Komm.ONE

Cyber-Sicherheit wird zur Daueraufgabe

[29.06.2026] Der IT-Dienstleister Komm.ONE warnt beim Cybersicherheitstag 2026 vor zunehmender Professionalisierung der Angreifer. Prävention, Zusammenarbeit und Künstliche Intelligenz gewinnen an Bedeutung.

Die Bedrohungslage im Cyber-Raum verschärft sich weiter. Angriffe auf Kommunen nehmen zu, die Täter agieren immer professioneller und Künstliche Intelligenz verändert sowohl die Methoden der Angreifer als auch die Möglichkeiten der Verteidigung. Diese Botschaft zog sich wie ein roter Faden durch die Pressekonferenz anlässlich des Cybersicherheitstags 2026 des baden-württembergischen IT-Dienstleisters Komm.ONE.

Gemeinsam mit Vertretern der Cybersicherheitsagentur Baden-Württemberg (CSBW), Sicherheitsexperten und Psychologen diskutierte Komm.ONE über aktuelle Bedrohungen, notwendige Schutzmaßnahmen und die Frage, wie Kommunen ihre digitale Resilienz stärken können. Ein zentrales Fazit: Cyber-Sicherheit ist längst keine rein technische Aufgabe mehr, sondern betrifft Organisation, Führung und Mitarbeitende gleichermaßen.

Bedrohungslage verschärft sich weiter

„Die Cyber-Sicherheitslage war schon immer angespannt, aber die Gefahren steigen weiter an“, erklärte Björn Schemberger von der Cybersicherheitsagentur Baden-Württemberg. Digitalisierung und zunehmende Vernetzung erweiterten kontinuierlich die Angriffsfläche öffentlicher Einrichtungen. Gleichzeitig beschleunige der Einsatz Künstlicher Intelligenz sowohl Schutz- als auch Angriffsmöglichkeiten. Die Entwicklung spiegelt sich auch in den Fallzahlen wider. Während die Cybersicherheitsagentur vor wenigen Jahren rund 560 Sicherheitsvorfälle jährlich bearbeitet habe, liege die Zahl inzwischen bei annähernd 900 Fällen pro Jahr. Dabei reiche das Spektrum von ersten Verdachtsfällen bis hin zu vollständig durch Ransomware lahmgelegten Infrastrukturen.

Schemberger erwartet, dass KI den Wettlauf zwischen Angreifern und Verteidigern zunächst weiter beschleunigen wird. Moderne KI-Systeme seien inzwischen in der Lage, Softwareschwachstellen deutlich schneller zu identifizieren. Dadurch müsse künftig wesentlich mehr Aufwand in das zeitnahe Schließen von Sicherheitslücken investiert werden. Langfristig könne dies allerdings auch zu einer höheren Softwarequalität führen.

Cyber-Kriminalität ist längst organisierte Industrie

Besonders eindrücklich schilderte Wirtschaftspsychologe und Profiler Mark Hofmann die Entwicklung der Täterstrukturen. Cyber-Kriminalität sei heute hochgradig arbeitsteilig organisiert und gleiche in vielen Bereichen professionellen Wirtschaftsunternehmen. Nach Schätzungen verursache Cyber-Kriminalität weltweit Schäden von über 11 Billionen US-Dollar jährlich. Wäre Cybercrime ein Staat, so Hofmann, wäre dieser gemessen an seiner Wirtschaftsleistung die drittgrößte Volkswirtschaft der Welt.

Die klassischen Bilder vom isolierten Hacker im Kapuzenpulli seien längst überholt. Moderne Ransomware-Gruppen verfügten über technische Abteilungen, Finanzexperten und Affiliate-Netzwerke mit

teilweise mehr als hundert Mitarbeitenden. Selbst telefonischer „Kundendienst“ während laufender Erpressungen gehöre inzwischen zum Geschäftsmodell.

