Cyber-Angriffe

Wie Kommunen sich schützen

[13.08.2020] Kommunen sind begehrte Ziele für Cyber-Angriffe. Kommune21 sprach mit Kriminaloberkommissar Andreas Arbogast vom Cybercrime Präventionsteam des LKA Nordrhein-Westfalen und Stefan Cink, E-Mail-Sicherheitsexperte beim Unternehmen Net at Work, über die Gründe und wie sich Verwaltungen schützen können.

Herr Arbogast, Herr Cink, warum stehen Kommunen und andere öffentliche Einrichtungen besonders im Fokus von Cyber-Angriffen?

Arbogast: Im Grunde gibt es zwei Wege, wie Cyber-Angriffe in bare Münze umgesetzt werden können: Lösegeld erpressen oder Zugang zu wertvollen Informationen schaffen. Aus Sicht von Cyber-Kriminellen sind Kommunen in beiden Fällen interessante Ziele. Wichtige kommunale Verwaltungen können nicht tage- oder gar wochenlang blockiert sein, deshalb vermuten Angreifer, hier schnell Lösegeld einstreichen zu können – auch wenn es in Deutschland klare Verwaltungsvorschriften gibt, nicht auf solche Forderungen einzugehen. Kommunen verwalten außerdem in großem Umfang vertrauliche Informationen, die auf dem Schwarzmarkt Käufer finden können. Darüber hinaus ist das Hacken bekannter Verwaltungen mit einer entsprechend hohen medialen Aufmerksamkeit verbunden, was in Hacker-Kreisen als Reputationsgewinn verbucht wird.

Sehen Sie aktuell eine Steigerung der Bedrohungslage?

Arbogast: Wir beobachten einen drastischen Anstieg an Angriffen auf öffentliche Einrichtungen. In der aktuellen Corona-Krise sind Verwaltungen besonders gefordert, schnell viele neue Online-Lösungen zu finden. Damit steigt die Angriffsfläche. Auch alle Kommunikationskanäle brummen – insbesondere der Kontakt per E-Mail. Viele Mitarbeiter finden sich auf einmal im Homeoffice wieder. Die IT-Abteilungen stehen deshalb unter hoher Dauerlast. Zudem sind durch die Corona-Situation Mitarbeiter und Bürger abgelenkt und weniger aufmerksam in Bezug auf Cybercrime. Die Human Firewall ist quasi etwas löchriger. Aus Sicht der Angreifer ist das ein guter Zeitpunkt für gezielte Attacken auf die Kommunalverwaltung.

Was waren Ihrer Erfahrung nach die konkreten Angriffsmuster bei erfolgreichen Fällen?

Arbogast: E-Mail, E-Mails und noch mal E-Mails. Nach wie vor ist Ransomware zur Lösegelderpressung sehr verbreitet. Sie sucht in immer neuen Formen ihren Weg per E-Mail in die Verwaltung. Über Emotet-Angriffe wird versucht, Schad-Software gezielt einzuschleusen, um besonders vertrauliche Daten abzugreifen.

#bild2
Cink: Wir beobachten außerdem, dass die Angriffe mit Phishing-Mails oder auch durch Social Engineering mittlerweile qualitativ so gut sind, dass es für die Nutzer immer schwerer wird, einen Fake auch als solchen zu erkennen. Allein auf die Awareness der Nutzer zu setzen, ist aus unserer Sicht fahrlässig. Hier müssen Unternehmen und Verwaltungen umdenken und viel stärker auf das Prinzip einer echten E-Mail-Firewall setzen. Dabei wird stringent festgelegt, welche Kommunikation man zulässt, alles andere wird kategorisch abgelehnt. Durch selbstlernende Verfahren funktioniert das auch ohne großen

Administrationsaufwand.

Arbogast: Das kann ich nur unterstützen. Rund 70 Prozent der Angriffe kommen echt oder gefaked über die Supply Chain, also vermeintlich bekannte Kommunikationspartner. Hier können Automatismen zur intensiven Prüfung der Senderreputation einen deutlichen Beitrag zum Schutz leisten.

„Wenn die große Mehrheit von Unternehmen, Verwaltungen und Bürgern verschlüsselte E-Mail-Kommunikation einsetzt, erreichen wir quasi Herdenimmunität.“
Warum tun sich Kommunen und andere öffentliche Einrichtungen teilweise schwer mit der E-Mail-Sicherheit?

Arbogast: Aus unserer Erfahrung ist die IT in öffentlichen Einrichtungen oft personell unterbesetzt. Zusammen mit dem Druck zur weiteren Digitalisierung ist die Last auf den IT-Abteilungen – auch schon vor der Corona-Krise – besonders hoch und man kann den Eindruck gewinnen, dass Sicherheitsaspekte dann nicht die Aufmerksamkeit bekommen, die sie eigentlich bräuchten.

Cink: Hinzu kommt, dass oft auch noch falsche Vorstellungen über den Einführungsaufwand vorherrschen. Nehmen wir als Beispiel die E-Mail-Verschlüsselung: Durch die Automatisierung der Zertifikatsverwaltung und der zentralen Einrichtung können wir heute die Verschlüsselung der Kommunikation selbst von tausenden Nutzern innerhalb weniger Tage umsetzen. Gleiches gilt für unsere modernen Anti-Spam- und Anti-Malware-Lösungen. Der Administrationsaufwand ist durch Automatisierung und selbstlernende Systeme nur gering und kann auf Wunsch als Managed Service komplett ausgelagert werden. Auch die Kosten sind überschaubar. Für den Gegenwert von drei Briefmarken kann ein Nutzer einen Monat lang sicher und verschlüsselt per E-Mail kommunizieren.

Wie verbreitet und wichtig ist die E-Mail-Verschlüsselung?

Cink: Ich will es einmal deutlich sagen: Es ist grob fahrlässig, wenn Verwaltungen nicht standardmäßig verschlüsselte E-Mail-Kommunikation nutzen – untereinander zwischen Verwaltungen, aber auch mit Bürgern und Unternehmen. Immer mehr Unternehmen und Bürger haben mittlerweile die Technik dafür eingeführt, und gute Mail-Security-Produkte bieten heute auch Methoden für eine verschlüsselte Kommunikation mit Teilnehmern, die selbst keine Verschlüsselungsinfrastruktur haben. Das gehört zum Grundschutz, den keine Kommune vernachlässigen darf.

Arbogast: Hier lässt sich ein schöner Vergleich zur aktuellen Lage ziehen: Wenn wir erreichen, dass die große Mehrheit an Unternehmen, Verwaltungen und Bürgern verschlüsselte und damit signierte E-Mail-Kommunikation einsetzt, dann erreichen wir quasi Herdenimmunität gegenüber Massen-Malware und Spam. Es lohnt sich dann schlichtweg für die Angreifer nicht mehr. Insofern ist Cyber-Sicherheit auch eine gesellschaftliche Aufgabe und die Verwaltung sollte hier mit gutem Beispiel vorangehen.

()

Stichwörter: IT-Sicherheit, Ransomware, Net at Work, Cyber-Sicherheit