xSuite

It's simple. It's digital.

Whitepaper

Gefälschte Rechnungen. Eine echte Bedrohung!

www.wmd.de

WMD | GROUP

Inhalt

WMD | GROUP

01

Gefälschte Rechnungen sind an der Tagesordnung

Knapp die Hälfte (47%) der kleinen und mittelständischen Unternehmen (KMU) in Großbritannien hat im Jahr 2016 betrügerische oder zumindest verdächtige Rechnungen erhalten[1]. Dieser Wert verwundert nicht. In den letzten Jahren jagte ein Medienbericht über Schadsoftware – wie Trojaner, Ransomware oder Locky – den nächsten. Eine andere Zahl überrascht aber doch: Dieselbe Studie beziffert den jährlichen Schaden durch gefälschte Rechnungen auf durchschnittlich 1.658 GBP pro KMU. Das heißt, ein nicht unerheblicher Teil der Unternehmen muss auf die gefälschten Rechnungen auch tatsächlich hereingefallen sein.

Diese Zahl gibt zu denken und ist der Anlass für dieses Whitepaper. Nachfolgend möchten wir Sie dafür sensibilisieren, dass gefälschte Rechnungen – auch unabhängig von Schadsoftware – eine echte Gefahr darstellen. Wir beleuchten, was genau mit einer gefälschten Rechnung gemeint ist, welche Schwachstellen in Unternehmen und Prozessen sich Kriminelle zu Nutze machen und welche aktuellen Entwicklungen die Bedrohung noch verschlimmern können. Und natürlich geben wir Ihnen Tipps an die Hand, wie Sie gefälschte Rechnungen besser erkennen und zeigen auf, welchen Beitrag eine Automatisierungslösung dazu leistet.

[1]Vgl. https://www.telegraph.co.uk/business/digital-management/how-to-prevent-invoice-fraud/ und https://www.tungsten-network.com/blog/archive/the-staggering-scale-of-invoice-fraud/, abgerufen im Januar 2019.

02

Ein Beispiel aus der Praxis

Ahrensburg, im November 2018:
An die auf der Website angegebene allgemeine E-Mail-Adresse der WMD wurde folgende E-Mail gesendet:

Betreff: Abrechnung BZ3882560

Sehr geehrte Damen und Herren,

bitte korrigieren Sie die beigefügte Rechnung.
Wir freuen uns auf die weitere Zusammenarbeit!

Mit freundlichen Grüßen

Anhang: RECH-BZ3882560.doc

Die Signatur unter der E-Mail enthielt die korrekte Telefondurchwahl und Faxnummer sowie E-Mail-Adresse eines Ansprechpartners bei einem unserer Bestandskunden. Auch der Absender der E-Mail passte dazu. Alles sah täuschend echt aus.

Ein Hinweis unseres Datenschutzbeauftragten und ein Anruf beim Ansprechpartner auf Kundenseite brachte jedoch die Gewissheit: Die Rechnung war nicht echt, es handelte sich um die neueste Trojaner- Generation[2]. Die Sensibilisierung über die letzten Jahre zum Thema Schadsoftware hatte also Früchte getragen.

So wie bei uns, ist die Situation in vielen Unternehmen: In den vergangenen Jahren ist ein Bewusstsein entstanden für die Gefahren durch als Rechnung oder Rechnungsanhang getarnte Schadsoftware. Dadurch ist eine ebenfalls nicht zu unterschätzende Gefährdung allerdings aus dem Fokus geraten: Gefälschte Rechnungen können auch ganz ohne Trojaner oder Verschlüsselungssoftware im Anhang zu nicht unerheblichen Schäden führen.

[2]Vgl. https://www.heise.de/security/meldung/Trojaner-Achtung-bei-angeblichen-Rechnungen-4219043.html, abgerufen im Januar 2019.

