Elektronische Erpressung mit Bewerbungen

Der Feind in meinem Netz

Gutes Personal ist knapp. Daher freuen sich Unternehmen über ansprechende Bewerbungen für freie Ausbildungsstellen und Arbeitsplätze. Diese Freude ist aber schnell vorüber, wenn sich die Bewerbung als IT-Angriff mit einer Verschlüsselungssoftware entpuppt.

Im digitalen Zeitalter gehört auch die Onlinebewerbung zu den Standards in der Personalabteilung. Weniger Papier muss verbraucht werden, Portokosten entfallen. Gleichzeitig steigt aber unter Umständen auch die Gefahr eines Angriffs auf die Daten der Unternehmen. In der Vergangenheit sind häufiger sog. Ransomwareangriffe erfolgt. Dabei werden die Unternehmensdaten zunächst verschlüsselt und anschließend Geld verlangt, um sie zu entsperren. Ziel dieser Attacke sind nicht nur Großunternehmen. Auch kleine und mittelständische Unternehmen geraten immer häufiger ins Visier der Cyberkriminellen.

Ein mittelständisches Beratungs- und Dienstleistungsunternehmen* aus Mülheim an der Ruhr zum Beispiel bot einen neuen Ausbildungsplatz an. Die Bewerbungen sollten vorrangig elektronisch eingereicht werden; dazu wurde extra eine entsprechende Mailadresse eingerichtet. Unter den Einsendungen war dann auch eine als Bewerbung getarnte Mail mit Schadsoftware.

Die Zeiten, in denen man virenverseuchte Mails an kryptischen Mailadressen, Tippfehlern und frei gestaltetem Satzbau erkennen konnte, sind vorbei. „Die Absenderadresse war vollkommen unauffällig, in der Mail selbst war ein kurzer, fehlerfreier Text, der auf die Bewerbung und den Lebenslauf im Anhang hinwies“, erinnert sich Tanja Schmidt von dem Unternehmen. Die im pdf-Format beigefügte Bewerbung wirkte durchaus positiv. „Die Anrede war persönlich, die Bewerbung bezog sich auf die ausgeschriebene Stelle, ein ansprechend sympathisches Foto war dabei – zunächst haben wir keine Auffälligkeit gesehen“, so Schmidt. Da bis dahin alles in Ordnung schien, öffnete sie den Lebenslauf, der als Exceldatei angehängt war. Zunächst zeigte sich eine leere Datei. Daher klickte sie auf das Feld „Bearbeitung aktivieren“, in der Erwartung, dann den Lebenslauf zu sehen.

Mit dem Klick nahm jedoch die Schadsoftware ihre Arbeit auf und begann die Dateien auf Schmidts Rechner zu verschlüsseln. Glück im Unglück: „Wir sind im Vorfeld regelmäßig geschult worden, was in solchen Fällen zu tun ist.“ Sie reagierte schnell und schaltete sofort den Rechner aus. Der Schaden konnte so noch relativ gering gehalten werden; andere Arbeitsplätze wurden nicht befallen. Wenige Zeit später trudelte noch erwartungsgemäß eine E-Mail ein. Darin wurde Geld gefordert, um alle Dateien wieder zu entsperren. Da die betriebseigene IT sich bereits um den befallenen Rechner gekümmert hatte, wurde sie ungelesen gelöscht.

Es hätte durchaus schlimmer kommen können. Von Vorteil war, dass der richtige Umgang mit so einem Notfall bekannt und geprobt war. Schnelles Handeln kann in solchen Fällen vor zu großen Kosten schützen. Es zeigt aber auch: Schadsoftware wird immer professioneller. Neben einer aktuellen technischen Infrastruktur kommt es immer stärker auf das Bewusstsein der Mitarbeiter an – und ihr Handeln. Dies sollte wie bei diesem Unternehmen regelmäßig geschult sein.

Aber auch technisch können sich Unternehmen wappnen: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt beispielweise, regelmäßig Updates der eigenen Software und Systeme vorzunehmen, um Sicherheitslücken zu schließen. Makros sollten nicht automatisch gestartet werden. Des Weiteren bietet es sich an, ein Datensicherungskonzept vorzuhalten. Dies kann davor schützen, dass im Fall eines Ransomwareangriffs alle Daten endgültig verloren gehen. Die wichtigste Schutzmaßnahme bleibt jedoch sicherlich die Sensibilität der Mitarbeiter.

Vollkommene Sicherheit wird es nicht geben. Vielmehr kommt es darauf an, das Risiko soweit es geht zu minimieren und die Einfallstore klein zu halten – und im Schadensfall auf einen Notfallplan zurückgreifen zu können. Zugleich empfiehlt es sich, die Behörden einzuschalten. Denn nur wenn ein Täter ermittelt wird, kann er aus dem Verkehr gezogen werden. Und, ganz wichtig: Nicht auf die Geldforderung der Cyberkriminellen eingehen. Denn zum einen gibt es keine Gewähr, dass die Verschlüsselung zurückgenommen wird. Zum anderen würden die Täter eine Zahlungsbereitschaft erkennen, die sie ggfs. weiter ausreizen würden.

Ist das Unternehmen ein Einzelfall? Nein, vergleichbare Vorfälle berichteten ebenfalls ein mittelständischer Schuhfachhandel, ein Callcenter oder auch ein Träger von Betriebskindergärten. Die Vorgehensweise war dabei stets gleich. Für das Mülheimer Beratungsunternehmen ist es daher wichtig, auch andere Betriebe zu sensibilisieren. Schließlich kann jeder ins Visier der Cyberkriminellen rücken.

Workshop „Digitaler Dienstag"

IT-Sicherheit und Datenschutz stehen auch im Fokus des nächsten Workshops der Reihe „Digitaler Dienstag". Am 6. Juni 2017 geht es um das Spannungsfeld zwischen den rechtlichen Anforderungen und der wirtschaftlichen Umsetzung eines IT-Sicherheitsmanagements. Der Impuls kommt von Uwe Rydzek, ITZ Informationstechnologie GmbH aus Essen. Die Teilnehmerzahl ist auf 12 begrenzt. Weitere Informationen und die Anmeldung gibt es im Netz unter **www.essen.ihk24.de**, Nummer für das Suchfeld: **12296729**

Verzichtet das Unternehmen deswegen von nun auf elektronische Bewerbungen? „Nein", erklärt Tanja Schmidt. „Wir bevorzugen weiterhin Onlinebewerbungen. Den Kopf in den Sand zu stecken und die Vorteile der digitalen Prozesse zu verzichten, kann nicht die Antwort auf solche Vorfälle sein", erklärt sie. Vielmehr wurden die IT-Sicherheitsmaßnahmen noch einmal analysiert und angepasst. Neu eingegangene Bewerbungen werden weiterhin bearbeitet – immer mit einem wachen Auge. Und im Zweifel werden die IT-Kollegen zu Rate gezogen. ■ *Jan Borkenstein*

* Der Firmenname wird auf Wunsch des Unternehmens nicht genannt; der Name der Ansprechpartnerin wurde ebenfalls geändert.