Die Digitalisierung ist in vollem Gange.

Daten sind zum wichtigsten Rohstoff unserer Zeit geworden. Die Vorteile neuer Technologien, wie z. B. künstlicher Intelligenz, dem Internet-der-Dinge oder Industrie 4.0, klingen verlockend: Wirtschaft und Verwaltung profitieren von effizienteren, produktiveren Arbeitsabläufen, jeder Einzelne von uns von verbesserten Dienstleistungen und Angeboten. Doch die neue digitale Welt ist in Gefahr. Cyberangriffe werden immer mehr zur Bedrohung für Wirtschaft und Gesellschaft. Da alles mit allem vernetzt ist, werden die Schäden, die durch Angreifer und Cyberkriminelle entstehen, immer größer. Mittlerweile melden drei Viertel der deutschen Unternehmen digitale Attacken. Aber nicht nur die Wirtschaft ist bedroht. Es betrifft jeden Einzelnen von uns. So sind bereits über die Hälfte der Internetnutzer in Deutschland Opfer von Cyber-Kriminalität geworden. Auch Attacken auf die neue digitale Arbeitswelt haben weltweit zugenommen, wie der aktuelle Lagebericht des BSI vom Oktober 2020 verdeutlicht. So wurden im Darknet gehackte Zugangsdaten für Videokonferenzen angeboten. Ungesicherte Server, Laptops und Router bedrohen das Homeoffice zusätzlich.

Die Bedrohungslage sähe jedoch noch sehr viel düsterer aus, hätten wir in den letzten Jahren nicht gewaltige Fortschritte sowohl bei der Erforschung neuer IT-Sicherheitslösungen als auch bei deren Umsetzung in Produkte und Anwendungen erzielt. Die Geschwindigkeit, mit der die Digitalisierung nicht zuletzt durch den Covid-19-Schub vorangetrieben wird, zeigt aber auch sehr deutlich weiteren dringenden Handlungsbedarf auf. Denn es geht nicht nur um mehr Effizienz und Produktivität: Die Verwundbarkeit bisher als sicher geglaubter Infrastrukturen untergräbt das Vertrauen in unsere gesamte moderne Wirtschafts- und Gesellschaftsordnung.

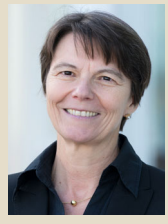
Mir liegt derzeit besonders das Thema „technologische Souveränität“ am Herzen. Souveränität bedeutet selbstbestimmtes staatliches oder aber auch unternehmerisches Handeln. Dies ist nicht mehr möglich, wenn die wirtschaftlichen und gesellschaftlichen Prozesse massiv von Dritten beeinflusst werden können. Das ist etwa dann der Fall, wenn die Funktionsfähigkeit der erforderlichen Technologie gezielt durch Ausspionieren und Manipulieren gestört oder aber auch die Bereitstellung der Technologien gezielt verweigert oder verzögert werden. Jedoch ist es ökonomisch nicht leistbar, alle erforderlichen Informations- und Kommunikationstechnologien (IKT) in Deutschland oder in der EU selbst zu entwickeln. Deutschland wird weiterhin auf nicht-europäische IKT-Produkte und -Dienstleistungen angewiesen bleiben. Es ist daher an der Zeit, Maßnahmen zu ergreifen, um die technologische Souveränität Schritt für Schritt zu erhöhen: Erstens müssen wir unsere IKT-Kompetenzen weiter ausbauen, um mögliche Risiken besser beurteilen zu können und kritische Abhängigkeiten zu reduzieren. Zweitens müssen Prüf- und Zertifizierungsverfahren etabliert werden, um sicherheitskritische Technologien zu beurteilen und beherrschbar nutzen zu können. Und drittens müssen wir in Forschung und Entwicklung investieren, um Zukunftstechnologien wie 6G und Quantencomputing frühzeitig zu gestalten.