03

Rechnungsfälschung – Die kleine Schwester des CEO-Fraud

Auch das Schlagwort „CEO-Fraud“ oder „CEO-Betrug“ hat in der vergangenen Zeit für Wirbel gesorgt. Dabei verschaffen sich Cyber-Kriminelle Zugang zum E-Mail-Account eines leitenden Angestellten oder Mitglieds der Geschäftsführung oder imitieren diesen, sodass sie in dessen Namen E-Mails versenden können. Diese Betrugsmasche wird auch als BEC (für „Business Email Compromise“) bezeichnet. In diesen, oftmals täuschend echten E-Mails, wird dann ein Mitarbeiter des Unternehmens zur dringenden Überweisung einer größeren Geldsumme aufgefordert. Es gibt zahlreiche Beispiele, wie Unternehmen aller Größen so teils um mehrstellige Millionenbeträge erleichtert wurden. Das beliebteste Ziel der E-Mail-Betrüger sind CFOs und Finanzvorstände.[3]

Einen ähnlichen Ansatz verfolgen gefälschte Rechnungen: Der Betrüger gibt sich nicht als Geschäftsführer aus, sondern als Lieferant. Häufig werden zur Tarnung Lieferanten gewählt, mit denen das Opfer bereits eine Geschäftsbeziehung unterhält und regelmäßig Rechnungen über nicht allzu hohe Summen erhält. Typische Beispiele sind Lieferanten für Bürobedarf oder Putzdienste, deren Rechnungssummen jeweils unter üblichen Freigabeschwellen liegen, zum Beispiel unter 1.000 EUR. Häufig wird bei gefälschten Rechnungen Dringlichkeit erzeugt, um zu einer schnellen, unüberlegten Zahlung zu verleiten, beispielsweise durch den Hinweis „Zahlung 90 Tage überfällig“. Der/die Kriminelle gibt dann andere Kontodaten an und meist fliegt der Betrug erst auf, wenn sich der echte Lieferant meldet und Mahnungen sendet.[4] Dass diese Form der Cyberkriminalität, CEO-Fraud und Rechnungsfälschung, ein relevantes Thema ist, spiegelt sich auch im umfangreichen Angebot an „Vertrauensschadenversicherungen“ wider, die oft auch explizit diese Themen abdecken.[5]

Man könnte meinen, dass der Bedarf hierfür vor allem bei KMUs besteht. Diese können weniger dediziertes Fachpersonal für das Thema Security vorhalten und mögen als weniger professionell und vielleicht sogar gutgläubiger als größere Unternehmen gelten, erscheinen also gefährdeter. Dem ist aber nicht so. Es kristallisiert sich heraus, dass Cyber-Kriminelle sich zunehmend auf mittelgroße und größere Unternehmen spezialisieren. Zum einen ist bei diesen eine größere Beute zu erhoffen, zum anderen gehen deutlich mehr Rechnungen ein und die Prozesse sind komplizierter und vor allem anonymer – die perfekte Ausgangsposition für einen möglichen Rechnungsbetrug.[6]

[3]Vgl. https://www.wiwo.de/technologie/digitale-welt/chef-betrug-wie-falsche-chefs-millionen-ergaunern/14616996-all.html und
[3+4+6]https://www.springerprofessional.de/internetkriminalitaet/risikomanagement/ceo-betrug-nimmt-drastisch-zu/12173276, abgerufen im Januar 2019.
[4]https://www.financialfraudaction.org.uk/businesses/advice/invoice-fraud/ und https://blog.procurify.com/2016/05/12/whats-invoice-fraud-prevent-invoice-fraud/, abgerufen im Januar 2019.
[5]Einige Beispiele für Vertrauensschadenversicherungen: https://www.eulerhermes.de/vertrauensschadenversicherung.html und https://www.axa.de/geschaeftskunden/vertrauensschadenversicherung und https://www.zurich.de/de-de/geschaeftskunden/kredit-und-kaution/kreditversicherung/

04

Warum werden gefälschte Rechnungen nicht als solche erkannt?

Trotz Sensibilisierung und spektakulären Medienberichten zu Fällen von CEO-Fraud, kommt es immer wieder dazu, dass gefälschte Rechnungen nicht als solche erkannt und daher bezahlt werden. Woran liegt das?

