IT-Sicherheit auf neuem Niveau: IBM findet Wege für den gesteigerten Schutz kryptografischer Schlüssel

Ziel ist es, die Kompromittierung kryptografischer Schlüssel und Codes zu vermeiden

Armonk, NY, USA - 24 Jul 2017: Kryptografische Schlüssel und Codes sind für eine effektive Informationssicherheit unabdingbar. Werden sie gehackt, liegen die vermeintlich verschlüsselten Daten auf dem Präsentierteller. Ein neues Patent von IBM macht kryptografische Schlüssel und Codes auf Leiterplatten sicherer und kann vor Manipulation schützen. Gleichzeitig ist das Herstellungsverfahren der Schutzschicht kostengünstiger. Kryptografische Schlüssel und Codes sind in Schaltkreisen gespeichert und werden genutzt, um sensible Daten zu ver- und entschlüsseln. Wenn diese auf den Leiterplatten innerhalb eines elektronischen Geräts gespeichert werden, ist es wichtig, dass die physikalische Manipulation oder der Zugriff auf die Schaltplatten verhindert werden. So kann vermieden werden, dass Codes kompromittiert werden. Das neue Patent, das Ingenieure von IBM nun erhalten haben, führt dazu, dass physikalische Manipulationen der auf der Leiterplatte in den Schaltkreisen gespeicherten kryptografischen Schlüssel und Codes besser verhindert werden können.

Bei dem Patent handelt es sich um einen Ansatz, der die inhärente Struktur einer Leiterplatte (Printed Circuit Board, PCB) nutzt. Im Gegensatz zu bisherigen Systemen erfordert das von IBM patentierte keine umfangreiche Verwendung von Harz oder anderen Materialien, um ein Modul oder eine Verpackung, die Schlüssel und Codes enthält, zu umhüllen. Dadurch kann die Herstellungsausbeute deutlich verbessert werden.

Traditionelle Ansätze verwenden, um Manipulationen zu vermeiden, typischerweise ein Kunststoff- oder Epoxid-ähnliches Harz. Die Codes und Schlüssel enthaltenden Schaltkreise werden damit ummantelt oder „umgossen“. Dabei besteht jedoch das Problem, dass sich die Leiterplatten, auf denen sich umhüllte Module während der Harzhärtung befinden, verformen können. In manchen Fällen kommt es sogar zu Verwerfungen der Leiterplatten.

Der patentierte Ansatz von IBM verwendet stattdessen Schaltkreise auf Schichten einer Leiterplatte oder einer anderen laminierten Struktur, um die kryptographischen Schlüssel und Codes vor der Kompromittierung zu schützen. Zusätzliche Schichten der Leiterplatte oder Laminatstruktur werden oberhalb und unterhalb der Schichten, die Schlüssel und Codes enthalten, hinzugefügt. Sie wirken als physikalische Zugangsbarrieren. Die Schaltkreise, die die Tasten und Codes schützen, können in zufälligen Mustern oder Positionen innerhalb der Leiterplatte oder Laminatstruktur platziert werden, um den Zugriff oder die Entdeckung zu verhindern. Die Schaltungen im neuen patentierten Ansatz bestehen auch aus Materialien, die über Röntgenprüfung oder akustische Mikroskopie nicht nachweisbar sind und dadurch die Sicherheit der Tasten und Codes weiter erhöhen.
IBM arbeitet seit Jahrzehnten in diesem Bereich und hat vor kurzem einen neuen IBM Z Mainframe angekündigt, die nächste Generation des weltweit leistungsstärksten Transaktionssystems. Das System ist in der Lage, mehr als zwölf Milliarden verschlüsselte Transaktionen pro Tag durchzuführen. Das patentierte System ist Teil der langen Liste an Technologien, die sich in der Erschaffung von IBM Z und anderen IBM Systemen widerspiegeln.

„Vom Start-up über den Mittelständler bis zum Großkonzern – Unternehmen aller Größen verfügen über sensible Daten, die ihren Wettbewerbsvorteil sichern oder die sie für ihre Kunden oder Mitarbeiter schützen müssen“, sagt Christian Nern, Head of Security Software DACH bei IBM Deutschland. „Bei IBM gibt es deshalb Teams, die sich ausschließlich mit der Erarbeitung und Innovation von Datenschutz und Sicherheit beschäftigen. Dadurch können wir ganzheitliche Sicherheitslösungen anbieten, vom Großrechner Z14 bis hin zu cloudbasierten kognitiven Diensten wie IBM Watson for Cyber Security.“

Über IBM Security

Das Security-Portfolio der IBM bietet intelligente Lösungen, um Mitarbeiter, Daten, Anwendungen und Infrastrukturen umfassend zu schützen. Dazu gehören Identitäts- und Zugangsmanagement, Informations- und Eventmanagement, Sicherheitslösungen für Datenbanken, Anwendungsentwicklung, Risiko- und Endpoint-Management, Intrusion Protection und vieles mehr. IBM ist einer der weltweit größten Entwickler und Anbieter von Sicherheitslösungen.

Für weitere Informationen, besuchen Sie bitte www.ibm.com/security, www.securityintelligence.com oder folgen Sie @IBMSecurity auf Twitter. Weitere News von IBM Security jetzt auch über WhatsApp: http://whp.li/1up

Über IBM

Mehr Informationen finden Sie unter http://www.ibm.com/de

Kontaktinformation

Mag. Barbara Jax

Unternehmenskommunikation IBM Österreich +43-1-21145-3686 +43-664-618 72 37 barbara.jax@at.ibm.com

---