

Open Letter von Art Coviello vom 6. Juni 2011

Englische Version unter: <http://www.rsa.com/node.aspx?id=3891>



Sehr geehrte Kunden,

am 17. März 2011 gab RSA bekannt, dass das Unternehmen einen technisch hochentwickelten Cyber-Angriff auf seine Systeme entdeckt hat, bei dem bestimmte Informationen über RSA SecurID® ausgespäht wurden. Wir haben sofort Best Practices und nach Priorität geordnete Korrekturmaßnahmen veröffentlicht und mehrere tausend Kunden proaktiv bei der Umsetzung der von uns empfohlenen Schritte unterstützt. Wir sind noch immer davon überzeugt, dass Kunden, die unsere Empfehlungen befolgen, ihre Sicherheit zuverlässig aufrecht erhalten können. Wir haben von Kunden unterschiedlicher Branchen bisher positive Rückmeldungen in Bezug auf von uns bereitgestellten Maßnahmen erhalten.

Bestimmte Merkmale des Angriffs auf RSA lassen darauf schließen, dass der Angreifer wahrscheinlich bestimmte Sicherheitsinformationen erhalten wollte, mit denen sich geheime Informationen aus der Verteidigungsindustrie und entsprechende Betriebsgeheimnisse ausspähen lassen. Wir glauben nicht, dass der Angriff auf finanzielle Bereicherung, personenbezogene Daten oder eine Bloßstellung in der Öffentlichkeit abzielte. Aus diesem Grund haben wir als zusätzliche Vorsichtsmaßnahme die Token von Behörden und Unternehmen aus der Verteidigungsindustrie schnellstmöglich ausgetauscht. Diese Maßnahmen verfolgen wir weiter.

In den vergangenen Wochen gingen unzählige hochkarätige Cyber-Angriffe gegen Unternehmen wie Epsilon, Sony, Google, PBS und Nintendo durch die Medien. Diese Angriffe stehen mit dem Vorfall bei RSA jedoch in keinerlei Zusammenhang. Sie machen jedoch deutlich, dass das Bewusstsein der Öffentlichkeit geschärft ist und auch Bedenken von Kunden im Zuge der immer neuen Bedrohungen zunehmen.

Vor dem Hintergrund der Zunahme der Häufigkeit der Angriffe haben wir am 2. Juni 2011 bestätigt, dass im März bei RSA ausgespähte Informationen bei einem versuchten ausgedehnten Angriff auf Lockheed Martin, einem der größten US-amerikanischen Rüstungskonzerne, verwendet wurden. Lockheed Martin hat erklärt, dass dieser Angriff abgewehrt wurde.

Wir möchten unsere Kunden darauf hinweisen, dass der Angriff auf Lockheed Martin keine neue Bedrohung oder Schwachstelle der RSA SecurID®-Technologie darstellt. Im Gegenteil bestätigt die Tatsache, dass ausgespähte Informationen über RSA-Produkte bisher nachweislich nur bei einem einzigen Angriff auf ein US-Rüstungsunternehmen verwendet wurden, unsere Einschätzung der Zielsetzung des Angreifers.

Wir sehen RSA SecurID® auch weiterhin als führende Multi-Faktor-Authentifizierungslösung und sind zuversichtlich, dass die Maßnahmen, die wir zur Verfügung gestellt haben, helfen werden unseren Kunden auch zukünftig ein Höchstmaß an Schutz zu gewähren. Dennoch ist uns bewusst, dass die Zunahme der Anzahl und Komplexität von Angriffen allgemein sowie der kürzlich bekannt gewordene Vorfall bei Lockheed Martin die Risikotoleranz mancher Kunden deutlich reduziert.

Wir möchten daher unseren Maßnahmenkatalog ausweiten und so das Vertrauen unserer Kunden in RSA SecurID®-Token und ihre allgemeine Sicherheit nachhaltig stärken. Dieses Programm beinhaltet auch weiterhin die unseren Kunden bereits im März zur Verfügung gestellten Best Practices. Darüber hinaus möchten wir unseren Kunden die beiden folgenden Angebote unterbreiten:

- Bei Kunden, deren Anwender sich hauptsächlich dem Schutz von geistigem Eigentum und Unternehmensnetzwerken widmen, werden SecurID®-Token ausgetauscht.
- Bei verbraucherorientierten Kunden mit einer großen Anwendergemeinde an verteilten Standorten werden zusätzlich risikobasierte Authentifizierungslösungen eingerichtet. Das gilt insbesondere für den Schutz finanzieller Transaktionen im Internet.

Wir arbeiten auch weiterhin mit unseren Kunden an der Bewertung ihrer einzigartigen Risikoprofile und Anwendergruppen und informieren sie darüber, welche Lösungen die größte Wirksamkeit zeigen und möglichst geringe Auswirkungen auf das Unternehmen und die Anwender haben.

Die Technologien von RSA, darunter auch die Authentifizierungslösung RSA SecurID®, helfen, viele der wichtigsten Informationen und Infrastrukturen überhaupt zu schützen. Die Bedrohungen für digitale Informationen nehmen weiterhin zu. Als führender Anbieter von Authentifizierungslösungen möchten wir sicherstellen, dass das enorme Potenzial und die zahlreichen Möglichkeiten einer vertrauenswürdigen digitalen Welt trotz dieser Bedrohungen erhalten bleiben. Wir glauben, dass SecurID® die leistungsstärkste Multi-Faktor-Authentifizierungslösung der Branche ist.

Wir werden auch weiterhin beträchtlich in SecurID® und risikobasierte Authentifizierungstechnologien investieren. Darüber hinaus werden wir weitere Faktoren für eine starke Authentifizierung bereitstellen. In diese Lösungen werden dann unsere Informationen zur Cyber-Kriminalität integriert, damit wir verdächtige Verhaltensmuster gegenüber Netzwerken, Transaktionen und Anwendersitzungen besser erkennen können. Mit unserer Cloud Trust Authority-Konsole stellen wir sicher, dass diese Technologien einen vertrauenswürdigen Zugriff auf virtuelle und Cloud Computing-Ressourcen ermöglichen. Des Weiteren unterstützen wir unsere Kunden dabei, noch effizientere mehrschichtige Schutzmaßnahmen einzusetzen, die im Kampf gegen moderne Bedrohungen so enorm wichtig sind. Dabei nutzen wir unser umfangreiches Portfolio zum Schutz vor Datenverlust, zur Verwaltung von Sicherheitsinformationen und -ereignissen (SIEM), DPI-Technologien sowie unser umfassendes Service-Know-how.

Unsere Kunden stehen für uns an erster Stelle.

Art Coviello, Executive Chairman, RSA

Weitere Informationen zu allen Korrekturmaßnahmen erhalten Sie bei Ihrem zuständigen RSA-Vertriebsmitarbeiter oder unter den folgenden Telefonnummern:

USA: 1-800-782-4362, Option 5 für RSA, Option 1 für das RSA SecurID® Remediation Program

Kanada: 1-800-543-4782, Option 5 für RSA, Option 1 für das RSA SecurID® Remediation Program

International: +1-508-497-7901, Option 5 für RSA, Option 1 für das RSA SecurID® Remediation Program