

REFERENZ · PRODUZIERENDES GEWERBE

Rechnungsbetrug per E-Mail: monatelang mitgelesen, an einem Arbeitstag rekonstruiert

Bei einem Reifenhersteller mit eigener IT-Abteilung landeten rund 50.000 Euro aus mehreren Rechnungen auf einem Konto im Ausland. Ohne bestehenden Vertrag haben wir den Weg des Angreifers an einem Arbeitstag rekonstruiert und am Folgetag Bericht und Maßnahmenplan übergeben.

Eckdaten

Branche	Reifenhersteller
Größe	mehr als 100 IT-Arbeitsplätze, eigene IT-Abteilung
Betroffene Zahlungen	mehrere Rechnungen, zusammen rund 50.000 Euro
Vertrag mit uns vorher	keiner
Vor Ort	innerhalb von 24 Stunden
Erstes Lagebild	innerhalb einer Stunde
Rekonstruktion	an einem Arbeitstag
Bericht mit Maßnahmenplan	am folgenden Tag
Unsere Rolle	Analyse → Rekonstruktion → Bericht und Maßnahmenplan; Umsetzung durch die interne IT

Ausgangslage: Eine Mahnung, die ins Leere ging

Aufgefallen ist der Angriff nicht in der IT, sondern in der Buchhaltung. Das Unternehmen mahnte einen Kunden wegen offener Rechnungen. Der Kunde erklärte, er habe längst bezahlt. Das stimmte: Das Geld war überwiesen worden, aber auf ein Konto im Ausland. Betroffen waren mehrere Rechnungen, zusammen rund 50.000 Euro.

Das Unternehmen stellt Reifen her, hat mehr als 100 IT-Arbeitsplätze und eine eigene IT-Abteilung. Einen Vertrag mit uns gab es nicht. Der erste Kontakt kam per Telefon, nach dem Angriff. Die interne Einschätzung lautete: Die Angreifer sind nicht mehr im System.

Unsere Antwort am Telefon: Das lässt sich so nicht ausschließen. Solange niemand belegt hat, wie der Angreifer hereingekommen ist, muss man davon ausgehen, dass er weiterhin Zugang hat

und mitliest. Wir haben empfohlen, sofort einzugreifen. Das Unternehmen hielt die Lage nicht mehr für akut und legte den Termin selbst fest; innerhalb von 24 Stunden waren wir vor Ort.

Die erste Stunde: ein Lagebild

Bevor irgendetwas geändert wird, muss klar sein, womit man es zu tun hat. Das erste Lagebild stand nach einer Stunde.

Was steht wo: Welche Systeme laufen im eigenen Haus, welche extern oder in der Cloud, welches E-Mail-System ist im Einsatz – und wer hat worauf Zugriff.

Wie der Angriff bemerkt wurde: Die wichtigste Frage. Hier war es keine Warnmeldung, sondern die Mahnung an einen Kunden. Kein technisches System hatte angeschlagen.

Die Arbeitsannahme: Bis zum Beweis des Gegenteils hat der Angreifer weiterhin Zugang – auch während wir am Tisch sitzen. Danach richtet sich, was in welcher Reihenfolge geprüft wird.

Der erste Tag: die Rekonstruktion

Am Ende des ersten Arbeitstages war der Weg des Angreifers nachgezeichnet, so weit die vorhandenen Spuren reichten.

Eine Doppelgänger-Domain: Der Angreifer hatte eine Domain registriert, die der echten Domain des Unternehmens zum Verwechseln ähnlich war. Wer nicht Zeichen für Zeichen liest, sieht keinen Unterschied.

Weiterleitungsregeln in Postfächern: In Postfächern des Unternehmens leiteten Regeln Nachrichten an den Angreifer weiter. So war er über Monate in die E-Mail-Kommunikation eingeschaltet.

