IT-Sicherheit

Bewerbung oder Attacke?

[07.06.2017] Eine von rund 100 an eine öffentliche Institution geschickten E-Mails enthält Schad-Software. Ein unerwartetes Einfallstor für solche Cyber-Attacken sind vermeintliche Bewerbungen. Schutz bieten hier Bewerbungsportale oder der Einsatz zertifizierter Software.

Der Cyber-Angriff mit der Erpressungssoftware WannaCry zeigt einmal mehr: Die Lage ist dramatisch. Laut dem aktuellen Report des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur Lage der IT-Sicherheit in Deutschland werden täglich rund 380.000 neue Schadprogrammvarianten gesichtet. Allein bis August 2016 waren insgesamt mehr als 560 Millionen verschiedene Schadprogrammvarianten bekannt. Laut dem Report gehören E-Mail-Anhänge sowie die von Anwendern unbemerkte Infektion des eigenen Systems durch den Besuch von Web-Seiten (Drive-by-Downloads) zu den häufigsten Infektionswegen eines Systems.
Ransomware, also Software, die Rechner vorwiegend über E-Mail-Anhänge befällt und die gesamten Daten einer Organisation verschlüsselt oder den Zugang sperrt, ist ein beliebter Weg für Cyber-Attacken. Erst wenn die Betroffenen infizierter Computer einen bestimmten Betrag bezahlt haben, wird der Zugang wieder freigegeben oder die Daten entschlüsselt. Im vergangenen Jahr war insbesondere Deutschland von einer massiven Welle von Ransomware-Infektionen betroffen. Ein bekanntes kommunales Opfer war Dettelbach. Die kleine unterfränkische Stadt bei Würzburg zahlte Lösegeld, um die durch die Schad-Software Tesla-Crypt verschlüsselten Rechner der Verwaltung wieder benutzbar zu machen.

Bewerbungen öffnen Zugang

Ein unerwartetes Einfallstor für solche Cyber-Attacken sind vermeintliche Bewerbungen. Maik Morgenstern, Technischer Leiter und einer der Geschäftsführer des Magdeburger IT-Security Instituts AV-Test, hat knapp 1,2 Millionen bösartige E-Mails mit Ransomware-Anhang untersucht. „Von diesen hatten 83 deutsche E-Mails laut Betreff einen Bezug zu Bewerbungen“, konstatiert Morgenstern. „Man kann also festhalten, dass Malware und zur Zeit insbesondere Ransomware über gefälschte Bewerbungsschreiben verteilt wird. Ob sich die Situation in Behörden deutlich unterscheidet, können wir anhand dieser Zahlen nicht ersehen. Denkbar ist aber, dass gerade öffentliche Einrichtungen zielgerichteter mit passenden Themen wie es Bewerbungen sein könnten, angegriffen werden.“
Dass insbesondere der öffentliche Sektor Ziel von Ransomware-Attacken ist, bestätigen die großen Antiviren-Software-Hersteller. Laut dem ISTR Government Report für Deutschland von Symantec enthält eine von 105 an eine öffentliche Institution geschickte E-Mail Schad-Software, mit der Kommunen oder öffentliche Einrichtungen attackiert werden.
Ebenso wichtig wie die Datensicherheit ist der Datenschutz. Bei Nichteinhaltung der einschlägigen Datenschutzbestimmungen des Bundesdatenschutzgesetzes (BDSG) oder der neuen EU-Datenschutzgrund-Verordnung (DGSVO, sie tritt ab Mai 2018 in Kraft) drohen hohe Strafen, die auch Kommunen treffen können. Laut Datenschutzberater Andreas Bethke sind öffentliche Organisationen zwar flächendeckend gut über die aktuelle Gesetzeslage und Sicherheitsmöglichkeiten informiert. In der Umsetzung hinken sie seiner Ansicht nach aber hinterher. „Insbesondere in der pragmatischen Umsetzung von Schutzmaßnahmen sehe ich momentan noch eine Herausforderung für öffentliche Einrichtungen. Mangelndes Know-how aus der Praxis verleitet zu einer Leichtgläubigkeit in die Technik. Aber genau das führt – bezogen auf die Anforderungen an den Datenschutz – schnell in eine Sackgasse.“ Bethke empfiehlt

den Betroffenen, sich schnellstmöglich mit dem Thema auseinanderzusetzen.

Bewerberportal erhöht Sicherheit

Die Installation aufwendiger Schutzmechanismen und Anti-Schad-Software ist heute unerlässlich. Den Bewerbungsprozess aber können auch einfache Maßnahmen sicherer und nicht zuletzt effizienter gestalten. Eine Lösung kann beispielsweise der Einsatz einer Bewerberportal-Lösung sein. Sie erschwert aufgrund ihres Aufbaus Missbrauch und Angriffsversuche. Dazu trägt bei, dass die Bewerberdaten über strukturierte Bildschirmmasken eingegeben und angehängte Dokumente über unterschiedliche Routinen nach relevanten Schadanteilen geprüft werden, bevor sie ins System übernommen und geöffnet werden. Wer ganz sicher gehen will, kann seine Organisation zusätzlich über externe Dienstleister prüfen und auf die Einhaltung der einschlägigen Datenschutzbestimmungen zertifizieren lassen. Derlei Zertifizierungen und Audits führen nicht nur private Anbieter durch. Auch staatliche Organisationen wie das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) oder der Landesbeauftragte für Datenschutz und Informationsfreiheit in Mecklenburg-Vorpommern bieten entsprechende Untersuchungsverfahren an. Weitere Vorteile ergeben sich durch den Einsatz datenschutzzertifizierter Software. Nach ausführlichen Audits bieten die erwähnten Organisationen auch hierfür Zertifizierungen an. Beispielsweise hat der brandenburgische, auf kommunale Personal-Management-Software spezialisierte Anbieter GfOP sein Produkt KOMMBOSS als erste Personal-Management-Software überhaupt bereits vor mehreren Jahren vom ULD zertifizieren lassen. Der Vorteil für Anwender: Für die regelmäßige Re-Zertifizierung bereits zertifizierter Software muss der jeweilige Software-Anbieter sorgen.
Die Gefahr, dass Cyber-Kriminelle sich den Fachkräftemangel im öffentlichen Dienst zunutze machen, um im Huckepack von Bewerbungen in öffentliche Institutionen einzubrechen, wächst mit jedem Tag. Für Kommunen haben deshalb sowohl die Sicherheit, in unserem Beispiel des Bewerbungsprozesses, als auch der Schutz vor Missbrauch höchste Priorität. Einen vollständigen Schutz wird es zwar nie geben, aber durch entsprechende Sicherheitsmaßnahmen muss die Latte für Angreifer so hoch wie möglich gelegt werden. Das Risikopotenzial ist zu groß, als dass Kommunen auf derlei Maßnahmen verzichten könnten.

()

Dieser Beitrag ist in der Juni-Ausgabe von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Ransomware, Bewerber-Management