eleven cyber security GmbH

Aktuelle Spam- & Phishing-Kampagnen

eleven

Inhalt

1. Vorstellung eleven + dataglobal Group
2. Vorstellung Ulrich Jansen
3. Aktuelle Spam- & Phishing-Trends
4. Alternative Wege gehen…
5. Vorstellung eXpurgate
6. Fragen? Antworten!

eleven

eleven cyber security GmbH

HAUPTSITZ IN BERLIN

GEGRÜNDET 2001

45 MITARBEITER

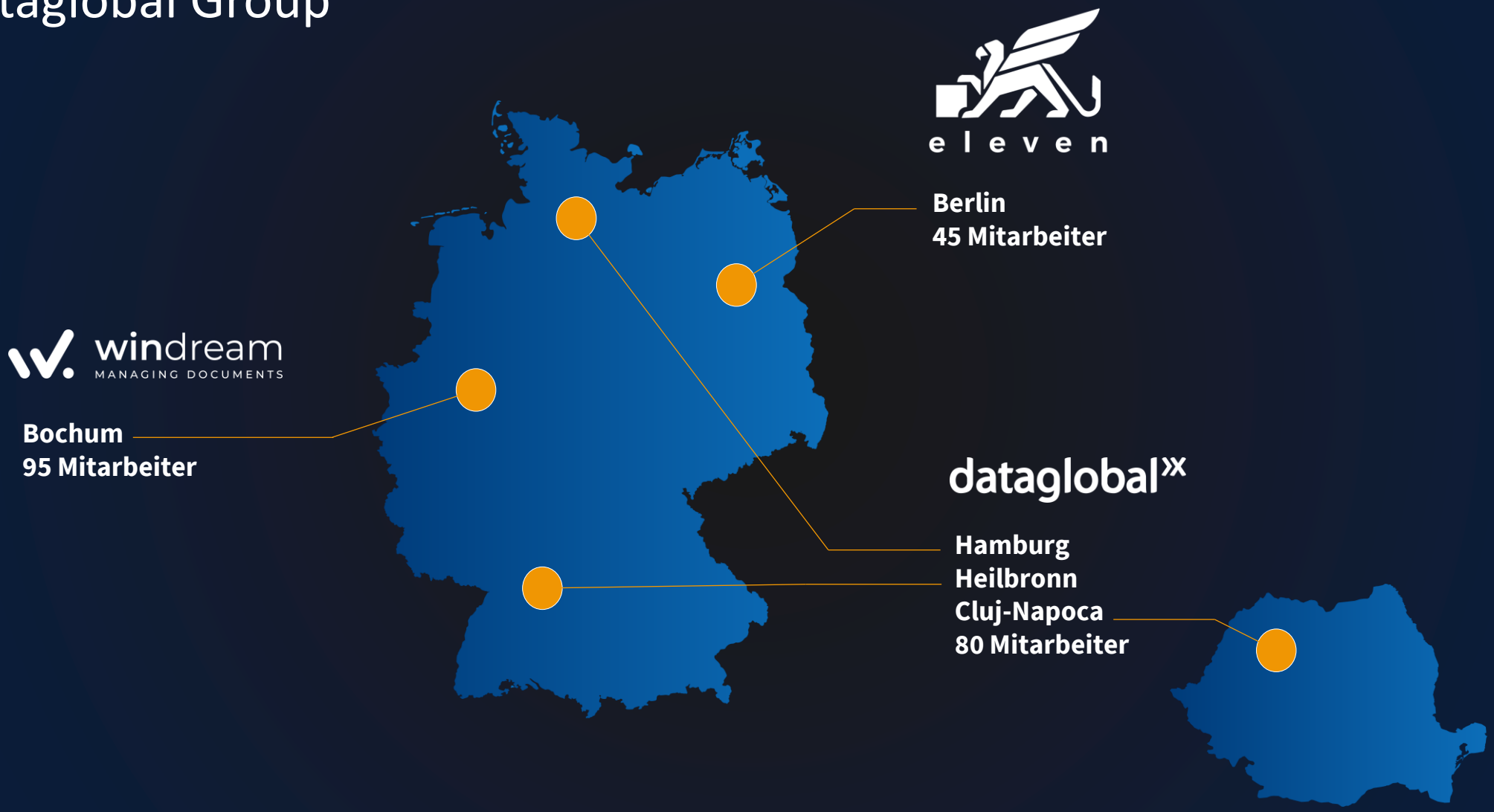
~ 1000 ZUFRIEDENE KUNDEN

KUNDEN AUF 3 KONTINENTEN

Ca. 1 Mrd. analysierte Mails am Tag

50 % ALLER PRIVATEN E-MAILS IN DEUTSCHLAND SIND DURCH eXpurgate GESCHÜTZT

dataglobal Group



Ulrich Jansen

Geschäftsführer eleven cyber security GmbH,
Vice President Technology dataglobal Group

- Bei eleven seit 2006, angefangen als Entwickler
- Geschäftsführer bei eleven seit 2014
- Seit August 2023 Leitung aller technischer Abteilungen bei der dataglobal Group

