Cyber-Sicherheit

Unterstützung von Sicherheitsstrategien und –systemen in der EZ

HINTERGRUND

Weltweit erfahren Menschen, wie Digitalisierung neue Chancen durch den gewinnbringenden Zugang zu Informationen, neuen Produkten und Dienstleistungen schafft. Grundlage dafür sind verlässliche und sichere Infrastrukturen. Jedoch wird weltweit deutlich: Der digitale Wandel und seine Anwendungen und Instrumente bringen neue Verwundbarkeit und Risiken. Digitale Sicherheit wird zunehmend zur Vorbedingung für ein freies und offenes Internet, für die demokratische Verfasstheit von Staaten, für gesellschaftliche, ökonomische und politische Teilhabe sowie für prosperierende Märkte und Nationalökonomien.

In den letzten Jahren haben die Angriffe auf digitale Infrastrukturen weltweit bedeutend zugenommen und zu beachtlichen gesellschaftlichen und wirtschaftlichen Schäden geführt. Gerade in Entwicklungs- und Schwellenländern sind digitale Infrastrukturen bzw. Informations- und Kommunikationstechnologien (IKT) noch nicht ausreichend gegen Cyber-Attacken geschützt. Somit entstehen Sicherheitslücken, die nicht nur für die Wirtschaft, Zivilgesellschaft und Regierung der einzelnen Staaten fatale Folgen haben können, sondern auch für Drittstaaten wie Deutschland.

ZIELE

In Entwicklungsländern ist der Einsatz von IKT oft deutlich weitgreifender als beispielsweise in Deutschland. Die großflächige Einrichtung von Handy-Bezahlsystemen, die Einführung digitaler Steuersysteme oder Online-Bildungsangebote müssen verlässlich funktionieren, wenn sie Rückstände der jeweiligen Sektoren nachhaltig überwinden sollen. Cyber-Sicherheit ist auch eine wichtige Grundlage beim Aufbau einer Digitalwirtschaft, da digitale Geschäftsmodelle ohne IT-Sicherheit und Vertrauen der Kunden nicht erfolgreich sein können.

Viele Partnerländer haben Unterstützungsbedarf bei der (Weiter-)Entwicklung und Umsetzung eigener Cyber-Sicherheits-Strategien und -Systeme. Rückstände im Aufbau von Cyber-Kapazitäten können gerade ärmere und benachteiligte Länder und Bevölkerungsgruppen Cyber-Bedrohungen aussetzen und in ihrer Entwicklung einschränken oder zurücksetzen. Die deutsche EZ muss bei der Arbeit mit Partnerländern jedoch im Auge behalten, dass einige Staaten das Thema Cyber-Sicherheit nutzen, um Freiheiten und Rechte ihrer Bürgerinnen und Bürger mittels Zensur und Repressionen einzuschränken. Dies kann bspw. Oppositionen schwächen. Stärkung und Schutz der digitalen Sicherheit ist eine wichtige Zukunftsaufgabe der deutschen EZ, da ohne sie das Potenzial des digitalen Wandels nicht (voll) entfaltet werden kann. Cyber-Sicherheit sollte daher als Komponente in allen digitalen EZ-Projekten mitgedacht werden.

UMSETZUNG

Das Strategiepapier Digitalisierung des BMZ legt einen Fokus auf Datensicherheit und die sichere Nutzung von Daten im globalen Süden. Insbesondere im Rahmen von guter Regierungsführung sollen zudem auch die Kapazitäten der Partnerländer im Bereich Cyber-Sicherheit zukünftig gestärkt werden.

Die GIZ hat zudem „Responsible Data Guidelines“ erarbeitet und die „Digital Principles“ unterzeichnet, die Handlungsprinzipien zur Arbeit mit Daten enthalten. Die KfW hat ihrerseits ebenfalls die „Digital Principles“ unterzeichnet und eine Cyber-Sicherheits-Checkliste erstellt, die alle Vorhaben erfüllen müssen. Zudem unterliegen die Durchführungsorganisationen europäischem Recht und müssen somit seit 2019 auch die Daten-schutz-Grundverordnung umsetzen.

Herausgegeben von:

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Impressum

Herausgeber:
Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Sektorprogramm Digitalisierung für
nachhaltige Entwicklung

E-Mail: toolkit-digitalisierung@giz.de

Im Auftrag des
Bundesministeriums für wirtschaftliche
Zusammenarbeit und Entwicklung (BMZ),
Referat 112 – Digitalisierung in der EZ

Stand: 10/2019