Hinzu komme eine ausgeprägte Arbeitsteilung innerhalb der kriminellen Szene. Spezialisierte sogenannte Access Broker verschaffen sich Zugang zu IT-Systemen und verkaufen diesen anschließend an andere Gruppen weiter, die den eigentlichen Angriff durchführen. Häufig liege zwischen der ersten Kompromittierung eines Systems und einer späteren Ransomware-Attacke ein Zeitraum von bis zu zwei Jahren.

KI senkt die Einstiegshürden für Täter

Besondere Aufmerksamkeit widmeten die Experten den Auswirkungen generativer Künstlicher Intelligenz. Hofmann erwartet, dass sich dadurch das Profil künftiger Täter grundlegend verändern wird. Bislang seien schwere Cyber-Angriffe überwiegend von hochqualifizierten IT-Spezialisten ausgegangen. Durch generative KI werde künftig jedoch wesentlich weniger technisches Wissen erforderlich sein. „Man braucht bald keinen Informatikabschluss mehr, sondern nur noch einen Laptop und ein Motiv“, lautete seine Einschätzung. Damit wachse der Kreis potenzieller Täter erheblich. Während bislang vor allem die technischen Fähigkeiten den Zugang zur Cyber-Kriminalität begrenzten, könnten KI-gestützte Werkzeuge diese Hürde künftig deutlich senken.

Der Mensch bleibt das größte Einfallstor

Trotz aller technischen Entwicklungen waren sich sämtliche Experten in einem Punkt einig: Der größte Risikofaktor bleibt der Mensch. Phishing-Mails, unsichere Passwörter oder fehlende Mehrfaktor-Authentifizierung zählen nach wie vor zu den häufigsten Einfallstoren. Gleichzeitig müsse Cyber-Sicherheit weit über die IT-Abteilung hinaus gedacht werden. „Cyber-Sicherheit muss Chefsache sein“, betonte Björn Schemberger. Von der Behördenleitung über Administratoren bis hin zu den Beschäftigten müssten alle Beteiligten Verantwortung übernehmen. Sicherheitsbewusstsein dürfe sich nicht auf einzelne Fachbereiche beschränken.

Auch Mark Hofmann plädierte dafür, Sicherheitskampagnen stärker an den Alltag der Beschäftigten anzupassen. Klassische Awareness-Schulungen erreichten häufig nur Menschen, die sich ohnehin für IT-Sicherheit interessierten. Entscheidend sei jedoch, jene Mitarbeitenden anzusprechen, die täglich E-Mails öffneten oder Anhänge bearbeiteten. Sein Appell lautet daher: „Make it about people and not just about business.“ Sicherheitskampagnen müssten persönliche Betroffenheit erzeugen und Themen aus dem privaten Umfeld – etwa Deepfakes oder den Enkeltrick – aufgreifen, um nachhaltige Verhaltensänderungen zu bewirken.

Komm.ONE setzt auf Prävention und Beratung

Für Komm.ONE erläuterten Uwe Sehner und Tobias Wenninger den Ansatz des kommunalen IT-Dienstleisters. Ziel sei es, Angriffe möglichst frühzeitig zu verhindern, anstatt erst im Schadensfall reagieren zu müssen. Dazu gehörten der sichere Betrieb der Netzinfrastruktur ebenso wie Beratungsangebote, Sensibilisierungsmaßnahmen und technische Sicherheitslösungen. Cyber-Sicherheit werde dabei bewusst als mehrschichtiges Gesamtkonzept verstanden.

Neben technischen Schutzmaßnahmen spiele insbesondere die Zusammenarbeit mit den Kommunen eine zentrale Rolle. Gemeinsam werde kontinuierlich daran gearbeitet, das Sicherheitsniveau zu erhöhen und aktuelle Erkenntnisse auszutauschen. Auch beim Einsatz Künstlicher Intelligenz sieht Komm.ONE großes Potenzial. KI unterstütze bereits heute Sicherheitslösungen bei der Analyse großer Datenmengen, erkenne ungewöhnliche Netzwerkaktivitäten schneller und ermögliche dadurch kürzere Reaktionszeiten.