Echte Namen, falsche Adressen: Er nutzte die echten Namen der Beteiligten als Anzeigenamen, ersetzte die Empfängeradressen durch Adressen seiner Doppelgänger-Domain, veränderte Nachrichten und schickte sie an die eigentlichen Empfänger weiter. Für beide Seiten sah die Korrespondenz gewöhnlich aus.

Erst beobachten, dann zuschlagen: Über Monate konnte er Schreibstil, Ansprechpartner, Abläufe und den Rhythmus der Rechnungen studieren. Erst als er genug wusste, schlug er mit geänderten Bankdaten zu.

Ein blinder Fleck: Weiterleitungsregeln waren bei den bisherigen Prüfungen nicht als Angriffsweg in Betracht gezogen worden.

Ein früherer Vorfall: Der Zugang muss Monate vorher entstanden sein. Die Analyse ergab Hinweise auf einen früheren Vorfall, der die Geschäftsführung nie erreicht hatte.

Der wahrscheinliche Ausgangspunkt: Nach den gewonnenen Erkenntnissen eine Firewall, die seit rund einem Jahr keine Herstellerunterstützung mehr hatte – also keine Sicherheitsupdates für bekannte Schwachstellen – und trotzdem weiter im Einsatz war.

Warum die Spur dort endet: Die Firewall speicherte lokal nur die letzten 10.000 Einträge, ein externes Protokollsystem gab es nicht. Im gewöhnlichen Betrieb ist ein solcher Speicher innerhalb weniger Tage überschrieben. Eine Rückverfolgung über Monate war damit nicht möglich.

Der zweite Tag: Bericht und Maßnahmenplan

Am folgenden Tag haben wir den schriftlichen Bericht mit Maßnahmenplan übergeben.

Bericht: Was festgestellt ist, was nur durch Indizien gestützt wird und was offen bleibt – getrennt aufgeschrieben, damit die Geschäftsführung weiß, worauf sie bauen kann.

Maßnahmenplan: Die Maßnahmen nach Dringlichkeit geordnet, so dass die interne IT in dieser Reihenfolge vorgehen kann.

Abgestimmt mit G DATA: Den Maßnahmenkatalog haben wir vorab mit G DATA CyberDefense abgestimmt. Ergebnis: Nach vollständiger Umsetzung und nachweislich sauberem Ausgangszustand wäre der Einsatz von G DATA Managed XDR möglich. Erst bereinigen, dann überwachen – Angriffserkennung setzt man nicht auf kompromittierte Systeme.

Umsetzung durch die interne IT: Die Umsetzung lag beim Unternehmen und seiner IT-Abteilung. Bei Unternehmen mit eigener IT ist das eine bewusste Aufteilung: Wir analysieren, berichten und priorisieren, die IT setzt um. Auf Wunsch übernehmen oder begleiten wir die Umsetzung.

Was belegt ist – und was nicht

Ohne historische Protokolle lässt sich nicht jede Aussage gleich sicher treffen. Deshalb unterscheiden wir, wie belastbar sie ist.

Unmittelbar festgestellt: Eine der echten Domain zum Verwechseln ähnliche Domain war registriert und wurde für die Kommunikation genutzt.

Unmittelbar festgestellt: In Postfächern des Unternehmens bestanden Weiterleitungsregeln, über die Nachrichten an den Angreifer gingen.

Unmittelbar festgestellt: Mehrere Zahlungen, zusammen rund 50.000 Euro, gingen auf ein Konto im Ausland.

Unmittelbar festgestellt: Die Firewall hatte seit rund einem Jahr keine Herstellerunterstützung, speicherte lokal nur die letzten 10.000 Einträge, und ein externes Protokollsystem gab es nicht.

Durch Indizien gestützt: Der Zugang entstand Monate vor den umgeleiteten Zahlungen; es gab einen früheren Vorfall, der die Geschäftsführung nicht erreichte.

Durch Indizien gestützt: Ausgangspunkt war die Firewall ohne Herstellerunterstützung. Lückenlos belegen lässt sich das nicht: Die Protokolle aus der fraglichen Zeit existierten nicht mehr.

