25.04.2017 – 10:03 Uhr

NTT Security stellt Global Threat Intelligence Report 2017 vor: 77 Prozent der Ransomware in vier Branchen

Schweiz (ots/PRNewswire) -

NTT Security (Switzerland) AG, Teil der NTT Group (NYSE: NTT) und Spezialist für Informationssicherheit und Risikomanagement, hat den Global Threat Intelligence Report (GTIR) 2017 vorgestellt. Der Bericht zeigt unter anderem, dass 77% der gefundenen Ransomware auf die vier Sektoren Business und Professional Services, öffentliche Verwaltung, Gesundheitswesen und Einzelhandel entfielen. Phishing-Angriffe sind für drei Viertel der vorhandenen Malware verantwortlich und für ein Drittel aller Authentifizierungsversuche werden lediglich 25 verschiedene Passwörter genutzt.

Der Global Threat Intelligence Report (GTIR) 2017 analysiert Daten der Tochterunternehmen der NTT Group, einschliesslich NTT Security, Dimension Data, NTT Communications und NTT Data sowie dem Global Threat Intelligence Center (GTIC, ehemals SERT), illustriert die Trends in den Bereichen Ransomware, Phishing und DDoS-Angriffe und zeigt, welche Auswirkungen die aktuellen Bedrohungen auf Unternehmen in aller Welt haben. Die Analyse basiert auf Logdateien und Daten zu Angriffen, Vorfällen und Schwachstellen im Zeitraum Oktober 2015 bis September 2016.

Zur Verbreitung von Ransomware - die den Zugriff auf Daten oder Geräte durch berechtigte Benutzer verhindert - wird heute hauptsächlich Phishing verwendet. Der Report zeigt, dass 77% der weltweit gefundenen Ransomware auf nur vier Branchen entfiel: Business und Professional Services (28%), öffentliche Verwaltung (19%), Gesundheitswesen (15%) und Einzelhandel (15%).

Auch wenn in den Medien vor allem die technisch raffinierten Angriffe auf die neuesten Schwachstellen thematisiert werden, sind viele Angreifer nach wie vor mit ganz einfachen Methoden erfolgreich. Laut GTIR lassen sich beinahe drei Viertel (73%) der Malware in Unternehmen auf Phishing-Angriffe zurückführen, wobei auf globaler Ebene der öffentliche Sektor (65%) sowie Business und Professional Services (25%) die meisten Angriffe verzeichnen. Eine Aufschlüsselung nach Ländern belegt, dass die meisten Phishing-Angriffe von den USA (41%), den Niederlanden (38%) und Frankreich (5%) ausgehen.

Der Report zeigt ausserdem, dass für fast 33% aller Authentifizierungsversuche bei den von NTT Security installierten Honeypots lediglich 25 verschiedene Passwörter genutzt wurden. Bei mehr als 76% der Anmeldeversuche wurde ein Passwort genommen, das im Botnetz Mirai implementiert ist - einem IoT-Botnetz, das für den bisher grössten Distributed-Denial-of-Service (DDoS)-Angriff genutzt wurde.

Auf DDoS-Angriffe gingen weltweit weniger als 6% aller Cyber-Angriffe zurück. Bei den Angriffen aus Asien waren es jedoch 16% und aus Australien sogar 23%.

Auf das Finanzwesen entfielen 14% aller globalen Angriffe, das damit der am häufigsten betroffene Sektor war. Er belegte dementsprechend als einzige Branche in allen analysierten geografischen Regionen einen der ersten drei Plätze, Manufacturing zählte in fünf der sechs Regionen zu den Top-Drei. Finanzsektor (14%), öffentliche Verwaltung (14%) und Manufacturing (13%) waren am häufigsten von Angriffen betroffen.

"Der GTIR ist der umfangreichste Bericht seiner Art", sagt Steven Bullitt, Vice President Threat Intelligence & Incident Response, GTIC, NTT Security. "Wir unterstützten Unternehmen bei der Untersuchung von Eindringversuchen, sammelten und analysierten globale Threat Intelligence und stellten eigene Nachforschungen zum Thema Sicherheit an. Diese Erkenntnisse flossen direkt in die Empfehlungen in diesem Bericht ein."