Spamverteilung 2023

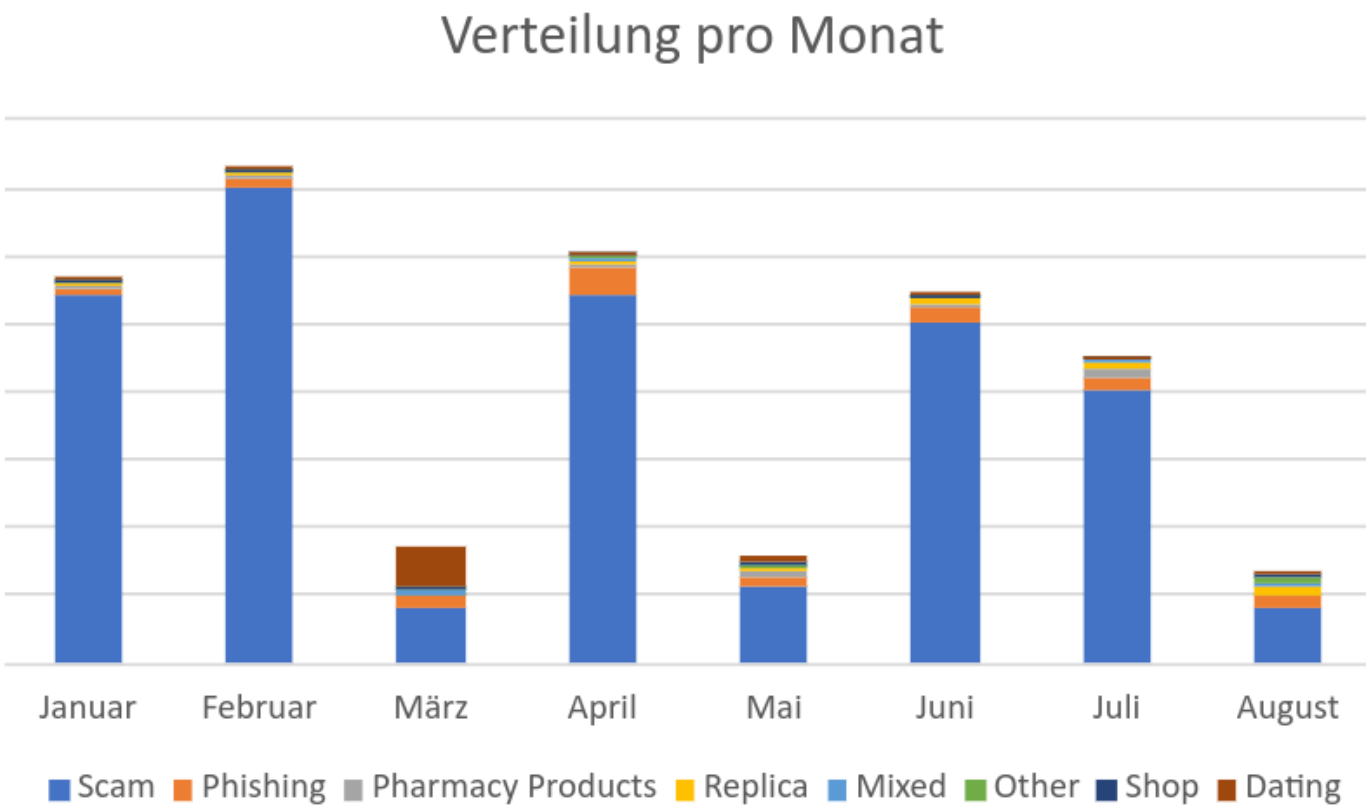
Aktuell größte Gefahren:

- Scam
- Phishing

Anmerkung:

(knapp 90% sind „Grundrauschen“ von kleineren, normalen Spamwellen mit z.B. „Pillenspams“, welche hier nicht gezeigt wird)

Aktuelles Jahr bis August 2023:



Top 2023-Mailing: Bitcoin-Erpressung

- Hohes Versandaufkommen im laufenden Jahr, >90% unter den Top Spams, etwa 9% insgesamt!
- Dominant in jeder Monatsstatistik
- Druckmittel: Vermeintliche Veröffentlichung intimer Video-/Fotoaufnahmen des Empfängers
- Erhöhter Handlungszwang durch Fristsetzung
- Anonyme Bezahlung via Bitcoin-Transaktion
- E-Mail benötigt keine Personalisierung
- Geringe Ressourcen benötigt
- "Fire-and-forget" - E-Mail versenden und auf Geldeingang warten

Top 2023-Mailing: Bitcoin-Erpressung

Ich bin ein Hacker und habe mir erfolgreich Zugang zu Ihrem Betriebssystem verschafft.
Ich habe auch vollen Zugriff auf Ihr Konto.

Ich beobachte Sie nun schon seit einigen Monaten.

Tatsache ist, dass Ihr Computer über eine von Ihnen besuchte Webseite für Erwachsene, mit Malware infiziert worden ist.
Wenn Sie damit nicht vertraut sind, werde ich es Ihnen erklären.
Ein Trojaner-Virus gibt mir vollen Zugriff und Kontrolle über einen Computer oder ein anderes Gerät.
Das bedeutet, dass ich alles auf Ihrem Bildschirm sehen kann, die Kamera und das Mikrofon einschalten kann, ohne dass Sie etwas davon wissen.
Ich habe auch Zugriff auf alle Ihre Kontakte und Ihre gesamte Korrespondenz.

Warum hat Ihr Antivirusprogramm keine Malware erkannt?
Antwort: Die von mir verwendete Malware ist treiberbasiert und ich aktualisiere alle 4 Stunden ihre Signaturen.
Daher kann Ihr Antivirenprogramm die Malware nicht erkennen.
Ich habe ein Video gemacht, das zeigt, wie Sie sich in der linken Hälfte des Bildschirms selbst befriedigen,
und die rechte Hälfte zeigt das Video, welches Sie sich gerade ansehen.

Mit einem Mausklick kann ich dieses Video an alle Ihre E-Mails und Kontakte in Ihren sozialen Netzwerken senden.
Ich kann auch Ihre gesamte E-Mail-Korrespondenz und den Chatverlauf in den von Ihnen verwendeten Messengern veröffentlichen.

Wenn Sie das nicht wollen, überweisen Sie 1400€ in Bitcoin an meine Bitcoin-Adresse
(wenn Sie nicht wissen, wie das geht, suchen Sie einfach bei Google "bitcoin kaufen").

Meine Bitcoin-Adresse (BTC Wallet) lautet: 1ABJTuJ2nKipgAg5Q1KvKg7XftdCJug7eK

Nachdem ich Ihre Zahlung bestätigt habe, werde ich das Video sofort löschen, und das war's. Sie werden nie wieder etwas von mir hören.
Ich gebe Ihnen 50 Stunden (mehr als 2 Tage) Zeit, um zu bezahlen. Wenn Sie diese E-Mail öffnen und der Timer beginnt, werde eine Benachrichtigung erhalten.
Es macht keinen Sinn, irgendwo eine Beschwerde einzureichen, denn diese E-Mail kann nicht nachverfolgt werden wie meine Bitcoin-Adresse.

