Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

„Bericht zur Lage der IT-Sicherheit in Deutschland 2020“

Am 20. Oktober 2020 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) den neuen „Bericht zur Lage der IT-Sicherheit in Deutschland 2020“ veröffentlicht.

Der jährliche Lagebericht der Cyber-Sicherheitsbehörde des Bundes bietet einen umfassenden Überblick über die Bedrohungen Deutschlands, seiner Bürgerinnen und Bürger und seiner Wirtschaft im Cyber-Raum. Zudem beinhaltet der Lagebericht Gegenmaßnahmen und Lösungsansätze des BSI zur Gestaltung der Informationssicherheit in der Digitalisierung für Staat, Wirtschaft und Gesellschaft.

Die Gefährdungslage bleibt aufgrund täglich neuer Schwachstellen, neuer Angriffsmethoden und steigender Komplexität in der IT-Landschaft dynamisch und angespannt, mit zum Teil dramatischen Auswirkungen auf Unternehmen, Behörden und Einzelpersonen.

Die Corona-Pandemie hat großen Einfluss auf die Cyber-Sicherheitslage in Deutschland. Corona hat für einen Digitalisierungsschub in Deutschland gesorgt. Maßnahmen wie die Einrichtung von Homeoffice-Arbeitsplätzen und digitalen Geschäftsprozessen, die Nutzung von Videokonferenzen und Bring-Your-Own-Device mussten kurzfristig umgesetzt werden. IT-Sicherheit spielte dabei eine untergeordnete Rolle. Diese Maßnahmen gilt es nun angemessen abzusichern, ohne auf die Vorteile der „neuen Normalität“ zu verzichten.

Der Corona-bedingte Digitalisierungsschub hat gezeigt, wie wichtig funktionierende, sichere IT ist.

Die aktuelle Gefährdungslage ist weiterhin geprägt von Cyber-Angriffen mit Schadsoftware, die in immer neuen Varianten und mit teils ausgefeilten Methoden eingesetzt wird. Die Zahl der Schadprogramme steigt weiter an, allein im Berichtszeitraum (Juni 2019 bis Mai 2020) sind 117,4 Millionen neue Varianten hinzugekommen, 320.000 pro Tag.

Weiterhin dominant ist die Schadsoftware Emotet. Emotet ermöglicht eine Kaskade weiterer Schadsoftware-Angriffe bis hin zu gezielten Ransomware-Angriffen auf ausgewählte, zahlungskräftige Opfer.

Von Cyber-Angriffen insbesondere mit Ransomware betroffen sind Unternehmen und Institutionen aller Größen und Branchen. Neben Automobilherstellern und ihren Zulieferern, Flughäfen und Fluggesellschaften waren auch KMU, die sich durch besonderes Know-how auszeichnen, Opfer von Cyber-Angriffen. Auch kommunale Verwaltungen, Krankenhäuser und Hochschulen waren von Ransomware-Angriffen betroffen.

Bemerkenswert ist die Bedrohung durch Daten-Leaks, das heißt den Diebstahl oder die unbeabsichtigte Offenlegung personenbezogener Datensätze (Kundendaten oder Patientendaten). So waren in einem Fall allein in Deutschland etwa 15.000 Patientendatensätze mit mehreren Millionen medizinischen Bildern öffentlich ohne Passwortschutz zugänglich.

Gerade im Gesundheitswesen wird deutlich, wie wichtig die Informationssicherheit als Voraussetzung einer erfolgreichen Digitalisierung ist. Sichere, verfügbare, funktionierende Informationstechnologie ist die Voraussetzung dafür, dass medizinisches Personal seine Aufgabe erfüllen kann. Dies gilt sinngemäß ebenso für jedes andere Berufsfeld.

Bei der Absicherung der Digitalisierung im Gesundheitswesen gibt es Nachholbedarf. Dies haben die teils erfolgreichen Cyber-Angriffe auf Krankenhäuser sowie auch bekannt gewordene Schwachstellen in Medizinprodukten gezeigt. Das BSI hat einige Initiativen und konkrete Unterstützungsmaßnahmen auf den Weg gebracht, die zur weiteren Absicherung des Gesundheitswesens beitragen.

Das BSI hat auch während der Corona-Krise intensiv daran gearbeitet, die Informationssicherheit in Bereichen zu gestalten und voranzutreiben, die für den Standort Deutschland wichtig sind, zum Beispiel 5G, Künstliche Intelligenz, das Smart Home oder das vernetzte, autonome Fahren.

Durch eine Vielzahl an konkreten operativen Maßnahmen, unterstützenden Kooperationen, richtungsweisenden Vorgaben und sensibilisierenden Empfehlungen leistet das BSI einen entscheidenden Beitrag dazu, den Weg in die digitalisierte Gesellschaft für jeden Einzelnen sicher zu gestalten.