Fachliche Bewertung: Ein fortbestehender Zugang des Angreifers ließ sich zum Zeitpunkt der Analyse nicht ausschließen.

Allgemeine Empfehlung: Protokolle mindestens zwölf Monate zentral, manipulationsgeschützt und außerhalb der Firewall aufbewahren. Das ist unsere Empfehlung aus der Praxis, keine gesetzliche Frist.

Allgemeine Empfehlung: Geänderte Bankdaten nie per E-Mail bestätigen, sondern über eine bekannte Telefonnummer zurückrufen – auf beiden Seiten.

Die Kette: sieben Glieder, sieben Stellen zum Unterbrechen

Es war nicht ein einzelner Fehler, sondern eine Verkettung. An jedem Glied hätte eine Maßnahme den Angriff aufhalten können.

1. **Firewall ohne Herstellerunterstützung** – unterbrochen hätte es: Lebenszyklus der Sicherheitstechnik überwachen und rechtzeitig ersetzen
2. **Unbemerktter Erstzugang** – unterbrochen hätte es: Anmeldungen und Zugriffe überwachen, Auffälligkeiten melden lassen
3. **Kein externes Protokollsystem** – unterbrochen hätte es: Protokolle zentral und manipulationsgeschützt aufbewahren, nach unserer Empfehlung mindestens zwölf Monate
4. **Weiterleitungsregeln nicht überwacht** – unterbrochen hätte es: Weiterleitung nach außen sperren, neue Postfachregeln melden lassen
5. **Kein Schutz gegen Doppelgänger-Domains** – unterbrochen hätte es: Ähnliche Domains beobachten oder vorsorglich selbst registrieren
6. **Keine Rückrufpflicht beim Zahlenden** – unterbrochen hätte es: Geänderte Bankdaten nur nach Rückruf über eine bekannte Nummer übernehmen
7. **Früherer Vorfall erreicht die Geschäftsführung nicht** – unterbrochen hätte es: Fester Meldeweg: Jeder Verdacht geht ohne Umweg zur Geschäftsführung

Kein Vorwurf an die IT-Abteilung

Die IT-Abteilung des Unternehmens bestand aus erfahrenen, guten Technikern, teils mit Jahrzehnten Berufserfahrung. Das Problem war nicht die Erfahrung, sondern die Art der Aufgabe.

Interne IT-Abteilungen sind dafür da, den Betrieb aufrechtzuerhalten: Server verwalten, Arbeitsplätze betreuen, Störungen beheben. Ein Angriff ist das Gegenteil davon. Jemand arbeitet gezielt daran, diesen Betrieb zu unterwandern und auszunutzen. Das ist kein Tagesgeschäft, und es ist keine Schande, dafür Unterstützung zu holen. Im Ernstfall braucht jede IT-Abteilung Hilfe von außen, auch die beste.

Dazu kommt ein schlichter Umstand: Eine Geschäftsführung kann technische Aussagen ihrer IT oft nicht selbst prüfen. Eine unabhängige Zweitmeinung schafft Klarheit, ohne jemanden bloßzustellen.

Sicherheitsvorfälle sind Chefsache

Der frühere Vorfall hatte die Geschäftsführung nie erreicht. Daraus folgt keine Schuldfrage, sondern eine Regel für den Meldeweg: Jeder Verdacht gehört ohne Umweg zur Geschäftsführung, auch wenn er sich später als harmlos herausstellt.

Für Unternehmen, die unter NIS2 fallen, nimmt § 38 BSI die Geschäftsleitung ausdrücklich in die Pflicht. Unabhängig davon gehört der Meldeweg in die Verfahrensdokumentation und das interne Kontrollsystem: wer meldet, an wen, wie schnell.