Spam- & Phishing-Kampagnen

Weitere aktuelle Beispiele:

- Gefälschte Paketankündigung - DHL
- Phishing - DKB
- Phishing - Lufthansa Miles & More
- Phishing – Telekom AG
- Phishing – cPanel via Dateianhang
- Phishing - DocuSign
- Quishing – QR-Code statt Verknüpfung

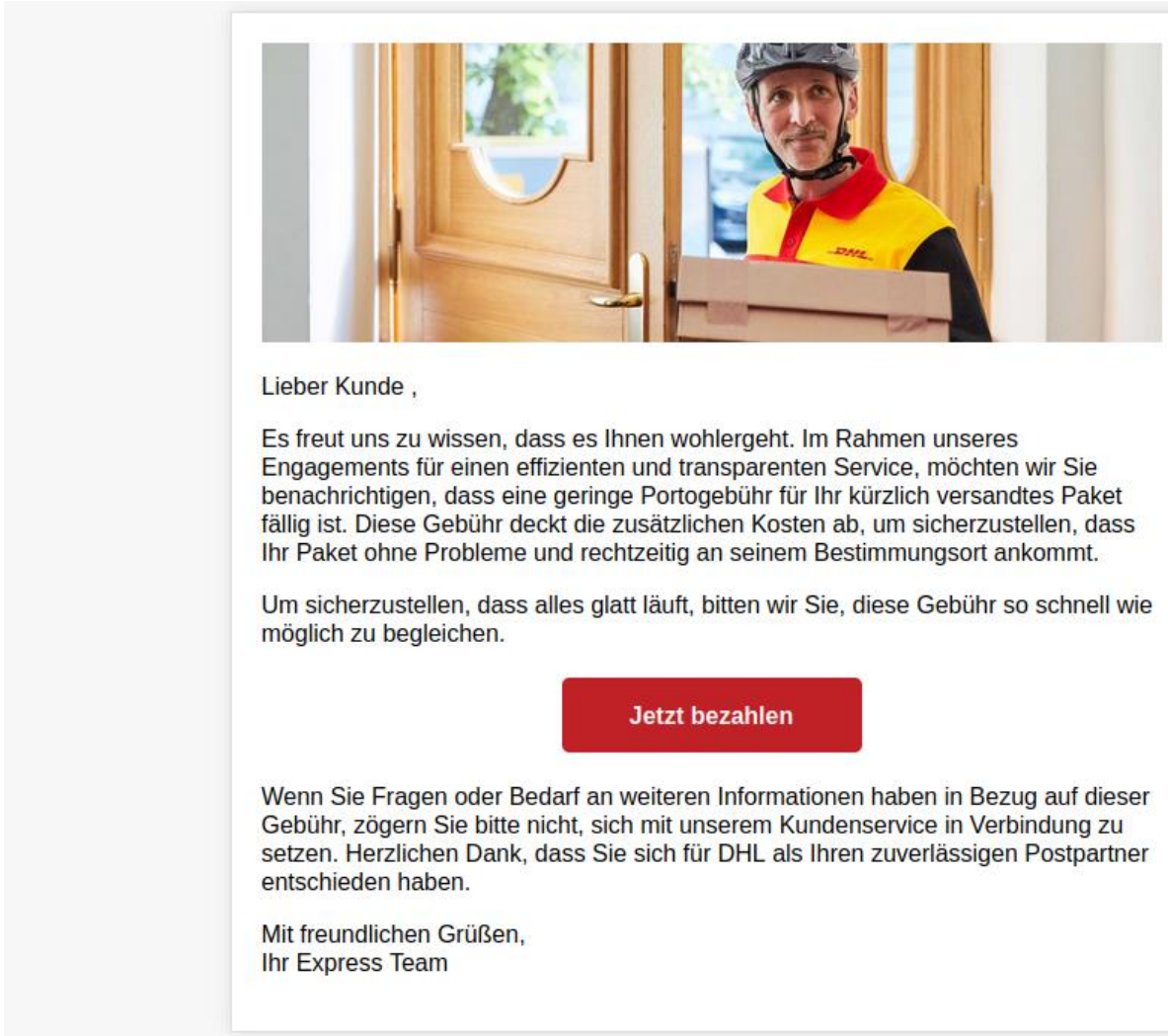
Gefälschte Paketankündigung - DHL

Betreffzeilen:

- "Erforderlich: Bestatigen Sie Ihre Sendung"
- "Ihr DHL-Paket liegt in der Filiale Lieferbereit"
- "Ihr Paket wartet auf die Lieferung"
- "Versandinfo – Dringend“

Absendernamen:

- "Paketdienstzentrum"
- "DHL Express"
- "DHL Post Group AG"



Lieber Kunde ,

Es freut uns zu wissen, dass es Ihnen wohlergeht. Im Rahmen unseres Engagements für einen effizienten und transparenten Service, möchten wir Sie benachrichtigen, dass eine geringe Portogebühr für Ihr kürzlich versandtes Paket fällig ist. Diese Gebühr deckt die zusätzlichen Kosten ab, um sicherzustellen, dass Ihr Paket ohne Probleme und rechtzeitig an seinem Bestimmungsort ankommt.

Um sicherzustellen, dass alles glatt läuft, bitten wir Sie, diese Gebühr so schnell wie möglich zu begleichen.

Jetzt bezahlen

Wenn Sie Fragen oder Bedarf an weiteren Informationen haben in Bezug auf dieser Gebühr, zögern Sie bitte nicht, sich mit unserem Kundenservice in Verbindung zu setzen. Herzlichen Dank, dass Sie sich für DHL als Ihren zuverlässigen Postpartner entschieden haben.

