Hüter des Datenschatzes

Die Sicherheit von IT-Systemen ist für Kommunen lebenswichtig – und eine große Herausforderung. Berater Stefan Spitz gehört zu einem Team der EnBW, das Städte und Gemeinden dabei unterstützt. Zum Auftakt unseres Gesprächs zeigt der 44-jährige Informatiker die Deckblätter mehrerer Regelwerke.

KommPlus: „IT-Grundschutzprofil", „Anforderungen für Landes- und Bundestagswahl", „Sicherheitsdokumentationen für die Rentenversicherung". Klingt nach viel Arbeit...
Spitz: Das empfinden IT-Verantwortliche in Kommunen ähnlich. In diesen vier Dokumenten stehen 600 Anforderungen, die Städte und Gemeinden in Sachen IT-Sicherheit erfüllen müssen. Es geht zum Beispiel um den Schutz und die Verfügbarkeit von Informationen, aber auch um die Abwehr von Cyberangriffen. Ziel ist, dass die kommunalen Verwaltungen ihre Aufgaben sicher und ohne Unterbrechung wahrnehmen können.

Wie verbindlich sind diese Vorgaben? Es sind Empfehlungen, die Organisationen, Verbände und das BSI, also das Bundesamt für die Sicherheit in der Informationstechnik, formuliert haben. Verwaltungen sind jedoch verpflichtet, ihre IT abzusichern. Diese Verpflichtungen stammen aus der EU-DSGVO und den Grundsätzen des rechtmäßigen Verwaltungshandelns. Die Empfehlungen zu ignorieren, könnte laut BSI als grob fahrlässig angesehen werden.

Und alle Kommunen erfüllen diese Anforderungen? Viele kennen die Anforderungen und die Bedeutung der IT-Sicherheit, doch häufig stehen zu wenige Ressourcen zur Verfügung, um sich sofort um alles zu kümmern. Ausgebildete IT-Fachkräfte zu finden, ist schwer. Daher konzentrieren sich Kommunen auf das, was mit der vorhandenen Mannschaft machbar ist.

Wie können Sie und Ihr Team die Kommunen unterstützen? Die Anforderungen haben wir in Module unterteilt und versuchen, diese in das Tagesgeschäft unserer Ansprechpartner in den Kommunen einzubinden. Wir unterstützen bei der Auswahl organisatorischer und technischer Maßnahmen wie dem Erstellen von Sicherheitskonzepten oder Notfallplänen.

Voriges Jahr verschlüsselten Kriminelle Daten des Landkreises Anhalt-Bitterfeld. Kann das auch anderen Kommunen passieren? Es geht nicht darum, ob, sondern wann eine Kommune Ziel eines Hacker-Angriffs wird. Deshalb muss es eine Verwaltung dem möglichen Eindringling so schwer wie möglich machen. Der potenzielle Schaden muss begrenzt oder am besten vermieden werden.

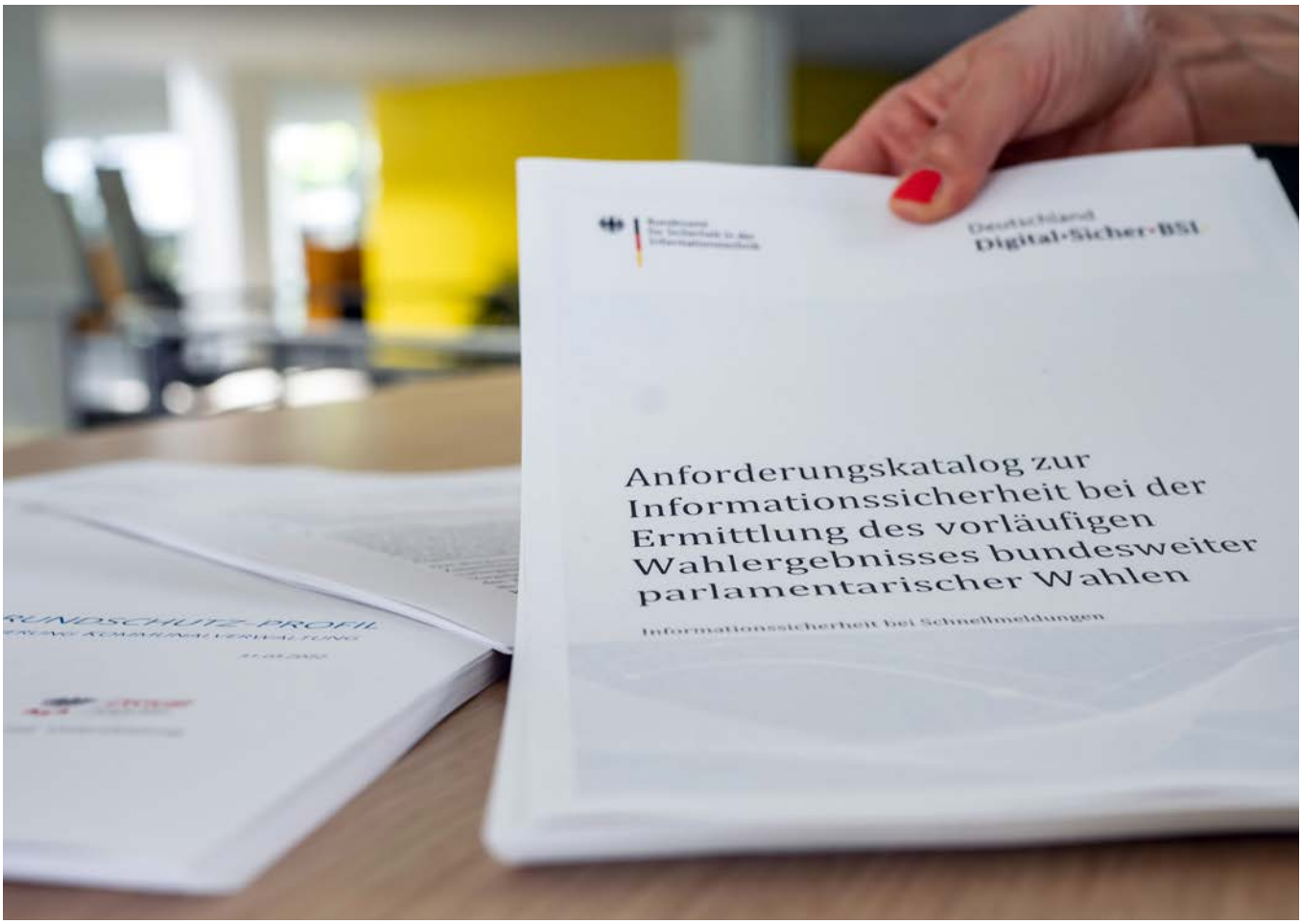
Was sind häufige Schwachstellen in der kommunalen IT? Dass Datensicherungen wichtig sind, ist den Kommunen bewusst. Verbesserungsbedarf gibt es etwa bei Fernwartungszugängen, über die externe Dienstleister Zugriff aufs System haben. Sie dürfen nur aktiviert werden, wenn ein Dienstleister tatsächlich arbeiten muss. Ansonsten müssen sie geschlossen bleiben.

