

26.04.2018 - 15:00 Uhr

## NTT Security analysiert Bedrohungslage: starker Anstieg der Angriffe auf den Finanzsektor

Schweiz (ots) -

NTT Security, das auf Sicherheit spezialisierte Unternehmen und "Security Center of Excellence" der NTT Group (NYSE: NTT), hat seinen Global Threat Intelligence Report (GTIR) für das Jahr 2018 veröffentlicht. Die Ergebnisse zeigen, dass der Anteil der Angriffe auf den Finanzsektor im Vergleich zum Vorjahr von 14% auf 26% gestiegen ist. Die Erkennung von Ransomware nahm um erstaunliche 350% zu; sie war 2017 für 7% der weltweiten Malware verantwortlich.

Auf der Grundlage der Überwachung von 40% des weltweiten Internetverkehrs hat NTT Security für den GTIR 2018 Daten aus mehr als 6,1 Billionen Logs und 150 Millionen Angriffen gesammelt. Der GTIR 2018 basiert auf Informationen über Logs, Events, Angriffe, Vorfälle und Schwachstellen aus allen Unternehmen der NTT Group und gibt einen Überblick über die neuesten Trends von Ransomware-, Phishing- und DDoS-Angriffen.

Der Report zeigt, dass das Volumen von Angriffen auf den Technologiesektor um 25% anstieg und damit 19% aller Angriffe auf diesen Sektor entfallen; er ist damit der einzige, der in jeder geographischen Region (Amerika, Asien, EMEA und Japan sowie weltweit) zu den fünf am stärksten angegriffenen Sektoren gehört. Dagegen verloren Angriffe auf Ziele im Öffentlichen Sektor an Priorität und fielen auf nur 5% zurück. In vier der fünf analysierten Regionen gehörten Finanzen, Einzelhandel und Produktion zu den fünf am stärksten angegriffenen Sektoren.

Der Wandel dominiert die weltweite Cyber-Security-Landschaft; so ergaben sich Verschiebungen zwischen Angriffszielen, -quellen, -profilen und den Arten der angegriffenen Technologien. Der Anstieg der erkannten Ransomware um 350% zeigt die immer zuverlässigeren Schadprogramme, die von Angreifern entwickelt wurden. So hat zum Beispiel WannaCry mit 400.000 betroffenen Computern in 150 Ländern innerhalb nur eines Tages einen neuen Standard für die Verbreitungsgeschwindigkeit gesetzt. Auch die Angriffsfläche wird immer grösser; angetrieben vor allem durch neue Cloud- und Mobilitätslösungen.

Weltweit überragten Spyware oder Keylogger mit 26% die Liste der entdeckten Malware und zählten auch zu den häufigsten Angriffsformen im Finanzsektor. Dies zeigt, dass Angreifer langfristig auf der Suche nach Informationen sind. An zweiter Stelle lagen Trojaner beziehungsweise Dropper mit 25%, an dritter Stelle Viren und Würmer mit 23%.

Im Gegensatz zu den beobachteten Veränderungen gibt es auch Konstanten: Cyber-Kriminelle nutzen regionale Quellen für Angriffe und das schnelle Erkennen von Angriffen bleibt eine der grössten Herausforderungen. Die von NTT Security gesammelten Daten zeigen global wie regional, dass eine erhebliche Anzahl von Angriffen aus derselben Region und oft sogar aus demselben Land wie das Opfer kommen, obwohl der Angreifer selbst seine Angriffe typischerweise von woanders ausführt. Während beispielsweise die Niederlande in jeder Region zu den sechs grössten Angriffsquellen gehört, ist es sehr wahrscheinlich, dass Cyber-Kriminelle lediglich spezielle Ressourcen in den Niederlanden für ihre Angriffe nutzen. Kompromittierte Systeme, angekauftes Hosting, ausgelagerte Exploit-Kits und Botnets erleichtern es Angreifern, auf lokale Ressourcen zuzugreifen und ihre Spuren zu verwischen.

"Der GTIR zeigt, wie schwierig es für Unternehmen ist, ein optimales Gleichgewicht zwischen betrieblicher Sicherheit und Compliance zu erreichen", erklärt Jon Heimerl, Senior Manager des Threat-Intelligence-Communication-Teams beim Global Threat Intelligence Center bei NTT Security. "Wer erfolgreich sein will, darf sich nicht zurücklehnen, sondern muss sich darüber im Klaren sein, dass Sicherheit ein wesentlicher Bestandteil des täglichen Business ist. In einer sich ständig weiterentwickelnden Bedrohungslandschaft ist die Verteidigung eines Unternehmens keine einfache Aufgabe und muss sich auf die in unserem Bericht beschriebenen Schlüsselbereiche konzentrieren. Dazu gehören Incident-Response-Pläne, starke Authentifizierung, umfassendes und zuverlässiges Patchen und praktisch nutzbare, aber effektive Sicherheitsmassnahmen. All das trägt dazu bei, die Sicherheit eines Unternehmens zu festigen."

Der NTT Security 2018 GTIR enthält weitere Informationen über die wichtigsten weltweiten Bedrohungen und Gegenmassnahmen, mit denen Techniker und Benutzer die Sicherheit verbessern können; der Report ist unter folgendem Link verfügbar: [www.nttsecurity.com/gtir-ch](http://www.nttsecurity.com/gtir-ch)

Weitere Ergebnisse des Global Threat Intelligence Report 2018:

- Die wichtigsten Länder, von denen Angriffe ausgehen, sind USA mit 27%, China mit 19% und die Niederlande mit 4%;
- Ransomware stieg von einem Anteil von 1% an der weltweiten Malware (GTIR 2017) auf nunmehr fast 7%;
- Das Ransomware Incident Response Engagement ging von über 22% der Vorfälle im Jahr 2016 auf gut 5% im Jahr 2017 zurück;
- Business und Professional Services gehören nun zu den fünf weltweit am stärksten angegriffenen Sektoren; mit 10% liegen sie an dritter Stelle;

- Der Gaming-Sektor war 2017 mit 20% am stärksten von Ransomware betroffen, gefolgt von Business und Professional Services mit 17%, Healthcare und Manufacturing mit 12% und Technologie mit 11%;
- Finanzdienstleistungen (18%) und Healthcare (15%) waren die beiden Sektoren, die am häufigsten Incident Response Services genutzt haben.

Der Global Threat Intelligence Report 2018 sammelt Daten von allen Unternehmen der NTT Group, dazu gehören NTT Security, NTT Communications, NTT DATA, Dimension Data sowie das Global Threat Intelligence Center. Der Report enthält auch Details aus Untersuchungen von NTT Security, einschliesslich weltweiter Honey Pots und Sandboxes in über 100 Ländern.

#### 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](http://www.nttsecurity.com/ch). Informationen zur globalen NTT Group finden sich unter [www.ntt.global.com](http://www.ntt.global.com).

#### Kontakt:

NTT Security  
NTT Security (Switzerland) AG  
Romy Däweritz  
Marketing Manager  
T +41 43 477 70 10  
[romy.daeweritz@nttsecurity.com](mailto:romy.daeweritz@nttsecurity.com)

PR-COM GmbH  
Hanna Greve  
Account Director  
Tel.: +49 89 59997 756  
[hanna.greve@pr-com.de](mailto:hanna.greve@pr-com.de)

Diese Meldung kann unter <https://www.presseportal.ch/de/pm/100062007/100814915> abgerufen werden.