



Wenn eine Phishing-Mail täuschend echt aussieht

KUNDENINFORMATION

Unser Kunde zählt zu den führenden Bau- und Infrastrukturunternehmen Europas und ist mit zahlreichen Niederlassungen und Baustellen deutschlandweit vertreten. Das Unternehmen realisiert anspruchsvolle Projekte im Hoch-, Tief- und Ingenieurbau.

Viele Standorte und mobile Arbeitsplätze stellen dabei besondere Anforderungen an die IT-Ausstattung und IT-Security.

HINWEIS

Auf Wunsch des Kunden verzichten wir auf eine öffentliche Nennung.

BRANCHE

Bau- und Infrastruktur

MITARBEITERANZAHL

ca. 250 Mitarbeitende

MR-ANSPRECHPARTNER

Lars Zadeh
L.Zadeh@mr-daten.de

AUSGANGSSITUATION

Phishing-Mails werden immer professioneller – und sind längst nicht mehr auf den ersten Blick als solche zu erkennen. Genau das wurde einem langjährigen Kunden der MR Datentechnik zum Verhängnis.

Eine Mitarbeiterin bzw. ein Mitarbeiter aus der Buchhaltung erhielt eine E-Mail, die vermeintlich von einer deutschen Behörde stammte. Aufmachung, Inhalte und Anhänge wirkten authentisch und ließen zunächst keinen Verdacht aufkommen.

Im weiteren Verlauf wurde die Person aufgefordert, persönliche Zugangsdaten einschließlich des Passworts einzugeben. Erst als zusätzlich Token-Informationen abgefragt wurden, kamen Zweifel auf. Daraufhin wurde die interne IT umgehend informiert, die sich dann an die Experten der MR Datentechnik wandte.

LÖSUNG

Unsere Spezialisten nahmen den Vorfall unmittelbar unter die Lupe. Bei einer ersten Prüfung waren keine Anzeichen für einen erfolgreichen Angriff auf die Systeme zu erkennen.

Doch gerade weil ein Account aus der Buchhaltung betroffen war und Zugangsdaten bereits eingegeben worden waren, reichte eine erste Einschätzung nicht aus. Wir wollten unserem Kunden Gewissheit bieten, ob tatsächlich kein Zugriff auf die Systeme ausgeführt wurde oder ob bereits Aktivitäten im Hintergrund erfolgten.

Der Vorfall sollte deshalb bis ins Detail untersucht werden.

UMSETZUNG

Für die tiefergehende Analyse arbeiteten unsere Security-Spezialisten mit den whitelishackers zusammen. Der Fall erhielt sofort höchste Priorität.

Innerhalb einer Stunde saßen MR Datentechnik, whitelishackers und der Kunde gemeinsam im ersten Abstimmungstermin. Die Situation wurde analysiert. Anhand der vorhandenen Fakten wurden daraufhin die nächsten Maßnahmen festgelegt.

Nach der Bereitstellung der notwendigen Informationen durch den Kunden und die MR Datentechnik starteten die Security-Experten unmittelbar mit der detaillierten Untersuchung.

Erste Ergebnisse innerhalb weniger Stunden

Bereits innerhalb eines halben Tages erhielt der Kunde eine erste ausführliche Analyse. Dabei wurde gezielt geprüft, ob es Hinweise auf einen erfolgreichen Angriff, verdächtige Aktivitäten oder eine weitergehende Kompromittierung der Systeme gab.

Damit bekam der Kunde nicht nur eine schnelle Einschätzung, sondern vor allem die notwendige Sicherheit, den Vorfall fundiert bewerten und die nächsten Schritte gezielt einleiten zu können.

Im Ernstfall zählt jede Stunde

Der Vorfall zeigt, wie professionell Phishing-Angriffe mittlerweile aufgebaut sein können. Selbst vermeintlich vertraute Absender, authentisch wirkende Inhalte und bekannte Dokumente sind keine Garantie dafür, dass eine

E-Mail tatsächlich aus der angegebenen Quelle stammt.

Entscheidend ist deshalb, was passiert, wenn der Verdacht auf einen Sicherheitsvorfall besteht: **schnell reagieren, die richtigen Spezialisten einbinden und mögliche Spuren konsequent untersuchen.**

Durch das Zusammenspiel der internen IT des Kunden, der MR Datentechnik und whitelishackers konnte innerhalb kürzester Zeit reagiert und eine fundierte Analyse durchgeführt werden. In diesem Fall ist alles gut ausgegangen und es gab schnell Entwarnung.

PARTNER