Es gibt verschiedene Einflussfaktoren, die dazu führen, dass gefälschte Rechnungen nicht erkannt werden. Ein wichtiger Punkt sind Strukturen und Prozesse, die sich aktuell im Wandel befinden. Nur 3% unserer Kunden nehmen heute immer noch ausschließlich Rechnungen in Papierform an – 97% erhalten Rechnungen sowohl in Papier- als auch in elektronischer Form.[7]

Zudem kommen bei elektronischen Rechnungen häufig verschiedene Formate wie E-Mail, PDF, Word, XML, EDI, JPG, etc. vor. Die Rechnungen gehen außerdem auf verschiedenen Wegen und an verschiedenen Stellen ein: im zentralen Posteingang, in den Niederlassungen oder Geschäftsstellen, in den Fachabteilungen, in zentralen E-Mail-Postfächern, in den individuellen E-Mail-Accounts von Mitarbeiter/innen.

Weiter verkompliziert wird die Situation durch Duplikate: Lieferanten senden Rechnungen als E-Mail-Anhang im PDF-Format und zusätzlich noch einmal per Post. Eine E-Mail-Rechnung wird von verschiedenen Mitarbeitern an ein zentrales Postfach weitergeleitet und liegt so doppelt vor. Die Möglichkeiten, wie es – häufig auch unabsichtlich – zu doppelten Rechnungen kommt, sind vielfältig.

Dieser unübersichtlichen Situation steht ein Buchhaltungsteam gegenüber, das gleichzeitig noch weitere Herausforderungen hat: Das Volumen der zu bearbeitenden Rechnungen steigt oftmals, während die Anzahl der Mitarbeiter/innen in der Buchhaltung gleich bleibt. Oder es können offene Stellen aufgrund von Fachkräftemangel nicht schnell genug nachbesetzt werden. Die Buchhaltung wird als reines Cost Center angesehen und steht damit unter stetigem Einsparungsdruck, es soll alles schneller und effizienter gehen. So oder so: Häufig ist die Arbeitslast der Buchhalter/innen für wirklich gründliche Arbeit zu hoch.

Wenn gefälschte Rechnungen nicht erkannt werden, muss das also nicht an der Nachlässigkeit zuständiger Buchhaltungsmitarbeiter/innen liegen. Häufig lassen sich in der gegebenen Situation und ohne Prozessautomatisierungen nur geringe Verbesserungen erreichen. Eine Automatisierungslösung kann hingegen die Finanzbuchhaltung deutlich entlasten, sodass die Mitarbeiter/innen sich besser auf ihre Kernaufgaben konzentrieren können und die Qualität steigen wird.

Ein konkretes Beispiel: Der Buchhalter/in spart Zeit, wenn die Rechnungsinformationen nicht händisch abgetippt werden müssen, sondern eine automatische Beleglesung dies übernimmt. Diese so gewonnene Zeit kann genutzt werden, um die ausgelesenen Inhalte noch einmal gründlich zu überprüfen.

[7]Vgl. „Elektronische Rechnungsverarbeitung 2018. Ergebnisse der WMD Kundenumfrage zu xFlow Invoice for SAP“

05

Wie sorge ich dafür, dass ich gefälschte Rechnungen erkenne?

Es gibt vier wichtige Stellschrauben, damit Sie gefälschte Rechnungen eher erkennen. Diese sollten in Ihren internen Kontrollsystemen berücksichtigt werden:

1. Abgleich der Rechnung mit der zugrundeliegenden Bestellung

Dieser Punkt mag selbstverständlich klingen – nichtsdestotrotz wird er im Alltag häufig nicht gründlich oder gar nicht ausgeführt. Achten Sie darauf, dass die Positionen, die Mengen und die Rechnungssumme sowie die Daten des Rechnungsstellers auf der Rechnung wirklich mit der Bestellung übereinstimmen. Prüfen Sie auch, dass zu der Rechnung bereits ein Wareneingang gebucht wurde. Wenn es einen sogenannten „3-Way-Match" zwischen Bestellung, Rechnung und Wareneingang gibt, ist das Risiko äußerst gering, dass es sich um einen Betrugsversuch handelt.[8]