"Wir möchten Cyber-Sicherheit für jeden, der von diesem Thema betroffen ist, und nicht nur für Sicherheitsexperten, interessant und verständlich machen", so Bullitt weiter. "Jeder sollte über diese Probleme im Bilde sein, sich seiner persönlichen Verantwortung für den Schutz seines Unternehmens bewusst sein und auch wissen, dass das Unternehmen verpflichtet ist, ihn dabei zu unterstützen, seinen Beitrag zur Sicherheit des Unternehmens zu leisten."

Mehr Informationen über die wichtigsten globalen Bedrohungen und die Aktionen, mit denen Management, technische Mitarbeiter und Benutzer die Sicherheit verbessern können, enthält der Report NTT Security GTIR 2017, den Interessierte unter folgendem Link herunterladen können: http://www.nttcomsecurity.ch/downloads/GTIR-2017

Zusammenfassung weiterer wichtiger Ergebnisse

- Die meisten Angriffe gingen von folgenden Ländern aus: USA (63%), Grossbritannien (4%), China (3%);

- 32% der Unternehmen verfügten über einen offiziellen Incident-Response-Plan - in den Vorjahren lag dieser Wert lediglich bei durchschnittlich 23%;

- 59% der Incident-Response-Einsätze entfielen auf vier Branchen: Gesundheitswesen (17%), Finanzwesen (16%), Business und Professional Services (14%) und Einzelhandel (12%);

- Über 60% der Incident-Response-Einsätze hatten mit einem Phishing-Angriff begonnen;

- Bei 22% aller Incident-Response-Einsätze müssen Ransomware-Angriffe - die häufigste 2016 beobachtete Angriffsform - abgewehrt werden;

- Bei 56% aller Sicherheitsvorfälle im Finanzwesen spielte Malware eine Rolle;

- Bei 50% aller Sicherheitsvorfälle in Einrichtungen des Gesundheitswesens spielte Ransomware eine Rolle.

NTT Security beobachtet 40% des weltweiten Internet-Datenverkehrs. Für den Global Threat Intelligence Report (GTIR) 2017 wurden 3,5 Billionen Logdateien und 6,2 Milliarden Angriffe ausgewertet. Analysiert wurden Logdateien sowie Informationen über Schwachstellen, Angriffe und andere Sicherheitsvorfälle. Berücksichtigt werden ausserdem 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.

Über NTT Security

NTT Security ist das auf Informationssicherheit und Risikomanagement spezialisierte Unternehmen der NTT Group (Nippon Telegraph and Telephone Corporation), einem der grössten IKT-Unternehmen weltweit. Der Experte für IT-Security steht für ein ganzheitliches Sicherheitskonzept und die Bereitstellung ausfallsicherer Lösungen, die den Anforderungen der Kunden vor dem Hintergrund des digitalen Wandels gerecht werden. Mit zehn globalen SOCs, sieben Zentren für Forschung und Entwicklung sowie mehr als 1.500 Sicherheitsexperten unterstützt NTT Security Unternehmen auf sechs Kontinenten bei der Reaktion auf Hunderttausende Sicherheitsvorfälle pro Jahr.

NTT Security bietet Kunden die richtige Mischung aus Beratung, Managed Services und Technologien, indem lokales Know-how optimal mit globalen Ressourcen kombiniert wird. Weitere Informationen finden sich unter http://www.nttcomsecurity.ch

Bei Rückfragen wenden Sie sich bitte an:

Kontakt:

NTT Security:
Hakan Cakar
Director Marketing, Central Europe
Tel.: +49 (0) 89 94 57 32 34
hakan.cakar@nttsecurity.com
Ansprechpartner:
Hanna Greve
Account Director
PR-COM Beratungsgesellschaft für strategische Kommunikation mbH
Tel.: +49 (0) 89 59997 756
hanna.greve@pr-com.de