Netzwerk Südbaden

Das regionale Wirtschaftsmagazin

WAS IST RESPEKT? ÜBER DAS ICH UND DIE ANDEREN ● BETRIEBSKLIMA: DAMIT ALLE GERN ZUR ARBEIT KOMMEN ● EHRENAMT: ARBEITEN OHNE BEZAHLUNG ● ALEMANNENSCHULE: WO DER LEHRER COACH IST ● HUT AB: QUEREINSTEIGER IN EINEM ALTEN HANDWERK ● MANUFAKTUR: AM ANFANG WAR DAS SALATDRESSING ● RHEINFELDEN: STADT DER BRÜCKEN ● AUSSTELLUNG: ALTDEUTSCHE MEISTER IN COLMAR ● LARS FELD ÜBER ASTERIX

9 770262 777279 06

#06/2024
E2014
6,50 Euro

Achtung!

Schwerpunkt Respekt

Die Gefahr schlummert im eigenen Postfach

Ein potenzieller Cyberangriff startet oft unscheinbar. Umso wichtiger ist es, wachsam zu sein, denn eine kleine Unachtsamkeit kann große Konsequenzen haben – wie das nachfolgende Beispiel des Unternehmens Muster & Söhne zeigt.

Julian Sayer ist Vorstand für Vertrieb, Marketing und Entwicklung der Continum AG. Das Freiburger Hostingunternehmen ist AWS-, Microsoft Azure sowie IONOS Partner und unterstützt Unternehmen auf dem sicheren Weg in die Cloud.

Das mittelständische Unternehmen Muster & Söhne ist ein erfolgreiches Familienunternehmen, das feinmechanische Werkzeuge herstellt. Die Firma, bekannt für ihre Präzisionsarbeit, wird von Hans Muster und seinem Sohn Thomas geführt.

Thomas verantwortet in der Geschäftsführung unter anderem den Bereich Marketing und Vertrieb und ist immer auf der Suche nach neuen interessanten Geschäftskontakten. Eines Morgens erhält Thomas eine E-Mail von einem vermeintlichen neuen Geschäftspartner, der sich als Einkäufer eines großen Maschinenbauunternehmens vorstellt. Die Nachricht klingt vielversprechend: „Sehr geehrter Herr Muster, wir sind beeindruckt von Ihren Produkten und würden gerne eine umfangreiche Bestellung aufgeben. Unsere Bestellung können Sie über den nachfolgenden Link einsehen." Soweit alles normal. Neugierig klickt Thomas auf den Link und gelangt auf die vertraute Seite der Bestellsoftware und gibt seine Login-Daten ein, um die Bestelldetails einzusehen.

Zeitgleich sitzt Hans in seinem Büro und erhält eine sehr ähnliche Anfrage von demselben Maschinenbauunternehmen. Da sein Sohn Thomas das Neukundengeschäft verantwortet, leitet Hans die E-Mail entsprechend weiter. Die E-Mail ist leicht abweichend formuliert. Zwei ähnliche Anfragen in so kurzer Zeit? Thomas wird misstrauisch, sein Bauchgefühl sagt ihm, dass da etwas faul ist, und informiert die IT-Abteilung.

Daraufhin untersuchen die IT-Experten von Muster & Söhne die E-Mails sowie die integrierten Links. Schnell stellen sie fest, die E-Mails sind fingiert – ein Phishing-Angriff! Die IT-Abteilung reagiert schnell und setzt alle Passwörter zurück, um den Zugriff der Angreifer zu verhindern. Außerdem informieren sie alle Mitarbeiter des Unternehmens und bitten sie, besonders kritisch auf verdächtige E-Mails zu achten. Gerade noch einmal gut gegangen!

Doch wie konnten die Angreifer an die notwendigen Informationen gelangen, um eine so realistische Anfrage und eine täuschend echte Website zu erstellen? Die IT-Experten klären Thomas und Hans auf, dass die Betrüger vermutlich sogenannte Social-Engineering-Techniken genutzt hatten, um an persönliche Informationen zu gelangen. Die Angreifer haben vermutlich über einen längeren Zeitraum die sozialen Netzwerke von Muster & Söhne durchsucht und persönliche Details gesammelt.

Die Erfahrung hinterlässt einen bleibenden Eindruck bei Muster & Söhne, auch wenn alle nochmal mit dem Schrecken davongekommen sind. Um das Risiko in Zukunft zu reduzieren, entscheidet Hans Muster, die Sicherheitsmaßnahmen zu verstärken und startet ein Unternehmensprojekt – dazu gehören regelmäßige IT-Sicherheitsschulungen, Integration weiterer technischer Cyber Security Lösungen sowie die Vorgabe eines klaren Verfahrens zum Umgang mit verdächtigen E-Mails.

Einige Wochen später erhält Hans Muster erneut eine E-Mail, diesmal von einem tatsächlichen Geschäftsinteressenten, der ebenfalls beeindruckt von ihren Produkten ist und eine größere Bestellung aufgeben möchte. Um sicherzugehen, dass die Anfrage auch tatsächlich von Ihrem Geschäftspartner kommt, kontaktiert er diesen kurz über die bereits bekannte Telefonnummer, bevor er ihm per E-Mail antwortet.

Obwohl diese Anfrage sich als echt herausgestellt hat, bleibt bei den beiden ein mulmiges Gefühl. Die jüngsten Phishing-Versuche hatten gezeigt, wie verwundbar das Unternehmen war und wie einfach es schiefgehen kann. Seit dem Vorfall fragt Thomas sich regelmäßig, wenn er den aktuellen IT-Sicherheitsbericht durchgeht, ob die neuen Maßnahmen ausreichen. Ist Muster & Söhne in der Lage, zukünftige Angriffe abzuwehren? Haben sie wirklich alle Schwachstellen geschlossen?

Die digitale Welt bleibt ein ständiges Katz-und-Maus-Spiel, bei dem nur kontinuierliche Prävention wirkt. Nur die Zeit wird zeigen, ob ihre Anstrengungen ausreichen, um den nächsten Angriff abzuwehren. Thomas und Hans Muster haben durch den Vorfall auf jeden Fall gemerkt, wie wichtig es ist, stets wachsam zu sein, E-Mails kritisch zu prüfen und die Sicherheitsmaßnahmen kontinuierlich weiterzuentwickeln.

Foto: PR