CYBERSPRINT
BREAKTHROUGH SECURITY

ANWENDUNGSFALL

PROVINZ OVERIJSSEL

provincie Overijssel

Für Regierungsorganisationen ist es wichtig, einen klaren Überblick über ihren digitalen Fußabdruck und ihre Risiken zu haben. Sie müssen sicherstellen, dass wirksame Richtlinien in Bezug auf die Cybersicherheit vorhanden sind. Um ihre Herausforderungen und die Vorteile der Verwaltung des digitalen Fußabdrucks zu veranschaulichen, haben wir einen unserer Kunden aus dem Regierungsbereich befragt. Rick Verkade, Spezialist für Sicherheit und Datenschutz der Provinz Overijssel, berichtet in diesem Interview über seine Erfahrungen.

Q **Rick, können Sie etwas über Ihre Rolle und die Organisationsstruktur der Provinz Overijssel erzählen?**

A „Natürlich. Den Herausforderungen der Cybersicherheit innerhalb der Organisation begegne ich ganz neu, da ich meine derzeitige Stelle erst vor einigen Monaten angetreten habe. Zuvor war ich im Bereich des Krisenmanagements tätig, wo ich eine Organisation auf Krisensituationen vorbereitet und das Management bei Zwischenfällen beraten habe. Bevor ich bei der Provinz dem Team Sicherheit und Datenschutz beitrat, erweiterte sich der Verantwortungsbereich der Abteilung. Das führte dazu, dass der CISO und der Datenschutzbeauftragte auch einige operative Aufgaben übernehmen mussten. Da diese beiden Positionen eher eine strategische Aufgabe erfüllen, entstand die Notwendigkeit meine aktuelle Stelle neu zu etablieren.

Die Provinz Overijssel fungiert sozusagen als Brücke zwischen der nationalen Regierung und den 25 kleineren Gemeinden innerhalb der Provinz. Sie kontrolliert weitestgehend die Richtlinien und Informationen, wie etwa die Infrastruktur und Umweltaspekte, aber auch Daten zu den 1,15 Mio. Einwohnern. Natürlich ist es wichtig, dass diese nicht angezapft werden oder durchsickern, unabhängig davon, ob die Daten sensibel sind oder nicht. Die Sicherheit und die Verwaltung der IT-Systeme sind meine Hauptaufgaben.“

Q **Was waren Ihre ersten Prioritäten und Herausforderungen?**

A „Zunächst musste ich zwei Dinge lernen: die Organisationsstruktur und -prozesse sowie die digitale Umgebung. Letzteres war das schwierigere Unterfangen, da dieses bereits vor meinem Berufsstart bei der Provinz eine

Herausforderung darstellte. Es waren der CISO und der Datenschutzbeauftragte, die mit der Abbildung unserer Online-Präsenz begonnen haben. Aufgrund knapper Ressourcen und ihrer verwaltungstechnischen Aufgaben, waren diese Bemühungen nur mäßig erfolgreich. So wurde mir diese Aufgabe allmählich übertragen. Auf diese Weise konnte ich Informationen zur Verfügung stellen, die für die Festlegung wirksamer Richtlinien benötigt wurden. Bevor man jedoch beginnen kann, über seine Sicherheitsniveaus zu berichten, muss man wissen, was man überhaupt sichern muss. Logischerweise sind Pläne und Richtlinien nützlicher, wenn sie auf der gesamten digitalen Infrastruktur basieren.

Q **Was machte die Notwendigkeit einer Lösung aus?**

A „Die erschwerenden Faktoren für unsere Bestandsaufnahme waren die Art und Weise, wie die IT und organisatorischen Abläufe eingerichtet wurden. Auf der IT-Seite nutzen wir ein Shared Service Center für bestimmte IT-Verfahren und für das Hosting unserer Domains. Auf organisatorischer Ebene verfolgen wir einen dezentralisierten Ansatz, was zu mehr Autonomie für die einzelnen Abteilungen führt. Wenn zum Beispiel ein Marketingteam eine Domain einrichten möchte, wird diese Anfrage vom Shared Service Center bearbeitet. Diese Vorgehensweise lässt aber bei uns viele Fragen offen, weil wir die genaue Domain-Anzahl, die gemeinsam genutzten Informationen über diese Domains, Sicherheitszertifikate und mehr nicht im Auge behalten können.

Es gab drei Fragen, die wir beantworten mussten:

/ Welche Domains gibt es?

/ Welche Domains werden von uns verwaltet?

/ Was sind die Sicherheitsrisiken der Domains?“

Q **Wie haben Sie diese Informationslücken geschlossen?**

A „Es gab keine wirkliche Lösung, weder manuell noch automatisiert. Wir brauchten Unterstützung, die das ständige Erkundigen beim Shared Service Center nach neuen Domain- und Sicherheitsupdates ersetzte. Die Informationssicherheit liegt in der Verantwortung meines Teams, deshalb wollten wir selbst die Kontrolle behalten und nicht

von unserem Service-Center abhängig sein — obwohl wir wissen, dass wir diesem vertrauen können.

Wir starteten also ganz von vorne. Da es keine frühere Lösung bzw. ein Werkzeug für die Bestandsaufnahme gab, mussten wir erst eine solide Grundlage schaffen. Die zielgerichtete und gründliche Arbeit war das zentrale Problem, und genau dabei brauchten wir Hilfe. Wir sind jetzt noch nicht in der Phase, in der wir die Sicherheitsleistung oder die Wirksamkeit der Richtlinien bewerten können, aber das Inventar ist mit jedem bestätigten Asset gewachsen, das die Plattform identifiziert hat. Wir haben auch bereits mehr Assets gefunden, als wir dachten."

Q **Was sind die nächsten Schritte?**

A „Wir werden weiterhin unseren digitalen Fußabdruck kartieren, um einen immer besseren Überblick zu erhalten. Die automatisierte Risikokategorisierung macht es einfacher, kritische Schwachstellen und Risiken sofort zu priorisieren. Bisher lag der Schwerpunkt darauf, ein vollständiges Bild zu erhalten, welche Bereiche mit unserer Organisation in Zusammenhang stehen und wer sie verwalten sollte. Wir übernehmen keine Verantwortung für Bereiche, die nicht unter der Kontrolle unseres Teams stehen, aber die detaillierten Informationen und Handlungsvorschläge pro Asset helfen, andere Abteilungen zu steuern. Gemeinsam haben wir erhebliche Fortschritte bei der Stärkung unserer Cyber-Resilienz erzielt."

Q **Vielleicht können wir uns in einigen Monaten noch einmal zu einem zweiten Gespräch treffen, um zu sehen, wie sich Ihre Erkenntnisse zum digitalen Fußabdruck entwickelt haben?**

A „Auf jeden Fall."