

Fujitsu warnt vor Desinformationskampagnen

Auf einen Blick:

- Desinformationskampagnen zielen darauf ab, Panik und Angst in der Gesellschaft auszunutzen oder zu verbreiten
- Fujitsu geht davon aus, dass sowohl Unternehmen als auch Einzelpersonen angesprochen werden, basierend auf den Themen, die aktuell einen breiten Teil der Gesellschaft betreffen – wie Pflichtimpfungen, Gesundheitspässe und Lockdowns
- Hinter diesen Angriffen stecken kriminelle Banden und Nationalstaaten, die vor allem versuchen, Maßnahmen gegen die Verbreitung von Falschinformationen zu schwächen

Wien, 19. Januar 2021 – Fujitsu weist auf die Gefahren von Verbreitung von Falschinformationen hin, die sich auf die Coronavirus-Pandemie beziehen. Cyberkriminelle haben zuletzt aktuelle Themen wie den Brexit und die Wahlen ausgenutzt. Jetzt konzentrieren sie sich auf Themen, die einen breiten Teil der Gesellschaft betreffen. Auf umstrittene Fragen im Hinblick auf die persönliche Freiheit, wie die Verpflichtung zum Tragen eines Mundschutzes, die Einschränkung der Bewegungsfreiheit oder die Wirksamkeit von Impfstoffen.

Fujitsu geht davon aus, dass sich Desinformationskampagnen zur Verbreitung von Angst, Unsicherheit und Zweifel auf die Wirksamkeit von Coronavirus-Impfstoffen fokussieren und für Social-Engineering-Angriffe eingesetzt werden. Die raffiniertesten dieser Angriffe werden beide Seiten gegeneinander ausspielen - unter Ausnutzung der Grundüberzeugungen der Menschen. Dies könne das Vertrauen in Informationsquellen ins Wanken bringen und sich auf Unternehmensmarken auswirken, die in das Kreuzfeuer geraten.

Laut Fujitsu richten sich diese Kampagnen sowohl an Unternehmen als auch Einzelpersonen. Die Cybersecurity-Experten von Fujitsu rechnen mit Multi-Vektor-Angriffen, die sowohl von kriminellen Banden als auch von Nationalstaaten ausgehen und die Länder ins Visier nehmen werden, die bereits versuchen, sich gegen gezielte Desinformationskampagnen zu wehren.

Phishing im Mittelpunkt von Desinformationskampagnen

Paul McEvatt, Head of Cyber Security Innovation bei Fujitsu, kommentiert: „Phishing steht im Zentrum dieser Angriffe. Menschen fallen eher auf Phishing-Angriffe herein, die ein Thema ansprechen, an das sie glauben oder mit dem sie sich identifizieren. Heute ist die Coronavirus-Pandemie ein globales Thema. Und ein hochemotionales dazu, zumal es um persönliche Freiheiten und Faktoren wie Bewegungseinschränkungen geht.“

Im Laufe des Jahres 2020 hat Fujitsu mehrere Beispiele verfolgt, bei denen versucht wurde, gesellschaftliche Probleme und deren Lösungen auszunutzen, um Falschinformationen zu verbreiten. Im vergangenen April meldete das [National Cyber Security Centre](#) in Großbritannien 2.000 aufgedeckte Betrugsversuche. Darunter 471

gefälschte Online-Shops, die versuchten, Menschen zu täuschen, die nach Dienstleistungen im Zusammenhang mit dem Coronavirus suchen, sowie 200 weitere Phishing-Seiten. Im März 2020 meldete das Sicherheitsunternehmen [Check Point](#) einen sprunghaften Anstieg der Registrierungen von Domain-Namen, die mit Zoom in Verbindung stehen. Cyberkriminelle rechneten mit einer steigenden Nachfrage nach Online-Konferenzdiensten und nutzten dies aus, indem sie ähnliche Domains kauften, um sie für Credential-Phishing zu verwenden.