Angewandte Cybersicherheitsforschung leistet hier im Schulterschluss mit der Wirtschaft einen wichtigen Beitrag: Forschungsteams entwickeln Sicherheitstechnologien, die IT-basierte Systeme und Produkte verlässlicher, vertrauenswürdiger und manipulationssicher machen. Dazu gehören auch Verfahren des Maschinellen Lernens, die bereits heute viele Bereiche unseres privaten und beruflichen Lebens beispielsweise durch Assistenzfunktionen (u.a. Spracherkennung, Fahrassistenz) prägen. Die Manipulationssicherheit derartiger Verfahren, aber auch das Erkennen von sogenannten Deep Fakes (gefälschte Bilder, Nachrichten, gesprochene Texte) sind technologische und gesellschaftliche Herausforderungen für die Sicherheitsforschung. Das Fraunhofer AISEC widmet sich deshalb mit Nachdruck auch dieser Thematik und entwickelt Verfahren, um Maschinelle Lernverfahren zertifizierbar zu machen, sie angriffsresilienter zu gestalten, aber auch um Deep Fakes effektiv zu erkennen.

Der technologische Wandel war und ist ein stetiger Begleiter des Menschen. Doch noch nie war der Wandel so rasant, so absolut und so durchdringend wie heute durch die Digitalisierung. Die Macht der Daten vermag Lösungen für Herkules-Aufgaben wie Klimawandel, Bevölkerungswachstum und Pandemien in greifbare Nähe rücken. Doch diese Vision wird nur dann Wirklichkeit, wenn wir die Augen nicht vor den Gefahren neuer Technologien verschließen und geeignete Maßnahmen ergreifen, um auf die Bedrohungen zu reagieren. Dazu gehört auch, Angriffe auf Internet, Unternehmensnetzwerke und Homeoffice ernst zu nehmen und uns dagegen zu wehren. Wir benötigen eine neue Sicherheitskultur, die es zu gestalten gilt. Jeder muss hierzu einen Beitrag leisten. Sei es der Staat, der seiner Fürsorgepflicht nachkommen und regulatorische Rahmen für die Wirtschaft, Unternehmen und Verwaltung schaffen muss, um ein Mindestsicherheitsniveau zu gewährleisten, und dabei gleichzeitig die Kräfte des Marktes nicht zu stark regulieren sollte. Oder Unternehmen, die aufgefordert sind, Daten- und Informationssicherheit, aber auch Privatheit, von Anfang an bei der Entwicklung neuer Produkte und Dienstleistungen zu berücksichtigen, und nicht zuletzt die Bürger, die sich ihrer eigenen Verantwortung beim Umgang mit ihren privaten, aber auch den unternehmerischen Daten und beim Einsatz von IT-Systemen bewusst sein müssen.

Prof. Dr. Claudia Eckert

Prof. Dr. Claudia Eckert



Claudia Eckert forscht und lehrt seit über 20 Jahren im Bereich der IT-Sicherheit. Sie hat über 10 Jahre das Fraunhofer SIT in Darmstadt geleitet und zu einem Sicherheitsinstitut aufgebaut. Seit 2009 ist sie Professorin für Sicherheit in der Informatik an der TU München und Direktorin des von ihr gegründeten Fraunhofer-Instituts für Angewandte und Integrierte Sicherheit AISEC in Garching bei München mit derzeit über 100 hoch qualifizierten Mitarbeiterinnen und Mitarbeitern. Ihre Forschungsergebnisse wurden in über 160 wissenschaftlichen Publikationen, Zeitschriftenbeiträgen und Büchern international veröffentlicht. Als Mitglied verschiedener nationaler und internationaler industrieller Beiräte und wissenschaftlicher Gremien berät sie Unternehmen, Wirtschaftsverbände sowie die öffentliche Hand in allen Fragen der IT-Sicherheit. In Fachgremien wirkt sie mit an der Gestaltung der technischen und wissenschaftlichen Rahmenbedingungen in Deutschland sowie an der Ausgestaltung von wissenschaftlichen Förderprogrammen auf EU-Ebene.