Mit freundlichen Grüßen,
Ihr Express Team

Phishing - DKB

Betreffzeilen:

- "Wir haben Ihr Bankkonto vorübergehend gesperrt"
- "Verifizierung für Ihr DKB-Geschäftskonto erforderlich"

Absendernamen:

- "DKB"
- "DE Kreditbank AG"

DKB Deutsche Kreditbank AG

Sehr geehrter DKB-Kunde,

wir hoffen, dass diese E-Mail Sie gut erreicht. Wir möchten Sie darüber informieren, dass in letzter Zeit einige unregelmäßige Aktivitäten auf Ihrem DKB Business-Konto festgestellt wurden. Um die Sicherheit Ihres Kontos zu gewährleisten und Ihre finanziellen Interessen zu schützen, bitten wir Sie um Ihre sofortige Aufmerksamkeit, um diese Aktivitäten innerhalb der nächsten 24 Stunden zu überprüfen.

Wir sind darauf aufmerksam geworden, dass bestimmte Transaktionen oder Aktivitäten stattgefunden haben, die von Ihrem üblichen Kontoverhalten abweichen. Im Rahmen unseres ständigen Engagements für den Schutz Ihrer Finanzdaten haben wir verbesserte Sicherheitsmaßnahmen eingeführt, um potenzielle Risiken umgehend zu erkennen und zu beseitigen.

Um die Richtigkeit unserer Untersuchung zu gewährleisten und einen unbefugten Zugriff auf Ihr Konto zu verhindern, bitten wir Sie, die unten aufgeführten Schritte zu befolgen:

Klicken Sie auf den folgenden Link, um das sichere Verifizierungsportal aufzurufen: dkb.de/konto-portal

Bitte beachten Sie, dass, wenn Sie den Verifizierungsprozess nicht innerhalb der nächsten 24 Stunden abschließen, Ihr Konto vorübergehend gesperrt werden kann, um weiteren unbefugten Zugriff zu verhindern. Wir entschuldigen uns für etwaige Unannehmlichkeiten, die Ihnen dadurch entstehen, aber dies ist eine notwendige Maßnahme, um den Schutz Ihrer Gelder zu gewährleisten.

Wir danken Ihnen für Ihre schnelle Aufmerksamkeit in dieser Angelegenheit. Wir sind Ihnen dankbar, dass Sie uns dabei helfen, die Sicherheit und Integrität Ihres DKB-Kontos zu wahren.

Mit freundlichen Grüßen,

DKB Kundenbetreuung

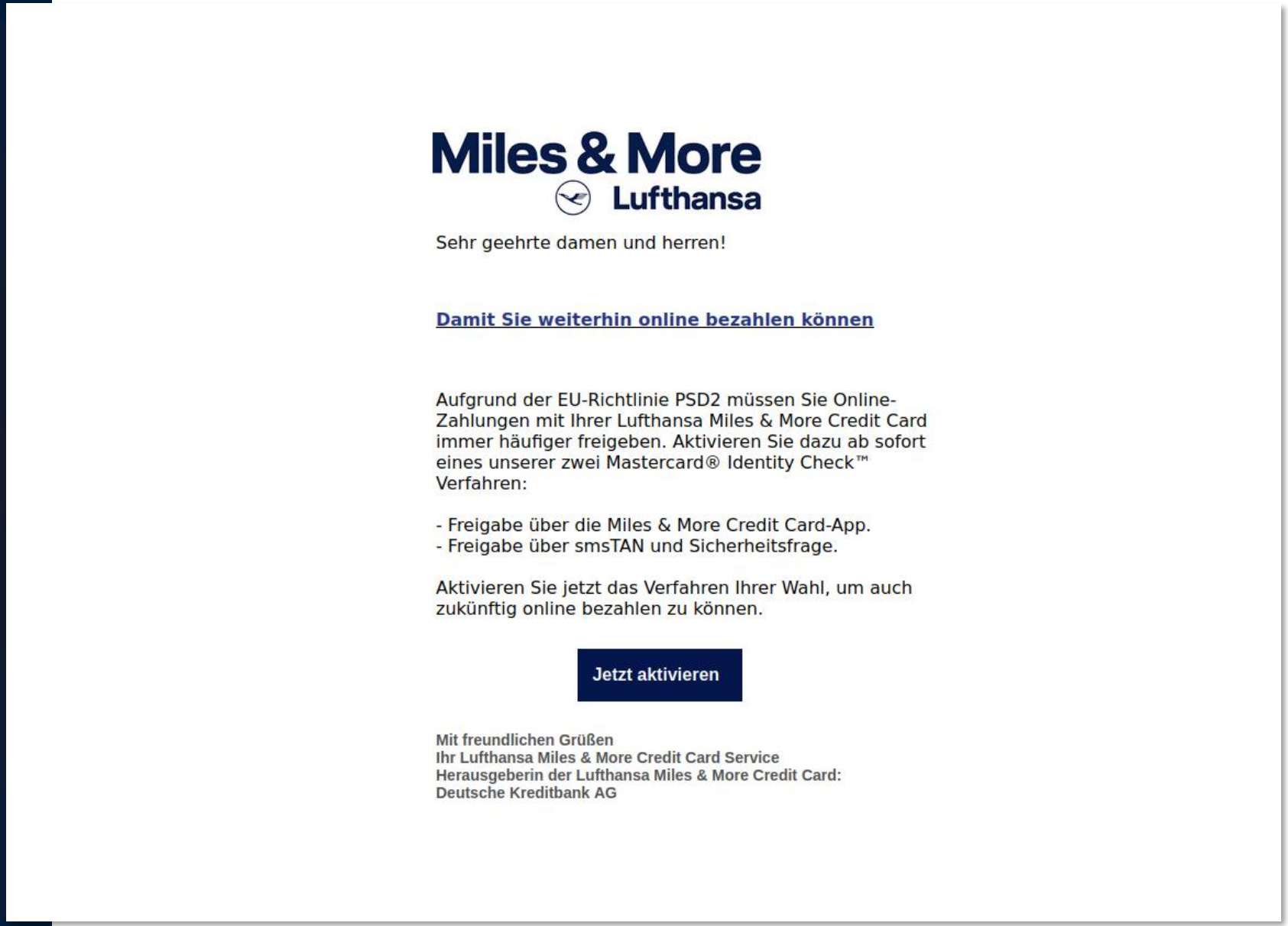
Phishing - Lufthansa Miles&More

Betreffzeilen:

- "Anmeldung zum Mastercard Identity Check!"
- "Servicekommunikation : 3DS-Doppelauthentifizierung aktivieren"

Absendernamen:

- "Miles & More"
- "Miles & More Kreditkarte"



Miles & More
Lufthansa

Sehr geehrte damen und herren!