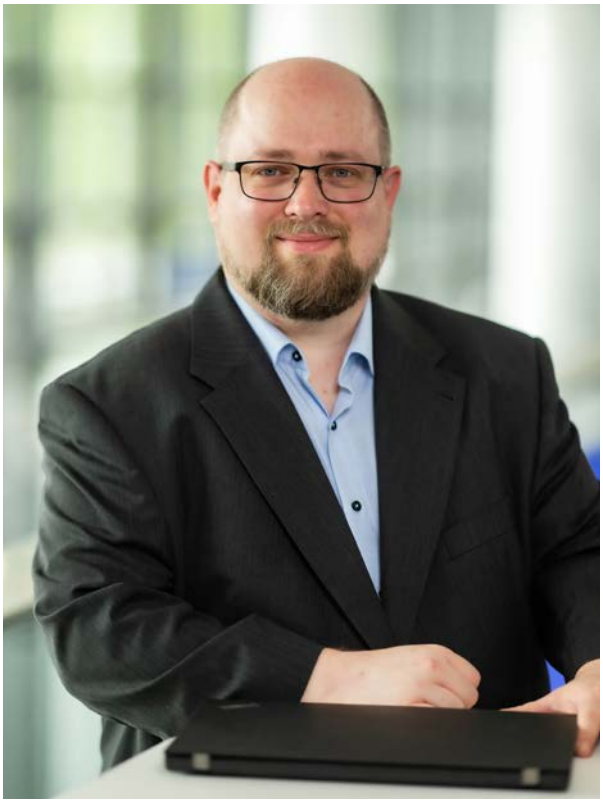
Wie gehen professionelle Hackergruppen vor? Sie bereiten Angriffe teils über Monate vor. Selbst wenn die IT heute eine Schwachstelle schließt, kann es sein, dass Hacker sie längst ausgenutzt haben. Hat ein Einbrecher durch die offene Veranda-tür den Zweitschlüssel geklaut, hilft es nichts, diese Hintertür auf Dauer zu verschließen. Der Einbrecher kann immer über die Haustür hereinkommen. Für Angriffe mit Erpressungssoftware sind übrigens Feiertage beliebt, weil IT-Fachleute nicht sofort reagieren können.

Wo haben Sie Ihre Qualifikationen erworben?
Ich habe an der Ruhr-Uni Bochum IT-Sicherheit studiert und dort promoviert. Die ersten Jahre war ich beim TÜV als Auditor im Bereich Informationssicherheit tätig. Danach wechselte ich zur EnBW und in die Beratung. Ein Kollege von mir bringt umfassende Erfahrung in der IT-Sicherheit mit. Er hat unter anderem das Kernkraftwerk Neckarwestheim vor Cyber-Angriffen geschützt.

Was motiviert Sie bei Ihrer Arbeit? Gibt es Ihnen einen Kick, besser zu sein als die Hacker? Wenn ich eine Kommune berate, ist es mein Ziel, sie besser gegen Angriffe zu schützen. Es geht nicht darum, stur Anforderungen abzuarbeiten, sondern gemeinsam passende Lösungen zu erarbeiten. Meine Motivation kommt aus der Begeisterung für das Thema und aus den vielen kleinen Erfolgen, die wir gemeinsam mit den Kommunen erzielen.

Vielen Dank für das Gespräch!





Viel zu tun: Stefan Spitz weiß, was Kommunen in Sachen IT-Sicherheit beachten müssen. Und er hilft ihnen dabei, die verschiedenen Anforderungskataloge umzusetzen,

151

Tage dauert es im Schnitt, bis Unternehmen Hackerangriffe bemerken.

Quelle: Cost of a Data Breach Report 2021, IBM Security