

Alarmstufe Rot: Thüringen bereitet sich auf Cyberangriffe vor!

Thüringer Innenminister Maier und Experten diskutieren am 14.05.2025 über Cyberangriffe und Katastrophenschutz im MDR-Livestream.



Erfurt, Deutschland - Die wachsenden Bedrohungen durch Cyberangriffe und Naturkatastrophen beschäftigen zurzeit nicht nur Politiker, sondern auch IT-Experten in Deutschland. Der Thüringer Innenminister Georg Maier (SPD) hat eindringlich vor einer „Katastrophen-Amnesie“ in Teilen der Bevölkerung gewarnt. Diese Kommentare wurden im Rahmen einer Veranstaltung laut, die sich mit den Herausforderungen des Katastrophenschutzes auseinandersetzt. Albrecht Broemme, Vorstandsvorsitzender des Zukunftsforums Öffentliche Sicherheit, betont, dass 24.000 Feuerwachen und 800 THW-Liegenschaften in Deutschland bei einem Stromausfall oder Wasserversorgungsstörungen kaum betrieben werden können. Dies zeigt die Dringlichkeit der Diskussion über effektive

Krisenmanagementstrategien.

An der Veranstaltung, die am Mittwochabend um 20:15 Uhr im Livestream auf MDR.DE und im MDR FERNSEHEN übertragen wird, nehmen neben Minister Maier auch Katastrophen-Experte Broemme und IT-Expertin Sabine Griebisch teil. Griebisch warnt, dass viele Kommunen einen extremen Nachholbedarf in der IT-Sicherheit haben. Hackerangriffe könnten das Vertrauen der Bürger in Staat und Verwaltung untergraben, weswegen ein Notfallplan für Kommunen dringend erforderlich sei. Die gesamte Veranstaltung zielt darauf ab, die Vorbereitungen der Stellen für Katastrophen- und Bevölkerungsschutz auf Ernstfälle zu erörtern.

Krisenmanagement in der digitalen Ära

Die Herausforderungen im Krisenmanagement sind laut [itsicherheit-online] erheblich, insbesondere bei der Koordination von Krisenstäben und IT-Teams in Unternehmen. Seit der Corona-Pandemie und dem Ukraine-Krieg haben Krisenstäbe häufig getagt, während die Anzahl der Cyberattacken zugenommen hat. Kommunikationsbarrieren, Informationsüberflutung und unklare Entscheidungsfindungsprozesse sind nur einige der Probleme, die Unternehmen in Krisenzeiten bewältigen müssen. Es wird dringend empfohlen, klare Rollen und Verantwortlichkeiten festzulegen sowie Kommunikationsprotokolle zu standardisieren, um die interne und externe Kommunikation zu verbessern.

Um das Vertrauen der Stakeholder zu stärken und den langfristigen Erfolg zu sichern, wird die Orientierungshilfe ISO 22361:2022 empfohlen. Diese bietet umfassende Leitlinien für das Krisenmanagement, insbesondere in Bezug auf die Verbesserung der Reaktionsfähigkeit und die Einhaltung gesetzlicher Anforderungen.

Cyberkrisen-Seminare zur Stärkung der

Resilienz

Ein Seminar zur Reaktion auf Cyberkrisen, das von [fraunhofer] angeboten wird, zeigt, wie wichtig die Vorbereitung auf solche Herausforderungen ist. In diesem Seminar lernen die Teilnehmenden durch realitätsnahe Krisensimulationen, wie sie auf verschiedene Bedrohungen wie Social Media Shitstorms oder DDoS-Angriffe reagieren können. Ein bemerkenswerter Fakt ist, dass über 50% der Unternehmen und Behörden von Wirtschaftsspionage, Sabotage und Datendiebstahl betroffen sind.

Die Teilnahme an solchen Seminaren fördert nicht nur das Bewusstsein für Cyberangriffe, sondern bietet auch praktisches Handlungstraining zur Verbesserung der Krisenkommunikation und reaktionsmuster im Team. Nach der Simulation erhalten die Teilnehmenden detailliertes Feedback, welches ihnen hilft, ihre Unternehmensprozesse zu optimieren und effizienter auf Krisen zu reagieren.

Im Kontext dieser Thematik ist die Verantwortung des Bundes im Katastrophenschutz und die Notwendigkeit einer verstärkten Zusammenarbeit zwischen verschiedenen Institutionen und Fachbereichen wichtiger denn je. Beide Expertisen aus den Bereichen Katastrophenschutz und IT-Sicherheit müssen in einem ganzheitlichen Ansatz zusammengeführt werden, um die Bevölkerung bestmöglich auf Krisenszenarien vorzubereiten.

Details	
Vorfall	Cyberkriminalität
Ort	Erfurt, Deutschland
Quellen	• www.mdr.de • www.itsicherheit-online.com • www.cybersicherheit.fraunhofer.de

Besuchen Sie uns auf: n-ag.de