Cybersicherheit | 24.01.2024 | Nr. 17/24

Uta Wentzel: TOP 42: Es gilt, die Resilienz aufzubauen und mehr Aufmerksamkeit auf unsere digitale Sicherheit zu richten.

Es gilt das gesprochene Wort!

Sehr geehrte Frau Präsidentin,
sehr geehrte Damen und Herren,

Anhalt-Bitterfeld, IHK, Handwerkskammer. Sie alle sind Opfer von Hackerangriffen geworden. Und stehen dabei beispielhaft für die Cyberkriminalität, die uns täglich bedroht. Die Digitalisierung hat unsere Welt grundlegend verändert. Doch neben den Vorteilen, die diese Vernetzung bietet, entstehen auch erhebliche Risken. Wir sind verwundbarer geworden.

Die Kriminalstatistik der Polizei verzeichnet einen kontinuierlichen Anstieg der Cyberkriminalität: 2022 wurden mehr als 130.000 Fälle erfasst. Auch bei uns in Schleswig-Holstein stiegen seit 2019 die Zahlen um fast 40 Prozent. Wir begrüßen daher sehr den Aufbau der Cyber-Hundertschaft durch das Innenministerium, um die Cyberkriminalität in Schleswig-Holstein wirksamer zu bekämpfen.

Nahezu alle Bereiche unserer Gesellschaft sind betroffen. Unternehmen, Behörden und private Haushalte – keiner ist sicher vor den kriminellen Machenschaften.

Datenlecks, Hacker-Angriffe und IT-Ausfälle sind für Firmen in Deutschland und weltweit zum größten Risiko geworden. Das geht aus dem neuen „Allianz Risk Barometer 2024“ hervor. 44 Prozent der befragten Unternehmen schätzen Cyberkriminalität als eine der größten Gefahren ein. Am meisten sehen sich Unternehmen durch Datenpannen bedroht, bei denen Kriminelle personenbezogene Daten oder Betriebsgeheimnisse abgreifen. Auch Angriffe mit Ransomware häufen sich. Solche Schadprogramme können Systeme komplett lahmlegen. Dabei verschlüsseln Kriminelle mit einem Trojaner die IT-Netzwerke ganzer Unternehmen und erpressen sie.

Was für Firmen geschäftsschädigend sein kann, ist für Kriminelle lukrativ. So sehr, dass sich darum Geschäftsmodelle gebildet haben. Im Darknet bieten kriminelle Hacker Auftragsarbeiten an und vermieten Erpressungssoftware.

Der deutschen Wirtschaft kommen Cyberattacken teuer zu stehen. Laut der Bitkom-Studie „Wirtschaftsschutz 2023“ summierte sich der jährliche Schaden für

Pressesprecher Max Schmachtenberg | Düsternbrooker Weg 70, Landeshaus, 24105 Kiel
0431/988-1440 | info@cdu.ltsh.de | http://www.cdu.ltsh.de

Unternehmen auf 206 Milliarden Euro. Die meisten Angriffe kommen aus Russland und China. Mehr als die Hälfte der befragten Firmen fühlen sich durch Cyberattacken in ihrer Existenz bedroht.

Auch in Schleswig-Holstein haben Hackerangriffe Schäden im Millionenbereich verursacht. Wie zum Beispiel 2021 bei den Mürwiker Werkstätten in Flensburg. Dort forderten die Angreifer von dem Unternehmen, das mehrere Einrichtungen für Menschen mit Behinderung betreibt, ein Lösegeld in Höhe von 2,3 Millionen Euro in Bitcoins für die Freigabe der verschlüsselten Daten. Auch hier weigerte man sich, zu zahlen und brauchte Monate, um die Systeme wieder zum Laufen zu bringen. Die Staatsanwaltschaft ermittelt und vermutet auch in diesem Fall eine russische Tätergruppe hinter dem Cyberangriff.

Seit dem russischen Angriffskrieg haben Cyber-Attacken insbesondere auf staatliche Stellen zugenommen. Ob kritische Infrastruktur, Gesundheitswesen oder die Verwaltung: jeder Bereich des Staates wird bedroht und muss geschützt werden, wie im Bericht detailliert aufggeführt.

Es gilt, die Resilienz aufzubauen und mehr Aufmerksamkeit auf unsere digitale Sicherheit zu richten.

Wir begrüßen daher den Antrag des SSW und danken der Landesregierung an dieser Stelle sehr für den nun vorliegenden, umfassenden Bericht zur Cybersicherheit unserer Infrastruktur. Der Bericht stellt die Notwendigkeit einer umfassenden Sicherheitsarchitektur dar, sowie Maßnahmen, die effektiv unsere Sicherheit verbessern.

Besonders relevant ist das "3-Säulen-Modell", das die Zusammenarbeit der verschiedenen Ebenen im Bereich der Informations- und Cybersicherheit darstellt.

Dieses Modell umfasst die drei Säulen:

1. polizeiliche Ermittlungen bei Cyberkriminalität (durch LKA und BKA),
2. das gesamte Informations- und Sicherheitsmanagement, das u.a. für den Ordnungsrahmen, die Landesstrategie digitale Resilienz und die Schnittstelle zum BSI, dem Katastrophenschutz und CERT Nord zuständig ist
3. und die Spionageabwehr (durch den Verfassungsschutz).

Der Bericht verdeutlicht, wie wichtig die Informationssicherheit auch für das Vertrauen in staatliches Handeln und digitale Souveränität ist.

Gemeinsam mit der ITVSH hat das Land das Projekt "Sicherheit für Kommunen in Schleswig-Holstein" entwickelt, kurz: SiKoSH. Das siebenstufige Programm hilft beim Aufbau eines professionellen Informationssicherheitsmanagements (ISMS) und ermöglicht auch kleineren Organisationen den gesetzlichen Verpflichtungen nachzukommen und die Daten der Bürgerinnen und Bürger zu schützen.
Das Ziel ist ein hohes gemeinsames Sicherheitsniveau.

Pressesprecher Max Schmachtenberg | Düsternbrooker Weg 70, Landeshaus, 24105 Kiel
0431/988-1440 | info@cdu.ltsh.de | http://www.cdu.ltsh.de

Doch eines müssen wir uns stets vor Augen führen: eine absolute Sicherheit wird es nie geben. Wir müssen uns kontinuierlich auf neue Entwicklungen und Bedrohungen einstellen. Auch im Haushalt 2024 stellen wir über 25 Millionen Euro für die Cybersicherheit bereit. Nur mit einer modernen Sicherheitsinfrastruktur können wir uns den Herausforderungen im digitalen Raum stellen.

Vielen Dank für Ihre Aufmerksamkeit!

Pressesprecher Max Schmachtenberg | Düsternbrooker Weg 70, Landeshaus, 24105 Kiel
0431/988-1440 | info@cdu.ltsh.de | http://www.cdu.ltsh.de