Damit Sie weiterhin online bezahlen können

Aufgrund der EU-Richtlinie PSD2 müssen Sie Online-Zahlungen mit Ihrer Lufthansa Miles & More Credit Card immer häufiger freigeben. Aktivieren Sie dazu ab sofort eines unserer zwei Mastercard® Identity Check™ Verfahren:

- Freigabe über die Miles & More Credit Card-App.
- Freigabe über smsTAN und Sicherheitsfrage.

Aktivieren Sie jetzt das Verfahren Ihrer Wahl, um auch zukünftig online bezahlen zu können.

Jetzt aktivieren

Mit freundlichen Grüßen
Ihr Lufthansa Miles & More Credit Card Service
Herausgeberin der Lufthansa Miles & More Credit Card:
Deutsche Kreditbank AG

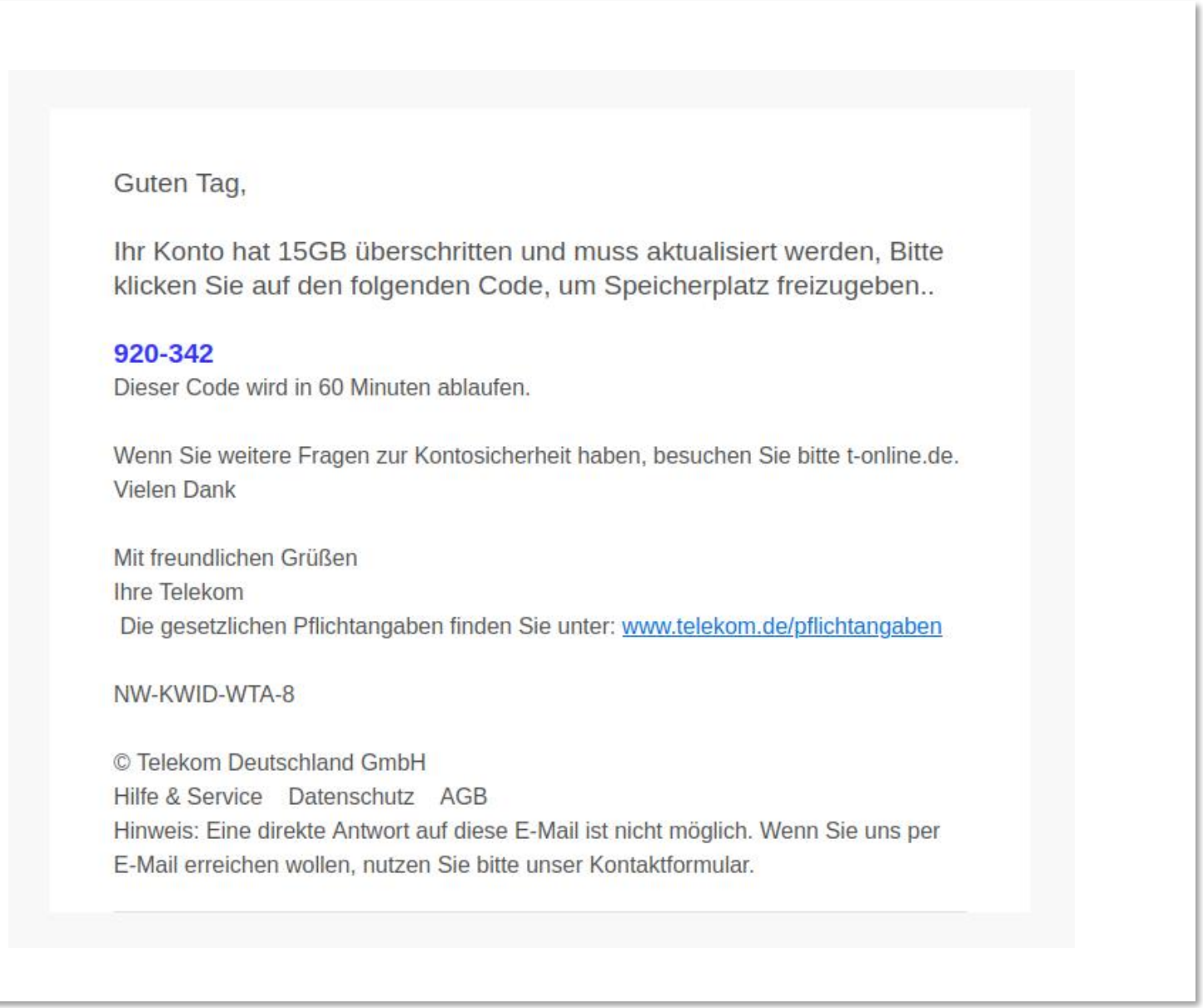
Phishing - Telekom AG

Betreffzeilen:

- "Ihr Konto hat 15GB überschritten und muss aktualisiert werden"
- "Server-Sweep-Warnung"

Absendernamen:

- "Telekom"
- "Telekom AG"



Guten Tag,

Ihr Konto hat 15GB überschritten und muss aktualisiert werden, Bitte klicken Sie auf den folgenden Code, um Speicherplatz freizugeben..

920-342
Dieser Code wird in 60 Minuten ablaufen.

Wenn Sie weitere Fragen zur Kontosicherheit haben, besuchen Sie bitte t-online.de.
Vielen Dank

Mit freundlichen Grüßen
Ihre Telekom
Die gesetzlichen Pflichtangaben finden Sie unter: www.telekom.de/pflichtangaben

NW-KWID-WTA-8

© Telekom Deutschland GmbH
Hilfe & Service Datenschutz AGB
Hinweis: Eine direkte Antwort auf diese E-Mail ist nicht möglich. Wenn Sie uns per E-Mail erreichen wollen, nutzen Sie bitte unser Kontaktformular.