2. Auf Auffälligkeiten achten

Häufig werden für einen Rechnungsbetrug Lieferanten als Deckmantel genutzt, mit denen Sie bereits eine Geschäftsbeziehung haben und regelmäßig Rechnungen erhalten. Wenn Sie von einem Lieferanten sonst durchschnittlich 5 Rechnungen im Monat erhalten und plötzlich 50 im Monat, sollten Sie den Grund prüfen. Eine Hohe Dringlichkeit und zum Beispiel die Aussage, dass die Rechnung bereits deutlich überfällig ist, ist ebenfalls typisch bei Rechnungsbetrug. Viele Unternehmen haben 500 EUR, 1.000 EUR oder 5.000 EUR als Schwellwerte für Freigaben. Gefälschte Rechnungen weisen daher oftmals einen Wert aus, der knapp darunter liegt.[9]

3. Bei neuer Bankverbindung: Nachfragen

Wenn Sie eine Benachrichtigung von einem Kreditor erhalten, dass die Bankverbindung sich geändert hat oder feststellen, dass eine andere Bankverbindung angegeben wurde, sollten Sie dies in jedem Fall prüfen. Es empfiehlt sich dazu, nicht nur per E-Mail zu kommunizieren, sondern mit dem bisherigen Ansprechpartner zu telefonieren. Nur so können Sie sichergehen, dass die neuen Bankdaten korrekt sind. Erhalten Sie eine Rechnung von einem bisher unbekannten Kreditor, ist es sinnvoll, das Unternehmen zu googlen: Gibt es diese Firma? Existiert sie unter der angegebenen Adresse? Sind die Kontaktdaten korrekt?[10]

4. Sensibilisierung der Mitarbeiter/innen

Wichtig bei allen oben genannten Punkten: Nicht nur Sie als Abteilungsleiter/in müssen über die möglichen Gefahren im Bilde sein. Auch Ihre Mitarbeiter/innen, die die tägliche Bearbeitung und Freigabe von Rechnungen durchführen, müssen für diese Themen sensibilisiert werden. Eine schriftliche Dokumentation der Prozesse und klare Freigaberegeln sind sinnvoll.

[8]Vgl. https://guide.iacrc.org/potential-scheme-false-inflated-and-duplicate-invoices/ und https://www.financialfraudaction.org.uk/businesses/advice/invoice-fraud/ und https://www.accountingcoach.com/blog/what-is-three-way-match, abgerufen im Januar 2019.
[9]Vgl. http://www.nextprocess.com/ap-software/7-tips-for-preventing-invoice-fraud/, abgerufen im Januar 2019.
[10]Vgl. https://invoiced.com/blog/6-ways-to-spot-and-prevent-invoice-fraud, abgerufen im Januar 2019.

06

Nutzen einer Automatisierungslösung für die Rechnungsverarbeitung

Insbesondere zur Umsetzung der ersten beiden Punkte in Kapitel 05 ist eine Workflowlösung für die Rechnungsverarbeitung hilfreich. Durch die Automatisierung von zeitraubenden, monotonen Arbeitsschritten, wie zum Beispiel der Dateneingabe ins System, werden die Mitarbeiter/innen in der Buchhaltung deutlich entlastet. So bleibt mehr Zeit, um eingehende Belege konzentriert und gründlich zu prüfen. Die Gefahr, dass gefälschte Rechnungen nicht erkannt werden, sinkt.

Eine Automatisierungslösung kann außerdem dazu genutzt werden, Abweichungen zwischen Rechnung, Bestellung und Wareneingang automatisch festzustellen und entsprechende Warnhinweise zu geben. Definierte Freigabeprozesse und zusätzliche Sicherheitsvorkehrungen, wie zum Beispiel ein 4-Augen-Prinzip, können zudem im System hinterlegt werden. So wird die Einhaltung dieser Prozesse und Vorgaben sichergestellt, eine Automatisierungslösung kann so zur technischen Umsetzung Ihres internen Kontrollsystems beitragen.

