Baltimore ist „Smart City ready“ – wirklich?

31.05.2019, 14:01 | IT, New Media & Software

Pressemitteilung von: *NTT Security*

ISMANING, Deutschland, 29. Mai 2019 - Der aktuelle Hackerangriff auf die Stadtverwaltung Baltimore schlägt hohe Wellen. Wieder einmal zeigt sich, dass nicht gepatchte Systeme zu den größten Sicherheitsgefahren gehören. Die Herstellung einer Cyber-Security-Hygiene mit elementaren Sicherheitsmaßnahmen darf nicht am Geld scheitern, sagt NTT Security, ansonsten wird auch die Umsetzung ambitionierter Smart-Society-Ziele am Misstrauen des Bürgers scheitern.

Bei der Stadtverwaltung Baltimore haben Hacker unter Nutzung eines Verschlüsselungstrojaners zugeschlagen, der erneut die Windows-Schwachstelle „EternalBlue“ nutzt. Sie wurde von Microsoft aber bereits 2017 mit Updates aller betroffenen Windows-Versionen geschlossen.

Diskutiert wird im Fall Baltimore zum wiederholten Male die unglückliche Rolle der NSA, die die Sicherheitslücke ursprünglich entdeckte und mehrere Jahre für eigene Zwecke nutzte. Schön und gut, aber die Diskussion geht jetzt am eigentlichen Problem vorbei. Der Fall Baltimore verdeutlicht vielmehr zweierlei: Zum einen wird oft erst dann gehandelt, wenn ein Sicherheitsvorfall eingetreten ist – das betrifft Behörden und Unternehmen gleichermaßen. Zum anderen zeigt Baltimore, an welchem Punkt vielfach die eigentlichen Probleme in der IT-Sicherheit liegen. Es sind nicht die hochkomplexen neuesten Angriffsszenarien, die auf innovativen KI-basierten Verfahren fußen, sondern bekannte Schwachstellen, für die immer noch keine ausreichenden Sicherheitsmaßnahmen ergriffen werden. „Bevor also kostenintensiv in neueste Sicherheitstechnologien investiert wird, sollten zunächst einmal die grundlegenden Hausaufgaben erledigt werden – und die beginnen bei der Herstellung einer Cyber-Security-Hygiene mit elementaren Sicherheitsmaßnahmen wie Netzwerksegmentierung, Datenverschlüsselung oder Patch Management“, erklärt Kai Grunwitz, Senior Vice President EMEA bei NTT Security. Vor allem das Patch Management ist von grundlegender Bedeutung, wie das Beispiel Baltimore eindrucksvoll belegt. Bei einem Großteil aller Sicherheitsvorfälle sind nach Erfahrungswerten von NTT Security Verwundbarkeiten ungepatchter Systeme und Anwendungen im Spiel. Viele Angriffe und Schäden der vergangenen Jahre, etwa mit Wannacry oder Petya, hätte man so problemlos verhindern können.

„Und was die ganze Geschichte noch pikanter macht“, so Grunwitz, „Baltimore hat ambitionierte Ziele in Richtung Smart City. Erst im April 2019 wurde die Stadt auch als einer von fünf Gewinnern der ‚Smart Cities Readiness Challenge’ in den USA gekürt.“ Baltimore verfolgt also prinzipiell einen zukunftsgerichteten Weg. Dabei darf aber der letztlich ausschlaggebende Punkt nicht übersehen werden. „Grundvoraussetzung für die erfolgreiche Umsetzung von Smart-Society-Modellen wie Smart Mobility, Smart Healthcare oder auch Smart City ist immer die gesellschaftliche Akzeptanz und das Vertrauen jedes einzelnen Bürgers in die Sicherheit“, betont Grunwitz. Und dabei reiche es nicht, eine Smart City mit einer hochmodernen Infrastruktur und neuesten Technologien aufzubauen, die auch von Anfang an im Sinne eines Security-by-Design-Ansatzes auf Sicherheit getrimmt ist. Wenn dann nämlich das Smart Government von Baltimore in der IT auf Altgeräten und nicht gepatchten Systemen basiert, wird das Grundvertrauen des Bürgers stark erschüttert und kann nur schwer wiederhergestellt werden. Auch neue innovative Modelle werden damit nicht auf die erforderliche gesellschaftliche Akzeptanz stoßen.

Was bleibt nach Meinung von NTT Security also zu tun? „Baltimore zeigt zum wiederholten Male, dass das Thema Cyber-Security von elementarer Wichtigkeit ist. Investitionen in die IT-Sicherheit zu unterlassen oder zurückzustellen ist – zugespitzt formuliert – fast verantwortungslos“, so Grunwitz. „Und ohne Cyber-Security-Hygiene ist auch das neue Gesellschaftsmodell Smart Society nur schwer zum Erfolg zu führen.“

Portrait

Über NTT Security

NTT Security ist das auf Sicherheit spezialisierte Unternehmen und „Security Center of Excellence“ der NTT Group. Mit „Embedded Security“ ermöglicht NTT Security den NTT-Group-Unternehmen (Dimension Data, NTT Communications und NTT DATA) die Bereitstellung zuverlässiger Business-Lösungen für Kundenanforderungen 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 den Unternehmen der NTT Group 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 Sie auf: www.nttsecurity.com

Über die NTT Group in Deutschland

Zur NTT Group in Deutschland gehören neben NTT Security die Unternehmen Arkadin, Dimension Data, e-shelter, itelligence, NTT Communications und NTT DATA. In Deutschland repräsentiert die NTT Group mit 6.550 Mitarbeitern einen Umsatz von mehr als 1,8 Milliarden Euro. Weitere Informationen zur globalen NTT Group finden Sie auf www.ntt-global.com.

News-ID: 1050887 • Views: 849 (Stand: 07.06.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/1050887/Baltimore-ist-Smart-City-ready-wirklich.html