Vernetzung als Schlüssel zur Resilienz

Ein weiteres zentrales Thema der Pressekonferenz war die enge Zusammenarbeit zwischen den verschiedenen Akteuren. Die Cybersicherheitsagentur Baden-Württemberg versteht sich als zentrale Koordinierungsstelle für den öffentlichen Sektor. Informationen aus Landes- und Bundesbehörden, internationalen Partnern sowie aus eigenen Analysen laufen dort zusammen, werden bewertet und nahezu in Echtzeit an Kommunen und andere öffentliche Einrichtungen weitergegeben.

Schemberger sprach in diesem Zusammenhang von einer „Spinne im Netz“, die sämtliche relevanten Informationen bündelt und verteilt. Geschwindigkeit werde dabei immer wichtiger, da zwischen Bekanntwerden einer Sicherheitslücke und ihrer Ausnutzung oft nur noch Stunden oder sogar Minuten lägen. Auch zwischen Komm.ONE und der Cybersicherheitsagentur besteht ein enger Informationsaustausch. Gemeinsame Lagebilder und abgestimmte Reaktionen sollen dazu beitragen, Angriffe möglichst frühzeitig zu erkennen und Schäden zu begrenzen.

Investitionen bleiben unverzichtbar

Mehrfach wurde während der Diskussion die angespannte finanzielle Lage vieler Kommunen angesprochen. Gleichwohl waren sich die Experten einig, dass Investitionen in Cyber-Sicherheit alternativlos seien. „Nicht zu investieren ist keine Option“, stellte Schemberger klar. Die Kosten eines erfolgreichen Ransomware-Angriffs überstiegen den Aufwand präventiver Maßnahmen um ein Vielfaches. Wochenlange Betriebsunterbrechungen, hohe personelle Belastungen und erhebliche organisatorische Folgen seien die Regel. Dabei gehe es nicht zwangsläufig um enorme zusätzliche Budgets. Bereits durch moderne Sicherheitskonzepte, klare Verantwortlichkeiten und kontinuierliche Präventionsarbeit lasse sich die Widerstandsfähigkeit einer Kommune deutlich verbessern.

Sicherheitsbewusstsein wächst

Positiv bewerteten die Teilnehmer die Entwicklung des Sicherheitsbewusstseins in den vergangenen Jahren. Angebote wie die Cyber-Sicherheitstage, Notfallübungen oder Informationsveranstaltungen würden inzwischen deutlich stärker nachgefragt als noch vor wenigen Jahren. Nach Einschätzung der Experten entsteht dabei ein positiver Kreislauf: Je häufiger Sicherheitsvorfälle bekannt werden und je intensiver Kommunen ihre Erfahrungen austauschen, desto stärker wächst auch die Bereitschaft, in Prävention zu investieren.

Für Hofmann liegt darin sogar ein strategischer Vorteil gegenüber den Angreifern. Während sich Behörden, Unternehmen und Sicherheitsorganisationen offen austauschen könnten, herrsche innerhalb der kriminellen Szene ein tiefes gegenseitiges Misstrauen. Kooperation und Wissenstransfer seien deshalb auf der Seite der Verteidiger ein entscheidender Erfolgsfaktor.

Dauerhaften Führungsaufgabe

Die Botschaft des Cybersicherheitstags fiel damit eindeutig aus: Angesichts professioneller Angreifer, neuer KI-gestützter Bedrohungen und wachsender digitaler Abhängigkeiten wird Cyber-Sicherheit zu einer dauerhaften Führungsaufgabe in den Kommunen. Technische Schutzmaßnahmen allein reichen dafür nicht aus. Gefragt sind ebenso organisatorische Resilienz, kontinuierliche Sensibilisierung der Mitarbeitenden und eine enge Zusammenarbeit aller beteiligten Akteure.

()

Stichwörter: IT-Sicherheit, Komm.ONE, Cyber-Abwehr, Cyber-Sicherheit