Secur & Resi
IT-Sicherheit und Katastrophenschutz für Behörden

Externe Sicherheit im Behördenumfeld oft noch unterschätzt: Vier kritische Bereiche im Fokus

Spezialdienstleister Secur & Resi warnt Behörden und Organisationen vor potenziellen Einfallstoren und neuen Angriffsmethoden

Dreieich, 14.07.2026 – Behörden und Organisationen setzen einen Großteil ihrer IT-Security-Ressourcen oft für die interne Absicherung ein. Teilweise noch stark unterschätzt werden in diesem Umfeld häufig jedoch Risiken und Gefahren, die außerhalb des eigenen, geschützten Netzwerks entstehen.

René Rühl, Spezialist für IT-Sicherheit und Bevölkerungsschutz im Behördenumfeld und Inhaber des Dienstleistungsunternehmens Secur & Resi, sieht gerade in diesem Bereich der externen Sicherheit erheblichen Nachholbedarf:

„In vielen Behörden liegt der Fokus IT-Security-seitig auf Maßnahmen wie Firewalls, E-Mail-Sicherheit oder auch Cloud Security. Alles wichtig und absolut nachvollziehbar. Bislang deutlich weniger beachtet werden allerdings Einfallstore wie kompromittierte Dienstleister innerhalb der Lieferkette, geleakte Zugangsdaten, die zum Teil im Darknet gehandelt werden oder auch Fake Domains beziehungsweise täuschend echt nachgebaute Websites, über die sensible Daten abgefangen werden."

Der IT-Sicherheits-Experte weist darauf hin, dass Cyber-Kriminelle bewusst den einfachsten Weg wählen, um ihre Ziele zu erreichen. Und dieser ist in vielen Fällen nicht ein direkter, frontaler Angriff auf das (zumeist stark abgesicherte) Behörden- oder Organisations-Netz, sondern erfolgt über trickreiche Umwege.

„Viele Behörden und Organisationen unterschätzen beispielsweise die Problematik geleakter Zugangsdaten, die zum Teil im Darknet zum Kauf angeboten werden. Auch personenbezogene Daten von Behördenmitarbeitern sind auf diese Weise im Darknet zu finden. Ein weiteres Thema, das wir aktuell beobachten, sind Fake-Webseiten, die sich eng an die Domains offizieller Behörden anlehnen. Sie unterscheiden sich oft nur durch eine kleine, unauffällige Anpassung oder eine andere Top-Level-Domain. Solche Websites können als Vehikel für spätere Angriffe dienen", so Rühl.

Behörden und Organisationen sollten nach Meinung des Spezialisten den Fokus vor allem darauf legen, potenzielle Angriffe dieser und ähnlicher Art bereits im Vorfeld zu erkennen:

„Attacken werden oft über einen längeren Zeitraum vorbereitet. Fake-Seiten werden eingerichtet, Daten gesammelt oder auf dubiosen Kanälen zum Kauf angeboten. All dies hinterlässt Spuren. Mit geeigneten Mitteln und dem richtigen Know-how können Behörden aber Frühwarn-Systeme aufbauen, die im Idealfall Alarm schlagen, lange bevor tatsächlich etwas passiert. Dieser zeitliche Vorteil kann ein sehr wichtiger Faktor sein, um sich beispielsweise vor Social-Engineering-Angriffen zu schützen und rechtzeitig Gegenmaßnahmen zu ergreifen."

Rühl empfiehlt Behörden, zur Verbesserung ihrer externen Sicherheit den Fokus auf vier wesentliche Bereiche zu richten:

1. Schutz der externen Angriffsfläche

Kontinuierliche Aufklärung und Erfassung, um beispielsweise Risiken durch Schatten-IT und vergessene Assets zu erkennen.

2. Schutz und Überwachung der externen Lieferkette

Oft ist das schwächste Glied einer Kette der bevorzugte Angriffspunkt. Dabei kann es sich auch um Dienstleister von Dienstleistern handeln. Es gilt, Sicherheitsvorfälle bei Zulieferern frühzeitig zu erkennen und Risiken bei Drittparteien sichtbar zu machen.

3. Schutz sensibler Informationen außerhalb des eigenen Perimeters

Behörden müssen geeignete Prozesse und Systeme aufbauen, um Datenabflüsse außerhalb des eigenen Perimeters zu erkennen und Informationen bewerten und gegebenenfalls zurückholen zu können.

4. Externe Sicherheit beim Schutz von Personal und Schlüsselrollen

Entscheidend ist hier, Targeting-Aktionen gegen Funktionsträger frühzeitig erkennen zu können, hinsichtlich ihrer Tragweite und Gefährlichkeit zu bewerten und darauf basierend geeignete Maßnahmen einzuleiten.

Secur & Resi fungiert als Schnittstelle für IT-Sicherheit & Bevölkerungsschutz zwischen Behörden, BOS, Bundeswehr und spezialisierten Partnern. Das Unternehmen verfolgt dabei den Ansatz, die bislang organisatorisch oft getrennten Bereiche IT-Sicherheit und Bevölkerungsschutz miteinander zu verbinden und dadurch zusätzliche Synergieeffekte zu erreichen.

Weitere Informationen: www.secres.de

Über Secur & Resi

Secur & Resi hat sich auf die Themenfelder IT-Sicherheit und Bevölkerungsschutz im Behördenumfeld spezialisiert. Als deutschlandweit tätiger Dienstleister berät das Unternehmen insbesondere Behörden und Organisationen sowie die Bundeswehr. Dabei vernetzt Secur & Resi Organisationen und Behörden mit den passenden Lösungsanbietern und bietet ein umfangreiches Leistungsspektrum: Von der Bedarfsanalyse über die Auswahl geeigneter Projektpartner bis zur finalen Umsetzung. Secur & Resi versteht sich als Integrator und Moderator. Das Unternehmen legt zudem einen starken Fokus auf digitale Souveränität und arbeitet ausschließlich mit Technologie- und Dienstleistungspartnern aus der EU und der Schweiz zusammen.
Web: www.secres.de

Firmenkontakt:

Secur & Resi
René Rühl
Kastanienweg 4
63303 Dreieich
Tel. +49 6103 388 12 12
E-Mail: Rene.Ruehl@secres.de