Phishing – cpanel via HTML-Dateianhang

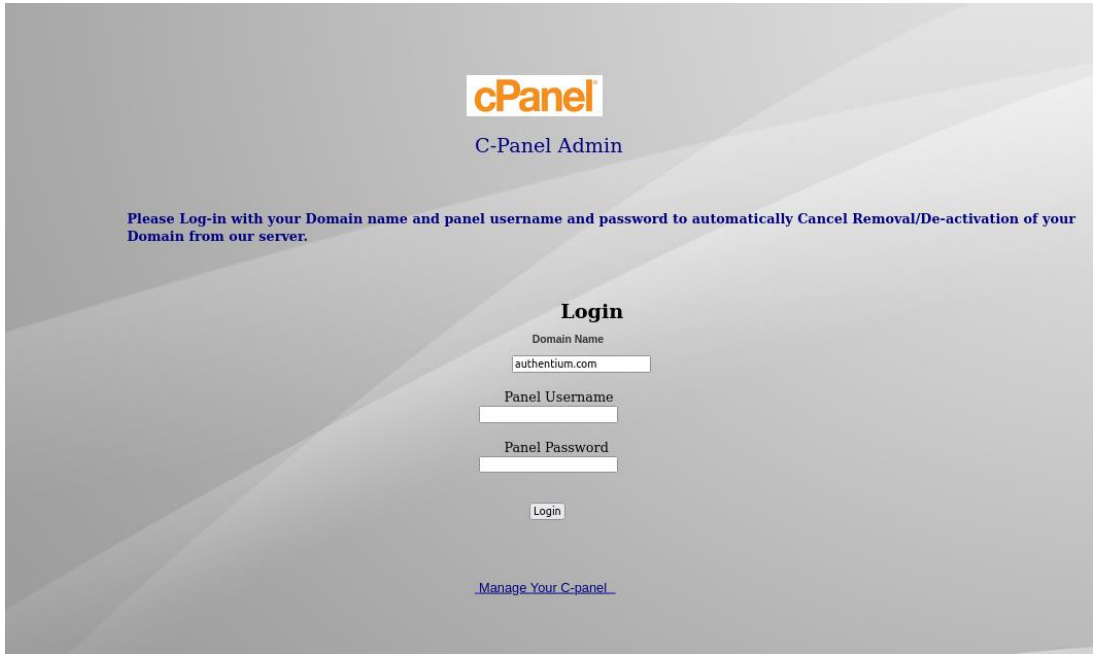
Betreffzeilen:

- "8/7/2023 2:45:31 a.m. Final Notice for Domain : authentium.com“

Absendernamen:

- "cPanel on authentium.com"

HTML-Dateianhang:



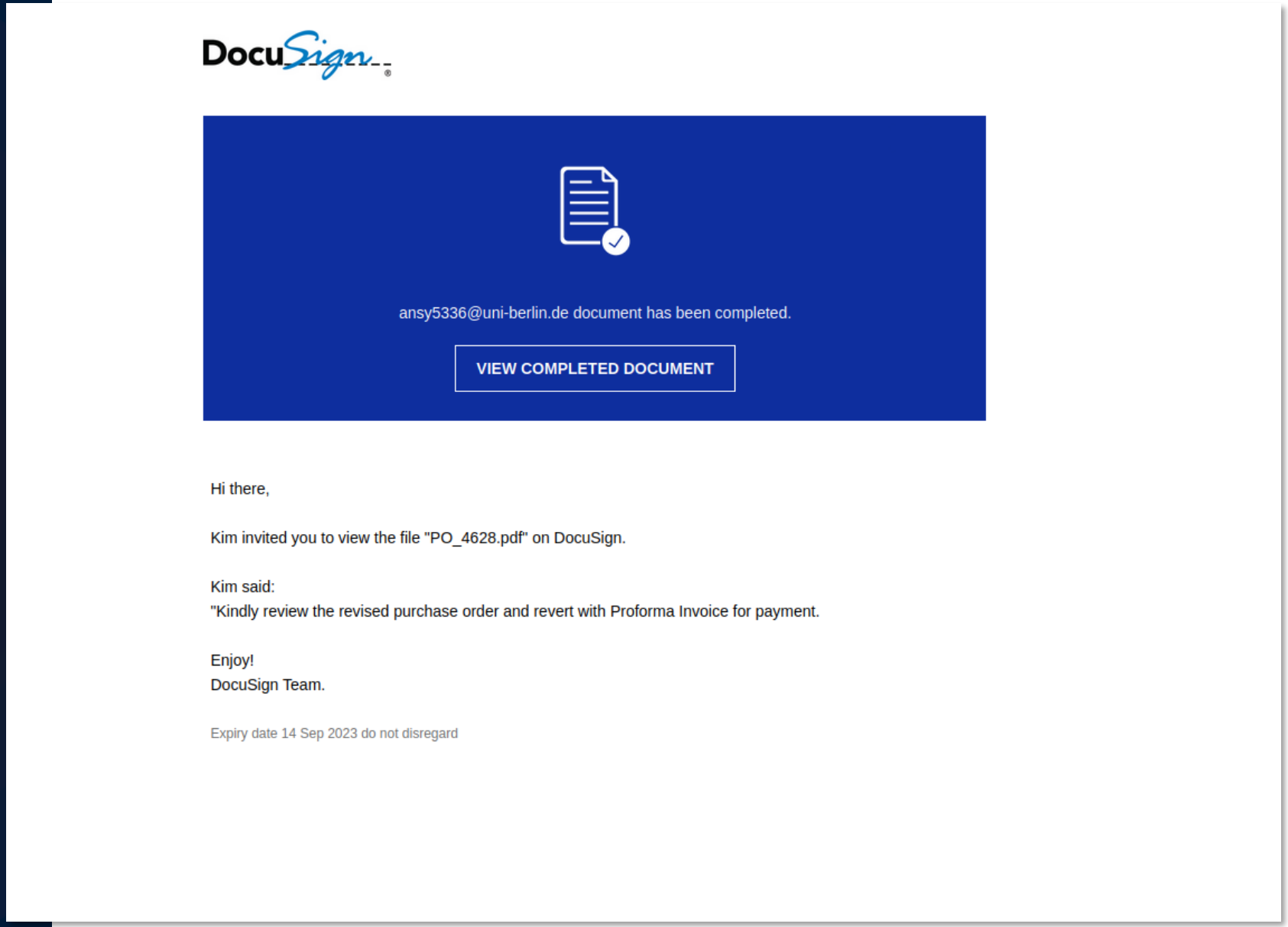
Phishing – DocuSign

Betreffzeilen:

- "You have received a new Document using DocuSign"
- "A secured document was shared with you via DocuSign"
- "You have a message via DocuSign Sharepoint"

Absendernamen:

- "DocuSign"
- "DocuSign Disclosure"



DocuSign

ansy5336@uni-berlin.de document has been completed.