Auch bieten Automatisierungslösungen häufig verschiedenste Auswertungsmöglichkeiten, beispielsweise zur Anzahl und den Summen von Rechnungen pro Kreditor in einem bestimmten Zeitraum. So werden Abweichungen und Unregelmäßigkeiten sichtbar. Durch eine durchgängige Protokollierung lassen sich zudem auch im Nachhinein noch alle Schritte im Detail nachvollziehen.

Eine Automatisierungslösung für die Eingangsrechnungsverarbeitung kann Ihnen zwar keinen 100%igen Schutz vor gefälschten Rechnungen garantieren, aber steigert deutlich die Chance, diese frühzeitig zu erkennen.

07

Fazit gefälschte Rechnungen: Gefahr erkannt, Gefahr gebannt!

In den letzten Jahren sind als Rechnung getarnte Trojaner und Ransomware eines der meistdiskutierten Security-Themen gewesen. Darüber ist ein anderes – genauso reales – Risiko für Unternehmen in den Hintergrund des Bewusstseins getreten: Betrugsversuche mit Hilfe von gefälschten Rechnungen.

Es zeichnet sich ab, dass Kriminelle zum einen immer raffinierter werden und zum anderen zunehmend mittlere und größere Unternehmen gezielt ins Visier nehmen. Rechnungsbetrug erfolgt dann häufig nach dem Vorbild des CEO-Fraud.

Mit einigen Maßnahmen lassen sich gefälschte Rechnungen schneller erkennen. Die vier wichtigen Schritte dazu sind:

1. Gründlicher Abgleich von Rechnung und Bestellung
2. Auf Auffälligkeiten achten
3. Bei neuer Bankverbindung: nachfragen
4. Sensibilisierung der Mitarbeiter.

Insbesondere die Umsetzung von Punkt 1 wird durch den Einsatz von Automatisierungslösungen für die Eingangsrechnungsverarbeitung deutlich erleichtert. Zudem liefern diese Transparenz, Auswertungsmöglichkeiten sowie dauerhafte Nachvollziehbarkeit und bilden so die Grundlage für Punkt 2. Demgegenüber sind die Punkte 3 und 4 rein organisatorische Maßnahmen.

--

Über die WMD Group

WMD wurde 1994 gegründet. Als Softwarehersteller und SAP Silver Partner bieten wir mit unserer Informationsmanagement-Plattform xSuite® im Bereich Dokumentenmanagement besondere Kompetenz und Expertise an. Die ganzheitlichen Lösungen umfassen die Bereiche digitale Posteingangsverarbeitung, workflowgestützte Rechnungs-, Bestell- und Auftragsbearbeitung, Akten- und Vertragsmanagement sowie Archivierung. Das Produktportfolio der klassischen On-Premises-Lösungen wurde um Services in der Cloud erweitert. Realisiert werden Projekte für Kunden aller Branchen unter Einbindung der jeweils im Einsatz befindlichen ERP-Systeme.

Die WMD bietet alles aus einer Hand: Analyse, Beratung, Projektrealisation, Hard- und Software, Service und Schulung. WMD unterstützt bei Themen wie GoBD und Verfahrensdokumentation und erarbeitet Lösungen, die effizient und kostensparend durch die digitale Betriebsprüfung führen.

Die WMD hat ihren Hauptsitz in Ahrensburg (bei Hamburg) sowie Tochtergesellschaften in Europa, Asien und den USA.

Deutschland
Benelux
Großbritannien
Skandinavien
Singapur
Spanien
Slowakei
USA

WMD Group GmbH
Hamburger Straße 12
22926 Ahrensburg
Tel. +49 (0)4102 88 38 0
info@wmd.de
www.wmd.de

WMD | GROUP