Cyber-Resilienz - ein Muss in der 'neuen Normalität‘

Thesenpapier von Rajesh Dhuddu
Blockchain & Cybersecurity Practice Leader, Tech Mahindra

Während die Welt mit der Pandemie beschäftigt ist und sich mit der neuen Normalität zurechtfindet, ist die Schaffung von Cyber-Resilienz von entscheidender Bedeutung, damit diese Bemühungen nicht beeinträchtigt werden.

Wir durchleben heute in der Tat sehr unvorhersehbare und herausfordernde Zeiten. Alle mussten ihr persönliches und berufliches Leben auf eine "neue Normalität" umstellen, in der Meetings nicht mehr in der physischen Welt stattfinden, in der Geschäftsstrategien über die Cloud diskutiert und umgesetzt werden, in der wir digitale und kollaborative Plattformen nutzen.

In dieser schnelllebigen Welt, in der unser Handeln von leistungsstarken und allgegenwärtigen technischen Innovationen angetrieben wird, kämpfen wir jedoch ständig mit den Herausforderungen der Informationssicherheit. Nennen Sie es die Gefahren einer globalisierten Wirtschaft, aber Tatsache bleibt, dass Cybersicherheit heute eines der wichtigsten Probleme von Unternehmen ist.

Mit der zunehmenden Nutzung von Smartphones und anderen Geräten, die uns helfen, virtuell miteinander in Verbindung zu treten, verbringen Menschen heute einen großen Teil ihrer Zeit in der Cyberwelt. Die Covid-19-Pandemie hat den Übergang in die digitale Welt nur beschleunigt, was uns noch anfälliger für Angriffe und Bedrohungen aus Cyberspace gemacht hat. Die Cyberabwehr, die in der Covid-19-Welt erforderlich ist, hat innerhalb von 0 Tagen 15 Jahre übersprungen und Unternehmen sowie Einzelpersonen in hohem Maße exponiert. Ja, Cyber-Resilienz ist das Gebot der Stunde!

Eine digitale Welt - nicht länger ein abstraktes Konzept!
Um alles nahtlos am Laufen zu halten, wird die Welt immer schneller digital – unter anderem mit mehr künstlicher Intelligenz (KI), maschinellem Lernen (ML), dem Internet der Dinge (IoT), virtueller Zusammenarbeit und Meeting-Plattformen. Während all diese Technologien Einzug gehalten haben, um uns vor der Covid-19-Pandemie zu schützen, müssen Organisationen sicherstellen, dass ihre Systeme, Prozesse, Pläne und Transaktionen sicher und vor allen Arten von Cyber-Schwachstellen geschützt sind.

Zusätzlich zu all diesen Anpassungen sind in globalen Netzwerken und Foren Gespräche über 5G im Gange, das ein enormes Potenzial in verschiedenen vertikalen Märkten freisetzen kann. Dazu zählen das Gesundheitswesen, intelligente Städte, autonome Fahrzeuge, Industrie 4.0 und das Internet der Dinge (IoT), was wiederum zu weiteren Schwachstellen in einer hyper-verbundenen Umgebung führen kann.

In dieser neuen Normalität gefährden Cyber-Angreifer die Sicherheit dieser digitalen Welt, von der wir so abhängig sind. Dem Weltwirtschaftsforum zufolge ist die Cybersicherheit die größte vom Menschen verursachte Sorge für CEOs weltweit, und es ist davon auszugehen, dass die Cybersicherheitsbranche in den kommenden Jahren erheblich wachsen wird.

Risiken reduzieren und managen

Um durch die Beseitigung von Schwachstellen Risiken einzudämmen, müssen sich Organisationen auf die Stärkung von End-to-End-Cyber-Sicherheitsstandards konzentrieren und eine robuste Sicherheitsinfrastruktur implementieren.

Zwar hat die Pandemie den Fußabdruck von Angriffen von außen vergrößert, doch kann die Bedrohung auch von innen kommen. Daher sollten sich Organisationen mit einer Zero-Trust-Network-Architektur befassen. Das heißt, es muss eine strenge Zugangskontrolle gegeben sein, da Vertrauen eine Schwachstelle innerhalb der Organisation sein kann.

Und da immer mehr Anwendungen in die Cloud verlagert werden, ist auch eine Mikrosegmentierung erforderlich, d.h. die logische Aufteilung des Netzwerks in verschiedene isolierte Sicherheitssegmente bis hinunter zur individuellen Arbeitslast und die anschließende Definition von Sicherheitskontrollen und -diensten für jedes einzelne Segment.

Die Containerisierung ist eine weitere Möglichkeit, Systeme zu sichern – sowohl eine einzelne Anwendung wie auch die Ressourcen, um sie im selben virtuellen Paket auszuführen. Abgesehen von all diesen Maßnahmen ist eine grundlegende Security-Hygiene unter den Nutzern, wie häufiges Ändern von Passwörtern und Vermeiden von zweifelhaften Links und ähnlichen Dingen, ein Muss.