VIEW COMPLETED DOCUMENT

Hi there,

Kim invited you to view the file "PO_4628.pdf" on DocuSign.

Kim said:
"Kindly review the revised purchase order and revert with Proforma Invoice for payment.

Enjoy!
DocuSign Team.

Expiry date 14 Sep 2023 do not disregard

Quishing – QR-Code statt Verknüpfung

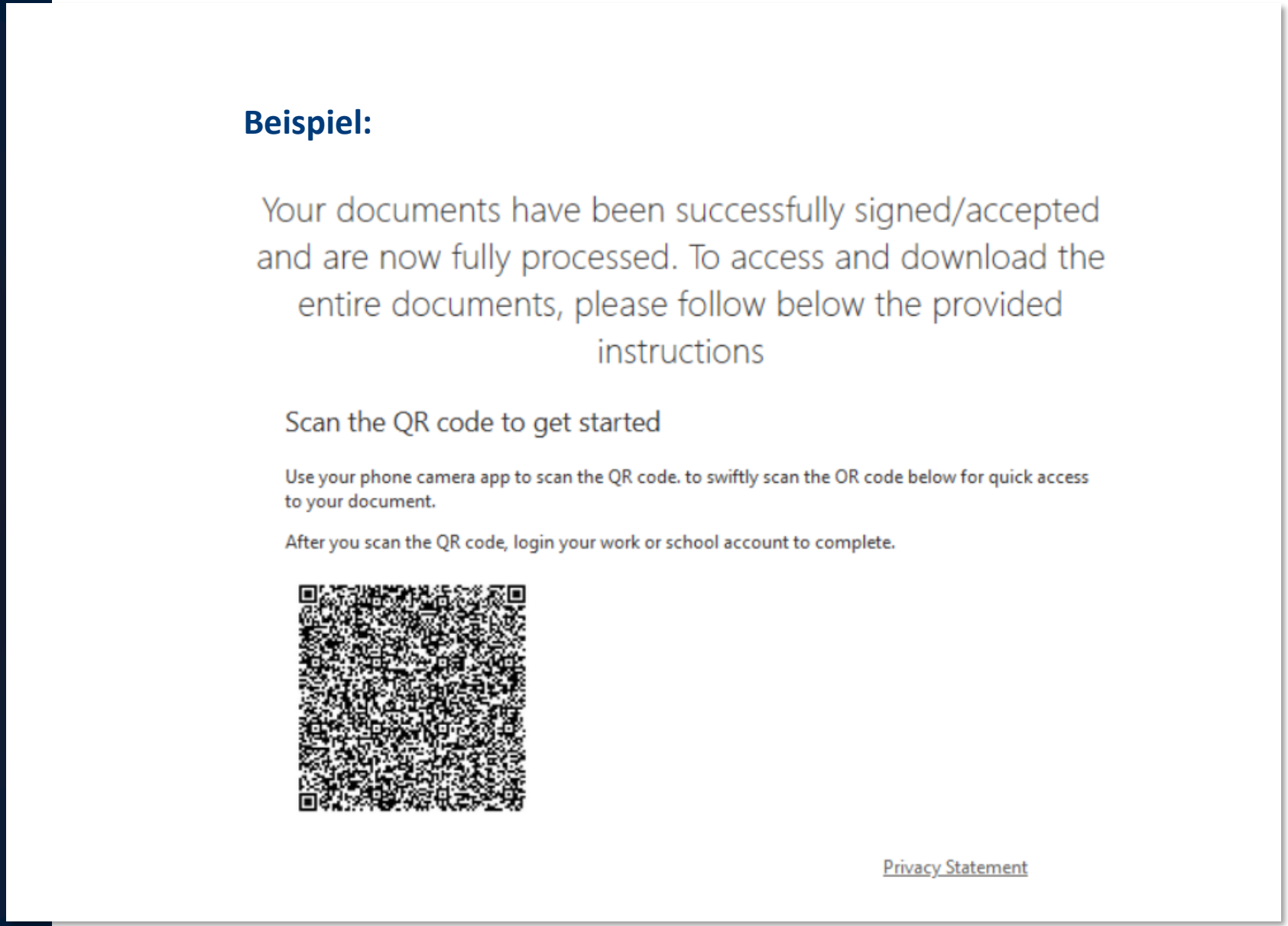
Betreffzeilen

- "Annual 401k contribution statement"
- "Salary Increase, Compensation Modification, Insurance Revision, and Benefit Package Enhancement“

Absendernamen:

- "HR Benefit Scheme"
- "Management"

Beispiel:



Alle hier gezeigten Nachrichten wurden durch

eXpurgate der **eleven cyber security GmbH** erkannt.

