EMPA
Materials Science & Technology

Forschungsdaten abgeschirmt:
Empa vertraut auf SMS PASSCODE

Eine wirkungsvolle Absicherung von Remote-Zugängen, preisgünstig und einfach zu verwalten war das Ziel bei Empa im schweizerischen Dübendorf. Ein bestehendes Hardware-Token-System wurde erfolgreich durch SMS PASSCODE 4 ersetzt. Das neue Verfahren nutzt das Mobiltelefon zur Authentisierung, wodurch der Anwender keine zusätzliche Hardware mehr benötigt.

ÜBERBLICK

Die Empa (Swiss Federal Laboratories for Materials Science and Technology) ist eine interdisziplinäre Schweizer Forschungs- und Dienstleistungsinstitution für anwendungsorientierte Materialwissenschaften und Technologieentwicklung. Ziel der Empa ist es, Lösungen für vorrangige Probleme von Industrie und Gesellschaft zu erarbeiten, etwa in den Bereichen Energie, Umwelt, Mobilität, Gesundheit und Sicherheit. Forschungsschwerpunkte setzt sie in fünf Bereichen: nanostrukturierte Materialien, Sustainble Built Environment, Materialien für Gesundheit und Leistungsfähigkeit, natürliche Ressourcen und Schadstoffe sowie Materialien für Energietechnologien.

Standort: Dübendorf, Schweiz

Kunde: Empa – Swiss Federal Laboratories for Materials Science and Technology

Anforderungen: Zwei-Faktor-Authentisierung bei Remote-Zugängen zur Umsetzung allgemeiner IT-Compliance-Vorgaben sowie unternehmensspezifischer Sicherheitsbestimmungen. Ablösung einer bestehenden Token-basierten Authentisierung.

Lösung: SMS PASSCODE 4

Einsatzbereiche: Cisco VPN

Überwiegend physische Server mit Remote-Zugängen im Einsatz

Die Daten aus Forschung und Kommunikation laufen im Empa-Rechenzentrum in Dübendorf, in der Nähe von Zürich, zusammen. Dort sind etwa 1000 Anwender zu betreuen. Die 90 installierten Server sind zu etwa 25 Prozent unter VMware virtualisiert. Etwa 120 Remote-Zugänge sind derzeit bei der Empa in Betrieb. Sie werden zum Beispiel für die Arbeit im Home Office genutzt. Viele Empa-Mitarbeiter sind auch an anderen Instituten tätig oder haben Lehraufträge im Ausland. Sie alle greifen mit Cisco VPN auf das Firmennetzwerk zu.

Wichtig ist dabei, dass die hochsensiblen Forschungsdaten zuverlässig gegen unbefugten Zugriff gesichert werden. Deshalb war bei der Empa schon seit längerem eine Mehrfaktor-Authentisierung im Einsatz. Diese basierte auf Tokens von RSA.
Das etablierte System hatte zwar einwandfrei funktioniert, „die Hardware-Tokens haben allerdings etliche Nachteile“, weiß Thomas Gusset, Network & Security Engineer bei der Empa. „Die Geräte haben eine begrenzte Lebensdauer und sind nicht gerade billig. Ein hoher Aufwand entsteht auch bei der Verteilung und Verwaltung. Man muss schauen, dass jeder das richtige Token bekommt und wieder abgibt, wenn er die Empa verlässt. Außerdem war eine Anwenderschulung nötig.“

Sicherheitslücken durch verlorene Tokens

Ein weiteres Problem bei den Hardware-Authentisierern: Die Anwender hüten sie nicht gerade wie ihren Augapfel. „Manchmal wurde der Verlust eines Tokens erst nach einiger Zeit bemerkt und gemeldet“, berichtet Thomas Gusset. Die Verzögerung bei der Sperrung des Accounts kann zu Sicherheitslücken führen.

Hohe Kosten, umständliches Deployment und geringe Wertschätzung für das Token waren für Gusset die Gründe, sich nach einer SMS-basierenden Authentisierung umzusehen. „Wir haben uns zunächst eine Lösung unseres bisherigen Anbieters angesehen“, so Gusset. Diese war jedoch nicht direkt in den Login-Prozess integriert. Das Passwort musste erst umständlich von einer anderen Internet-Seite angefordert werden.

Nicht zuletzt wegen des komfortablen Handlings für Administrator und Anwender machte SMS PASSCODE das Rennen. Der Remote-User loggt sich einfach mit seinem bestehenden Domain-Account ein. Dann erhält er auf sein Mobiltelefon eine SMS mit einem Einmal-Passwort, das nur kurze Zeit gültig ist. Für jeden Login ist ein neues Passwort erforderlich. Die Einmal-Passwörter sind für Hacker und Cracker nutzlos, auch wenn sie, zum Beispiel über einen Keylogger, ausspioniert werden sollten. Die Einrichtung eines SMS-authentisierten Fernzugangs ist für den Administrator denkbar einfach: Es reicht ein Eintrag im Active Directory.

Auch die Gefahr durch verloren gegangene Authentisierungsgeräte ist unter SMS PASSCODE deutlich geringer. „Auf ihr Handy geben die Leute eben weit mehr Acht“, erklärt Thomas Gusset. „Ein Verlust wird sofort bemerkt und gemeldet. Für die Authentisierung werden Firmen- aber auch etliche Privat-Handys eingesetzt. Bedenken gegen die Preisgabe privater Mobilfunknummern gibt es bei der Empa-Belegschaft nicht. Die für die SMS-Authentisierung hinterlegte Telefonnummer ist im Active Directory nicht öffentlich sichtbar, um die Privatsphäre der Anwender zu schützen.

Implementierung mit freundlicher Remote-Unterstützung

Der virtualisierte Authentisierungs-Server wurde von den Empa-Spezialisten selbst installiert. „Wegen unserer nicht gerade alltäglichen Domain-Struktur war das gar nicht so einfach“, erzählt Thomas Gusset und lobt ausdrücklich den Support des Herstellers, der in einer Remote-Sitzung die Probleme rasch analysierte und beseitigte.

Die komplette Installation einschließlich Modem für den SMS-Versand war in etwa einem Arbeitstag abgeschlossen. Seitdem funktioniert das neue Authentisierungssystem problemlos parallel zum bisherigen. Sukzessive werden nun die Tokens abgeschafft und durch SMS PASSCODE ersetzt. Konfigurationsdateien auf den Clients sorgen dafür, dass jeweils die richtige Login-Methode angewandt wird.

Für die Zukunft rechnet Thomas Gusset noch mit einem Anstieg bei den Remote-Zugängen, denn Home Office-Arbeitsplätze werden immer beliebter. „Wir werden als Dienstleister auf den Bedarf reagieren und das System weiter ausbauen, zum Beispiel mit einem zweiten Modem. SMS PASSCODE ist gut skalierbar“.

ÜBER SMS PASSCODE

SMS PASSCODE® ist der Technologieführer in einer neuen Generation der Zwei-Faktor Authentifizierung zum Schutz vor aktuellen Bedrohungen aus dem Internet.
Try it live at: http://www.smspasscode.com