Ergebnis: Klarheit am zweiten Tag

Nach einem Arbeitstag war nachgezeichnet, wie der Angreifer vorgegangen war. Am folgenden Tag lagen Bericht und Maßnahmenplan vor, abgestimmt mit G DATA.

Der Bericht trennt, was festgestellt ist, was nur Indizien stützen und was offen bleibt. Beim mutmaßlichen Erstzugang ist das entscheidend: Ohne historische Protokolle lässt er sich nicht lückenlos belegen, und das steht auch so im Bericht.

Was andere daraus lernen können

- **„Die Angreifer sind raus“ ist eine Annahme** Ohne Beleg gilt das Gegenteil. Was nach Ihrem Anruf in welcher Reihenfolge geschieht.
- **Geänderte Bankverbindung: immer zurückrufen** Woran Zahlende eine umgeleitete Rechnung erkennen und welche Regel davor schützt.
- **Die eigene Domain absichern** SPF, DKIM und DMARC schützen vor gefälschten Absendern Ihrer Domain – nicht vor Doppelgänger-Domains. Was Ihre Domain heute festlegt.
- **Firewall-Lebenszyklus im Blick** Was eine Firewall ohne Herstellerunterstützung bedeutet und wann sie ersetzt werden sollte.
- **Meldewege festlegen** Wie Meldeweg und Zuständigkeiten in Verfahrensdokumentation und internem Kontrollsystem stehen.

Für IT-Verantwortliche: der Fall technisch

- **Angriffstyp: Business E-Mail Compromise (BEC)** – Eingriff in die geschäftliche E-Mail-Kommunikation mit dem Ziel, Zahlungen umzuleiten –, kombiniert mit einer Doppelgänger-Domain (Typosquatting). Umgangssprachlich oft „Man-in-the-Middle“ genannt; technisch genauer: ein Angreifer in der E-Mail-Kommunikation, nicht im Netzwerk.
- **Abgrenzung:** Beim CEO-Fraud gibt sich jemand als Geschäftsführung aus. Hier hat sich der Angreifer in echte Geschäftsvorgänge eingeschaltet.
- **Mechanismus:** Weiterleitungsregeln in Postfächern; Nachrichten mit echtem Anzeigenamen und ersetzter Empfängeradresse; Inhalte verändert und weitergeleitet.
- **Erkennungslücke:** Postfachregeln waren kein Prüfpunkt. In Microsoft 365 gehören die Prüfung der Regeln (auch versteckter), eine Sperre automatischer Weiterleitung nach außen und eine Meldung bei neuen Regeln zur Grundausstattung.

- Protokollierung: Firewall lokal 10.000 Einträge, kein Syslog- oder SIEM-System; Rückverfolgung über Monate unmöglich. Das BSI behandelt zentrale Protokollierung und Archivierung im IT-Grundschutz-Baustein OPS.1.1.5. Die Frist von mindestens zwölf Monaten ist unsere Empfehlung; Zweck, Zugriff und Löschung gehören datenschutzkonform geregelt.
- SPF, DKIM und DMARC: Sie verhindern, dass jemand die eigene Domain als Absender fälscht. Gegen Nachrichten von einer fremden, ähnlich aussehenden Domain und aus einem übernommenen echten Postfach helfen sie nicht.
- Reihenfolge: erst bereinigen, dann überwachen. Angriffserkennung auf kompromittierten Systemen meldet im besten Fall den Ist-Zustand.
- Bewusst nicht genannt: Hersteller und Modell der Firewall, E-Mail-System und Version, Domainmuster, Bank und Zielland.

Projektwerte: Alle Zahlen stammen aus diesem einen Projekt und sind kein allgemeines Leistungsversprechen. Der Kunde bleibt aus Vertraulichkeitsgründen ungenannt. Online mit allen Verweisen: davinci-rechenzentrum.de/referenzen/rechnungsbetrug-reifenhersteller

Ihr Ansprechpartner: **Metehan Kurt**, Geschäftsführer

0621 877 55 990 · post@davinci-rechenzentrum.de