Alternative Wege gehen…

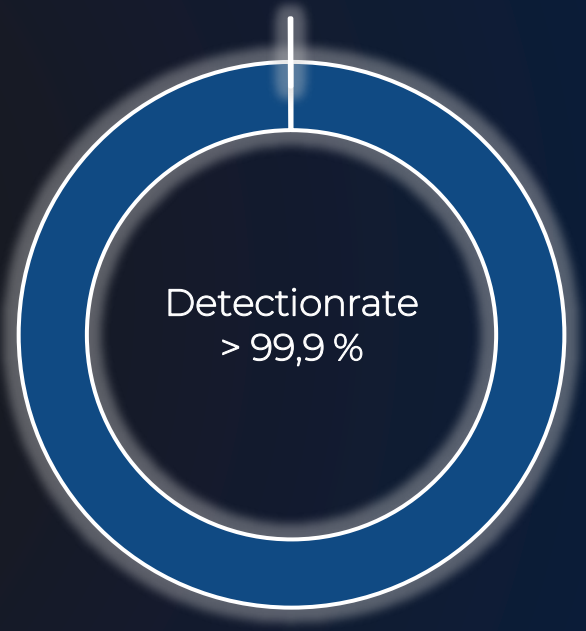
- Virus-Outbreak Detection
- FPL statt Blocklisten

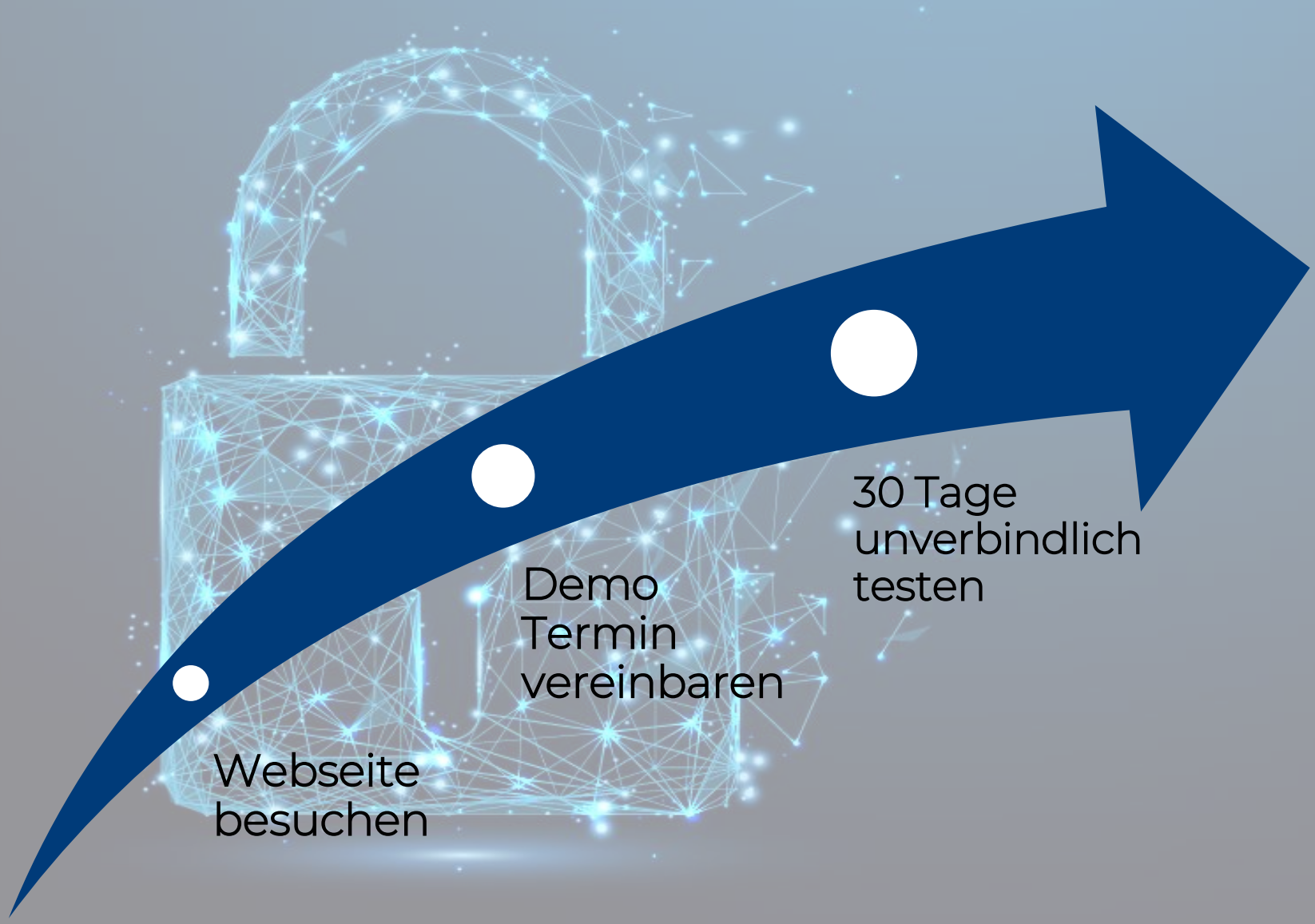
- Virus-Outbreak Detection
  - Erkennung von schädlichen Dateien anhand ihres Ausbreitungsverhaltens

    „Dateien, die schlagartig weltweit in unterschiedlichen Mailings auftauchen, sind entweder ein neues Virus, oder die neue Version von Morhuhn.“ ☺
- FPL statt Blocklisten
  - Die Absenderadresse ist kein gutes Merkmal, um Rückschlüsse auf den Inhalt einer E-Mail zu ziehen.
  - Bei Hochlast temporär nur E-Mails von Business-relevanten Servern annehmen

Warum eXpurgate?

- Erhältlich als Cloud Service, oder in diversen Ausprägungen als On-Premise Installation
- Schutz vor Advanced Threats (ATP):
  - Business-E-Mail Compromise, Ransomware, Scam, Phishings …
  - Real-Time Virus-Outbreak Detection
- 100% made & operated in Germany
  - Garantierte Verfügbarkeit: >99,9%
  - Keine einzige Downtime in ü 20 Jahren!
- Hohe Detectionrate und geringe FP-Rate
  - Erkennungsrate von 99,9%
  - FP-Rate: <0,00005%
- Expertise aus dem OEM-Bereich
- Channel Business & direkter Support aus Berlin





SCAN ME

eleven

Vielen Dank für deine Aufmerksamkeit!

Kontakt: Agnes Porombka

Partnermanagement

Tel.: +49 30 52 00 56 204

E-Mail: partner@eleven.de

eleven