Priorität muss die Sensibilisierung der Mitarbeiter für Cyber-Bedrohungen, z.B. Phishing-Angriffe, haben. Darüber hinaus gilt es, die Endgerätesicherheit (d.h. Einsatz und Aktualisierung von Antiviren- und Antispam-Software) zu fördern, das Threat-Management regelmäßig zu evaluieren und den Mitarbeitern verständlich zu machen, dass Cloud und SaaS (Software as a Service) dauerhaft bleiben werden. Daher ist es notwendig, aktiv Sicherheitsplattformen zu nutzen, die den Endnutzern robusten Cyberschutz und hohe Leistung bieten können.

Einzelpersonen sowie kleine und mittlere Unternehmen (KMUs) sind am schlechtesten ausgestattet und müssen in Sicherheitsfragen geschult werden. Organisationen müssen ihre Mitarbeiter auch in der Multi-Faktor-Authentifizierung weiterbilden, sie davor warnen, unnötige Software herunterzuladen, und ihnen die Gewohnheit einprägen, Geräte routinemäßig zu aktualisieren und zu patchen sowie auch Heimrouter mit der neuesten Firmware zu aktualisieren. Unternehmen müssen darauf bestehen, dass sich Mitarbeiter strikt an die Regeln des Mobile Device-Management der Organisation halten.

Denn kein Verbrechen wächst schneller als die Cyber-Kriminalität, da sie für die Angreifer sehr lukrativ ist. Und die Cyber-Kriminalität hat sich während der Pandemie aufgrund der sich vervielfachenden Schwachstellen extrem beschleunigt. Laut einer Studie von Cybersecurity Ventures wird Cyber-Kriminalität Unternehmen auf der ganzen Welt bis 2021 jährlich 6 Billionen Dollar kosten, gegenüber 3 Billionen Dollar im Jahr 2015. Während sich die Welt mit der Pandemie und der neuen Normalität zurechtfindet, ist die Schaffung von Cyber-Resilienz essentiell, um diese Bemühungen nicht zu gefährden.

Rajesh Dhuddu

Rajesh Dhuddu leitet die Blockchain & Cybersecurity Practice bei Tech Mahindra. Mit einem Team von mehr als 500 Cybersicherheitsexperten unterstützt er globale Kunden in EMEA, Asien-Pazifik & Japan sowie Indien dabei, ihre unternehmensweite Cybersicherheit zu stärken und eine hoch belastbare Sicherheitsorganisation aufzubauen. Er arbeitet eng mit Chief Information Security Officers zusammen und berät sie beim Einsatz von Best Practices hinsichtlich Technologien wie auch Betrieb von Cloud Security, Netzwerksicherheit, Advance Threat Management, Zero Trust, Offensive Security, Cyber-Risk-Quantification & SASE (Secure Access Service Edge). Lattice80 hat Rajesh in Anerkennung seiner Beiträge in den letzten fünf Jahren als einen der 100 besten Blockchain-Influencer der Welt aufgeführt. Thinkers360 hat ihn in der Top-3-Liste der Blockchain-Influencer weltweit anerkannt.

Er ist sowohl für Cybersecurity als auch für Blockchain Teil des Expertennetzwerks des Weltwirtschaftsforums, das weltweit nur 5000 ausgewählte Personen im Bereich neue Technologien umfasst. Außerdem ist er Gründungsvorsitzender der Blockchain Special Interest Group bei Nasscom (National Association of Software and Services Companies, Neu-Delhi, Indien).

###

Über Tech Mahindra

Mit seinen innovativen und kundenzentrierten Informationstechnologie-Services und -Lösungen für Unternehmen, Mitarbeiter und die Society to Rise™ steht Tech Mahindra für die vernetzte Welt. Das Unternehmen mit einem Umsatz von 5,2 Mrd. US-Dollar und über 124.500 Experten in 90 Ländern unterstützt 988 Kunden weltweit, darunter einige Fortune-500-Unternehmen. Die konvergenten, digitalen Design-Erfahrungen, Innovationsplattformen und wiederverwendbaren Assets verbinden eine Reihe von Technologien, mit denen das Unternehmen greifbaren Mehrwert und Erfahrungen für seine Stakeholder liefert. Tech Mahindra wurde vom Great Place to Work®-Institut 2020 als eines der 50 besten indischen Unternehmen anerkannt.

Tech Mahindra gehört zur Mahindra Group, die mit mehr als 240.000 Mitarbeitern in über 100 Ländern 21 Mrd. US-Dollar Umsatz erwirtschaftet. Der Konzern ist in wachstumsstarken Schlüsselindustrien tätig und nimmt eine führende Position in den Bereichen Traktoren, Nutzfahrzeuge, Aftermarket, Informationstechnologie und Ferienimmobilien ein.

In Deutschland ist Tech Mahindra mit rund 800 Mitarbeitern an zehn Standorten vertreten und bedient Kunden branchenübergreifend.

Folgen Sie uns auf https://www.techmahindra.com/de-de/ || Social Media

Für weitere Informationen kontaktieren Sie bitte:

Mark Roper, Head of Marketing - Europe
Mobile: +44 (0)7768 233334, **Email:** Mark.Roper@TechMahindra.com

Petra Röhrl, Agentur Lorenzoni GmbH, Public Relations
Tel: +49 8122 55917-14
E-Mail: petra@lorenzoni.de || www.lorenzoni.de