PRESSEINFORMATION

2019 Global Threat Intelligence Report: Der Finanzsektor kehrt in EMEA an die Spitze der am stärksten von Angriffen betroffenen Branchen zurück

AU ZH, Schweiz, 9. April 2019 – NTT Security, das auf Sicherheit spezialisierte Unternehmen und „Security Center of Excellence“ der NTT Group (NYSE: NTT), hat seinen Global Threat Intelligence Report (GTIR) 2019 veröffentlicht. Der neue GTIR zeigt, dass der Finanzsektor in EMEA die am häufigsten angegriffene Branche ist. 30% aller Attacken entfallen auf Finanzunternehmen, im Vergleich zu 17% weltweit. Damit hat die Finanzbranche in EMEA den Bereich Business und Professional Services vom ersten Platz verdrängt, der im letzten Jahr mit 20% der am stärksten angegriffene Sektor war**.**

Für den GTIR 2019 hat NTT Security Daten aus Billionen Logs und Milliarden Angriffen ausgewertet. Die Analyse basiert auf Informationen über Logs, Events, Angriffe, Vorfälle und Schwachstellen, die von allen Unternehmen der NTT Group gesammelt wurden. Der neue Bericht gibt wie gewohnt einen Überblick über die globalen Bedrohungstrends für insgesamt 18 Branchen.

Die GTIR 2019 zeigt, dass neben der Finanzbranche der Bereich Business und Professional Services (24%), der Technologiesektor (17%) und die Fertigungsindustrie (9%) zu den am stärksten betroffenen Branchen in EMEA gehören. Schuld daran sind vor allem Angriffe auf Webanwendungen, die über 43% der feindlichen Aktivitäten ausmachen und damit deutlich über dem weltweiten Durchschnitt von 32% liegen.

Die Finanzindustrie in EMEA verzeichnete dabei einen rapiden Anstieg der Web-Application-Attacken, die sich im vergangenen Jahr von 22% auf 43% fast verdoppelt haben. Eine massive Zunahme erlebte hier auch der Manufacturing-Bereich von vormals 9% auf 42%.

„Die Finanzbranche ist wieder einmal an der Spitze, wenn es um gezielte Angriffe geht. Diese Tatsache sollte genügen, um das Management davon zu überzeugen, dass Investitionen in die Cyber-Sicherheit ein absolutes Muss sind. Viele Finanzunternehmen bewegen sich zwar mit der digitalen Transformation vorwärts, leider aber ohne integrierte Sicherheit”, erklärt Kai Grunwitz, Senior Vice President EMEA bei NTT Security. „Während Legacy-Methoden und -Tools immer noch eine solide Grundlage für die Eindämmung von Angriffen bieten, werden von Kriminellen ständig neue Angriffsmethoden entwickelt. Die Security-Verantwortlichen sollten deshalb sicherstellen, dass der grundlegende Schutz stimmt, sie müssen aber auch an innovative Lösungen denken, wenn diese einen echten Mehrwert bieten.“

„Einige der am weitesten verbreiteten Hacker-Aktivitäten in EMEA im vergangenen Jahr waren Web-Application-Angriffe – und das ist nicht überraschend. Diese Angriffe beruhen in den meisten Fällen auf der Ausnutzung offener, nicht gepatchter Schwachstellen oder falsch konfigurierter Systeme und richten sich an Unternehmen mit hohem Aufkommen an geschäftskritischen Daten. Die Folgen können verheerend sein, den Unternehmen drohen finanzielle Einbussen und

Wirtschaftsspionage. Der GTIR verdeutlicht einmal mehr, dass kritische Schwachstellen – ob nun altbekannte oder neue – in Unternehmen so schnell wie möglich behoben werden müssen, insbesondere angesichts der Konvergenz der IT mit der Operational Technology."

In der Liste der Länder, von denen Angriffe ausgehen, ist China im diesjährigen GTIR um fast 40% auf 13% gefallen – und liegt damit hinter den Vereinigten Staaten mit 16%. Interessanterweise wurden die Top Five der am häufigsten in EMEA attackierten Branchen direkt aus der Region (75%) und nicht aus anderen Ländern angegriffen. Das zeigt, Cyber-Kriminelle nutzen regionale Quellen für ihre Angriffe. Die Tatsache, dass der Grossteil aus derselben Region und oft sogar aus demselben Land wie das Opfer kommt, ist in EMEA stärker ausgeprägt als in anderen Regionen.

Der GTIR 2019 bietet Unternehmen einen umfassenden Überblick über die heutige Cyber-Bedrohungslandschaft und ist unter folgendem Link verfügbar: www.nttsecurity.com/GTIR2019-CH.

Weitere Zitate

Fumitaka Takeuchi, Security Evangelist, Vice President, Managed Security Service Taskforce, Corporate Planning bei NTT Communications: „Viele Unternehmen kaufen Sicherheitslösungen für Probleme, die es eigentlich gar nicht gibt, oder Lösungen, die mehr kosten als ein potenzieller Verlust überhaupt ausmacht. Unser Rat für Unternehmen, unabhängig von der Branche, ist deshalb, auf vertrauenswürdige Experten im Cyber-Security-Bereich zu setzen und die Managed Service Maturity im Blick zu haben. In erster Linie ist es wichtig zu wissen, wo die tatsächlichen Risiken liegen, und dann entsprechende Lösungen umzusetzen."