Arbeit im Homeoffice macht Mitarbeiter anfälliger für Cyberangriffe

Fujitsu stellt fest, dass längere Phasen des Arbeitens von zu Hause Mitarbeiter anfälliger dafür machen, auf Phishing-Angriffe hereinzufallen. Fujitsu empfiehlt Unternehmen, drei wesentliche Gegenmaßnahmen zu ergreifen:

1. **Mitarbeiter befähigen, mit Cyberangriffen umzugehen:** Dabei geht es nicht nur darum, Mitarbeiter darin zu schulen, Cyberangriffe zu erkennen, sondern auch sicherzustellen, dass sie sich befähigt fühlen, jede E-Mail kritisch zu bewerten und sie schnell und ohne Angst vor Schuldzuweisungen zu melden.
2. **Bedrohungen verstehen:** Threat Intelligence ist ein bedeutender Teil der Sicherheit eines jeden Unternehmens. IT-Sicherheitsteams verstehen und mindern damit potenzielle Bedrohungen, bevor sie zu einem Risiko werden.
3. **Automatisieren:** Ein Blick auf das Ausmaß und die rasante Entwicklung dieser Bedrohungen zeigt, dass 2021 ein noch arbeitsreicheres Jahr für IT-Sicherheitsteams wird. Die Automatisierung von Sicherheitsprozessen verschafft IT-Sicherheitsteams einen Vorteil gegenüber diesen Bedrohungen. Außerdem können sie so reale Bedrohungen und einen umfassenderen Kontext untersuchen, um sicherzustellen, dass sie wissen, womit sie es zu tun haben.

Weitere Informationen finden sie in der neuen [Cyber Security Prediction Broschüre](#).

Weitere Informationen über Fujitsu erhalten Sie über

- Fujitsu Aktuell: <http://www.fujitsu.com/de/fujitsuaktuell>
- Twitter: https://twitter.com/Fujitsu_DE
- LinkedIn: <http://www.linkedin.com/company/Fujitsu>
- Facebook: <http://www.facebook.com/Fujitsu.DE>
- Fujitsu Bildmaterial und Media Server: https://mediaportal.ts.fujitsu.com/pages/dk_home.php
- Fujitsu Newsroom: <http://de.Fujitsu.com/newsroom>

Pressekontakt:

ikp Wien GmbH
Ines Schmied-Binderlehner
Tel.: +43 1 524 77 90-24
fujitsu@ikp.at

Über Fujitsu

Fujitsu ist der führende japanische Anbieter von Informations- und Telekommunikations-basierten (ITK) Geschäftslösungen und bietet eine breite Palette an Technologieprodukten, -lösungen und -dienstleistungen. Mit rund 130.000 Mitarbeitern betreut das Unternehmen Kunden in mehr als 100 Ländern. Fujitsu nutzt seine ITK-Expertise, um die Zukunft der Gesellschaft gemeinsam mit seinen Kunden zu gestalten. Im Geschäftsjahr 2019 (zum 31. März 2020) erzielte Fujitsu Limited (TSE:6702) mit Hauptsitz in Tokio, Japan, einen konsolidierten Jahresumsatz von 3,9 Billionen Yen (35 Milliarden US-Dollar). <http://www.fujitsu.at>

Fujitsu in Deutschland, Österreich und der Schweiz

Fujitsu unterstützt als führender Informations- und Telekommunikations-Komplettanbieter seine Kunden bei allen Aspekten der digitalen Transformation. Dafür kombiniert das Unternehmen IT-Dienstleistungen und Produkte mit zukunftsweisenden digitalen Technologien – wie Künstlicher Intelligenz (KI), dem Internet der Dinge (IoT), Blockchain, Analytics, Digital Annealing sowie Cloud- und Sicherheitslösungen – und schafft zusammen mit seinen Kunden und Partnern neue Werte. Das Produkt- und Service-Angebot kann passgenau auf die individuellen Bedürfnisse zugeschnitten werden – von der Konzeption bis hin zur Implementierung, dem Betrieb und der Orchestrierung von digitalen Ökosystemen.

In Deutschland, Österreich und der Schweiz hat Fujitsu rund 5.000 Beschäftigte und verfügt mit über 10.000 Channel-Partnern allein in diesen drei Ländern zudem über eines der leistungsfähigsten Partnernetzwerke der Branche. <http://www.fujitsu.com/de>