Senatsverwaltung
für Inneres, Digitalisierung
und Sport

BERLIN

„Cybersicherheit in Kritischen Infrastrukturen stärken!“

Ein Projekt der Senatsverwaltung für Inneres, Digitalisierung und Sport mit wissenschaftlicher Begleitung durch das Digital Society Institute (DSI) der European School of Management and Technology Berlin (ESMT) zur Stärkung der Cybersicherheit in kritischen Infrastrukturen im Land Berlin

Cyberangriffe auf kritische Infrastrukturen, aber auch kleine und mittelständische Unternehmen (KMU) sind längst keine Seltenheit mehr. Allein die wirtschaftlichen Schäden, die den Unternehmen infolge von Cyberangriffen entstehen, haben sich in Deutschland seit 2019 mehr als verdoppelt. Insbesondere vor dem Hintergrund des russischen Angriffskrieges auf die Ukraine lässt sich ein stark steigendes Risiko verzeichnen.
Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt „eine erhöhte Bedrohungslage für Deutschland im Kontext des Krieges in der Ukraine fest, die auf eine ohnehin schon angespannte Gesamtbedrohungslage trifft. (...) Das BSI ruft daher weiterhin Unternehmen, Organisationen und Behörden auf, ihre IT-Sicherheitsmaßnahmen zu überprüfen und der gegebenen Bedrohungslage anzupassen.“ (Quelle: BSI, Einschätzung der aktuellen Cyber-Sicherheitslage in Deutschland nach dem russischen Angriff auf die Ukraine, vom 03. August 2022)

Die Senatsverwaltung für Inneres, Digitalisierung und Sport (SenInnDS) unterstützt die Schaffung einer resilienteren Stadt gegenüber IT-Störfällen. Zur Förderung dieses Ziels, hatte die SenInnDS das Digital Society Institute (DSI) der European School of Management and Technology (ESMT) mit einer Workshopreihe beauftragt, die insbesondere eine Risikoanalyse des Landes Berlin beinhaltete.

Das Projekt, welches im Dezember 2020 begonnen hat und im Februar 2022 abgeschlossen wurde, umfasste vier sektorale Workshops mit Berliner KRITIS-Betreibern, den zuständigen Berliner Aufsichtsbehörden, der Polizei Berlin (LKA 72-Cybercrime-Dezernat), Berliner Feuerwehr und IHK sowie einen sektorenübergreifenden Workshop, bei dem die Ergebnisse präsentiert und mit den teilnehmenden Organisationen diskutiert wurden. Social Engineering, Identitätsbetrug, Phishing, Ransomware und Supply Chain Attacks wurden im Rahmen des Projektes als die aktuell größten Cyberbedrohungen für Unternehmen ermittelt.

Als ein Ergebnis des Projektes wurden u.a. die Risiken und gegenseitigen Abhängigkeiten (Interdependenzen) der einzelnen Sektoren benannt sowie Handlungsempfehlungen insbesondere für Berliner Unternehmen herausgearbeitet:

- Da Abhängigkeiten häufig ein unterschätztes Risiko darstellen, sollte ein erhöhtes Risikobewusstsein auch im Hinblick auf die bestehenden Interdependenzen geschaffen werden. Um ein Beispiel zu nennen: Unternehmen sind teilweise abhängig von einer großen Anzahl von Lieferanten und deren IT-Sicherheitsstandards.

- Um die Geschäftsrisiken so gering wie möglich zu halten, ist das Treffen von technischen Sicherheitsvorkehrungen - auch entlang der Lieferketten - ratsam. Um den Schutz gegen Supply Chain Attacks zu erhöhen, empfehlen sich beispielsweise Lieferantenaudits, da die Abhängigkeiten in den Lieferketten vermehrt von Cyberkriminellen ausgenutzt werden.
- Um das Risikobewusstsein im Hinblick auf Cyberbedrohungen zu erhöhen, ist der regelmäßige Austausch zwischen den Unternehmen durch die Nutzung regionaler und bundesweiter Plattformen zu empfehlen (z.B. in Netzwerken wie die Deutsche Cyber-Sicherheitsorganisation, Verbänden und Initiativen).
- Auch die stärkere Initiative und Teilnahme der KMU am Austausch mit Bundes- und Landesbehörden (z.B. Allianz für Cyber-Sicherheit) ist förderlich, um sich als Unternehmen auf dem Laufenden zu halten und für den Fall eines Cyberangriffs vorzusorgen.
- Oft werden die Mitarbeitenden als das schwächste Glied in der IT-Sicherheits-Kette beschrieben. Aber kompetente und motivierte Mitarbeitende sind das Rückgrat und ein wichtiger Erfolgsgarant für das Unternehmen. Deshalb sollte in die IT-Kompetenz der Mitarbeitenden investiert werden und Sensibilisierungs- und Awareness-Maßnahmen längst Standard sein.

Als weiteres Ergebnis aus dem Projekt ist neben einem Informations- und Funktionsmodell, welches die Informationsbeziehungen und -prozesse sowie die konkreten Zuständigkeiten der Beteiligten im Land Berlin abbildet, die Urbane Cyber-Risikoanalyse (UCR) des Landes Berlin entwickelt worden:

- Die UCR gliedert sich in eine Einführung, die Entwicklung methodischer Grundlagen (Risikoidentifikation, -bewertung und -evaluation), die Anwendung der Methode auf die Berliner KRITIS und ein Fazit.
- Ziel der UCR ist es, die Cyberrisiken zu identifizieren, diese im Kontext mit den Auswirkungen, Wahrscheinlichkeiten und dem Risikolevel zu bewerten und anschließend zu evaluieren, um den Risiken adäquat mit entsprechenden Maßnahmen des Risikomanagements begegnen zu können.
- Aufgrund ihrer dynamischen Funktionalität kann die UCR künftig auf mehreren Ebenen und in unterschiedlicher Tiefe durchgeführt werden. Sie bildet eine Blaupause und kann ebenso auf Kommunen, Länder oder Staatenverbunde angewandt, weiterentwickelt und beispielsweise um „Lokal-Impakt-Analysen“ als Grundlage für Cybersicherheitsstrategien erweitert werden.

Autor*innen: Frau Laura Pia, Herr Berkin Senkaya

Senatsverwaltung für Inneres, Digitalisierung und Sport
Abteilung III – Öffentliche Sicherheit und Ordnung
AG Cybersicherheit

Dezember 2022