Stefaan Hinderyckx, Senior Director Security Europe bei Dimension Data: „Der diesjährige GTIR zeigt deutlich, dass sich Angriffe auf die Cyber-Sicherheit ständig weiterentwickeln. Auch wenn das Volumen teilweise stagniert, gibt es dauernd neue Bedrohungen. 2018 war ein Rekordjahr, in dem so viele neue Schwachstellen wie nie zuvor identifiziert und gemeldet wurden. Die NTT Group arbeitet seit 15 Jahren mit Unternehmen zusammen, um sie bei der Abwehr der sich ständig weiterentwickelnden und immer komplexer werdenden Bedrohungslandschaft zu unterstützen. Das Erkennen von Bedrohungen hilft unseren Kunden, potenzielle Angriffe in der digitalen Welt vorherzusagen und zu minimieren."

Dieter Loewe, Managing Director Sales and Markets bei NTT DATA für EMEA: „Der Threat Report zeigt, dass die Vielfalt der Angriffe nicht so gross ist, wie es scheint, während die USA und China aber oftmals als die häufigsten Quellen identifiziert werden. Wenn besonders betroffene Branchen wie Finanzdienstleister ihre Unternehmen vor einfallsreichen Cyber-Kriminellen schützen, müssen die Führungskräfte mehr denn je eine absolut sichere Infrastruktur vom Endpunkt bis zum Kern gewährleisten, die es ihnen ermöglicht, sich auf den täglichen Betrieb zu konzentrieren."

Die Methodik des Global Threat Intelligence Report (GTIR)

Der NTT Security Global Threat Intelligence Report 2019 enthält globale Angriffsdaten, die von NTT Security und anderen Tochterunternehmen der NTT Group zwischen dem 1. Oktober 2017 und dem 30. September 2018 gesammelt wurden. Die Analyse basiert auf Informationen von Kunden über Logs, Events, Angriffe, Vorfälle und Schwachstellen. Der Report berücksichtigt zudem Forschungsergebnisse von NTT Security, die unter anderem von Honeypots und Sandboxes in über 100 Ländern stammen. Damit erhält NTT Security Einblicke in Umgebungen, die sich grundsätzlich von den Infrastrukturen in Sicherheitslaboren und Forschungseinrichtungen unterscheiden.

Für den GTIR 2019 hat NTT Security Daten aus Billionen Logs und Milliarden Angriffen ausgewertet. NTT Security sammelt Informationen über Logs, Events, Angriffe, Vorfälle und Schwachstellen, reichert diese um Kontextinformationen an und analysiert die kontextangereicherten Daten. Dadurch ist eine globale Bedrohungsaufklärung und Alarmierung in Echtzeit möglich. Aufgrund der Grösse und Vielfalt des Kundenstamms mit über 10.000 Kunden auf sechs Kontinenten liefert NTT Security Informationen, die für die Bedrohungen der meisten Unternehmen repräsentativ sind.

Die Daten stammen aus weltweiten Log-Events, die Angriffe basierend auf Art oder Menge identifizieren. Die Verwendung von validierten Informationen im Gegensatz zum Rohvolumen von Protokolldaten oder des Netzwerkverkehrs erfasst die tatsächliche Angriffszahl genauer. Ohne eine angemessene Kategorisierung der Angriffe würde das überproportional grosse Datenvolumen aus der Netzwerk-Traffic-Überwachung, Fehlalarmen, autorisiertem Security-Scanning und grossen DDoS-Fluten, die von Security Operations Centers (SOCs) überwacht und erfasst werden, die tatsächliche Häufigkeit von Angriffen verfälschen.

Die Einbeziehung von Daten aus den zehn SOCs und sieben Forschungs- und Entwicklungszentren von NTT Security liefert eine präzise Darstellung der sich ständig weiterentwickelnden globalen Bedrohungslandschaft.

Über NTT Security

NTT Security ist das auf Sicherheit spezialisierte Unternehmen und „Security Center of Excellence“ der NTT Group. Mit „Embedded Security“ bietet NTT Security Kunden zuverlässige Lösungen für ihre Anforderungen in der digitalen Transformation. NTT Security verfügt über 10 SOCs, sieben Zentren für Forschung und Entwicklung sowie mehr als 1.500 Sicherheitsexperten und behandelt jährlich Hunderttausende Sicherheitsvorfälle auf sechs Kontinenten.

NTT Security sichert eine effiziente Ressourcennutzung, indem Kunden der richtige Mix an ganzheitlichen Managed Security Services, Security Consulting Services und Security-Technologie zur Verfügung gestellt wird – unter optimaler Kombination von lokalen und globalen Ressourcen. NTT Security ist Teil der NTT Group (Nippon Telegraph and Telephone Corporation), einem der grössten IKT-Unternehmen weltweit. Weitere Informationen über NTT Security finden sich unter www.nttsecurity.com/ch. Informationen zur globalen NTT Group finden sich unter www.ntt-global.com.

Bei Rückfragen wenden Sie sich bitte an:

NTT Security

Romy Däweritz
Marketing Manager DACH
Tel.: +41 43 477 70 10
romy.daeweritz@nttsecurity.com hakan.cakar@nttsecurity.com

PR-COM GmbH

Franziska Fricke
Account Management
Tel.: +49 (0) 89 59997 707
franziska.fricke@pr-com.de