulungen erläutern.
- Sie nutzen bereits ein Treasury Management System? Dann bitten Sie Ihren Anbieter um einen Audit, im Rahmen dessen Schulungen, Fortbildungen und Notfallpläne beleuchtet werden.

Wie kann der richtige Anbieter helfen?

Ein ganzheitlicher Ansatz beim Thema Schulung und Weiterbildung geht über die Implementierungsphase hinaus. Er hilft Ihnen, Cybersicherheit in Ihren Alltag zu integrieren und gibt Ihnen einen Krisenplan an die Hand.

Das dürfen Sie von einem guten Partner erwarten:

- Regelmäßige Schulungen und Weiterbildungen zum Thema Cybersicherheit für alle Mitarbeiter, auch solche, die nicht vor Ort sind
- Unterstützung bei der Umsetzung einheitlicher Cybersicherheits-Standards
- Erarbeitung von Notfallplänen und deren Kommunikation

[4] https://www.comptia.org/content/research/the-evolution-of-security-skills
(2017) CompTIA, The Evolution of Security Skills. Zuletzt abgerufen am 10. September 2020

Gemeinsam stark: **Smarter Together**

Sie spielen eine große Rolle für die Cybersicherheit Ihres Unternehmens. Was aber halten Sie von der Idee, nicht nur Ihr Unternehmen, sondern auch andere bei der Betrugsprävention zu unterstützen, indem Sie Zugriff auf anonymisierte sicherheitsrelevante Daten aus der gesamten Community erlangen bzw. dazu beitragen?
Sie haben die Wahl. Bauen Sie auf ein noch stärkeres Fundament und profitieren Sie vom geballten Wissen aller, gemeinsam mit Coupa. Denn geteiltes Wissen ist doppeltes Wissen! Wir nutzen ausschließlich anonymisierte Daten und sorgen dafür, dass Ihnen kein Wettbewerbsnachteil entsteht. Ihnen bieten sich im Gegenzug ganz neue Möglichkeiten, von den Erfahrungen und Best Practices anderer zu lernen und das allgegenwärtige Thema Cybersicherheit gemeinsam anzugehen.

Cybersicherheit ist möglich.

Wie können wir Ihnen helfen? Jetzt Kontakt aufnehmen