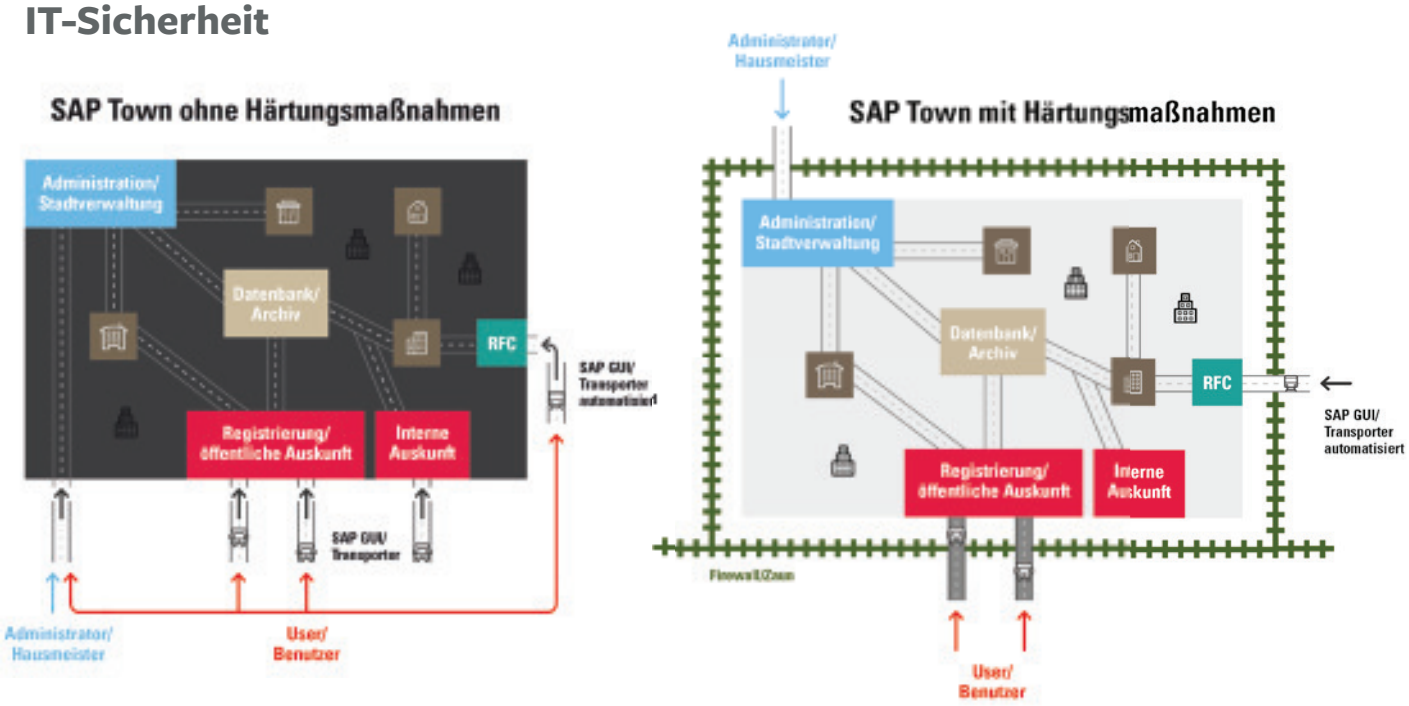

Beachtet man die Härtungsmaßnahmen, lässt es sich in SAP Town sicherer leben. Grafik: Syss GmbH

Mehr Sicherheit in SAP Town

Die (IT)-Sicherheit von SAP hat den Ruf, aufwendig und kompliziert zu sein. Im Folgenden sollen die potenziellen Schwachstellen sowie deren Behebung mit Hilfe einer Metapher erklärt werden.

TORSTEN LUTZ

Für ein SAP-System steht eine Firma, die wie ein Gebäudekomplex oder eine kleine Stadt aufgebaut ist: SAP Town. Die verschiedenen Gebäude und Räume in SAP Town stellen jeweils Dienste und Module innerhalb eines typischen SAP-Systems dar. Sie werden von normalen Benutzern (Usern) und Hausmeistern (Administratoren) genutzt beziehungsweise verwaltet. Für die Logistik (Datenaustausch) zwischen dem Benutzer und SAP Town sorgt ein Transporter (SAP GUI).

Zugang zu SAP Town: Wer darf rein?

Um Sicherheit in SAP Town zu gewährleisten, sollten wir als Erstes einen Zaun um unseren Gebäudekomplex ziehen (Netzseparierung, Firewall) und dabei zwischen einem Eingang für normale Benutzer und einem für Hausmeister (Administratoren) unterscheiden. Für beide schaffen wir getrennte Zufahrtswege. Ein legitimer normaler Benutzer kann den Zugang zur Stadtverwaltung (Administration) mit seinem Transporter idealerweise nicht erreichen (Zugriff für Benutzer ausschließlich via DIAG-Protokoll, gegebenenfalls über Web-GUI). Denn wenn ein Einbrecher (Angreifer) bereits vor der Tür steht, könnte er beispielsweise direkt versuchen, das Schloss zu knacken (Brute-Force-Angriff).

Aber auch beim Vorzeigen des Ausweises am korrekten Zufahrtsweg (Authentifizierung) bestehen zwei potenzielle Sicherheitsprobleme:

- Ein Einbrecher könnte sich mit einer Kamera unbemerkt postieren und Fotos von den Ausweisinformationen der Benutzer machen (Passwort-Sniffing). Damit könnte er sich in Zukunft als einer dieser Benutzer ausgeben und sich mit dessen Rechten Zugang zu SAP Town verschaffen.
- Ein Einbrecher könnte eine eigene Ausweiskontrolle vor der eigentlichen Kontrollstation aufsetzen und selbst die Ausweise kontrollieren (Man-in-the-Middle-Angriff). Dabei würde er ebenfalls in den Besitz aller notwendigen Informationen kommen, um sich als ein legitimer Benutzer auszugeben. Ein schlauer Angreifer würde die Informationen dann sogar so weiterleiten, dass keine ersichtliche zusätzliche Kontrolle stattfindet.

Zum Schutz vor diesen Gefahren müssen unsere Transporter (SAP GUI) erkennen können, ob sie von einem legitimen Kontrollpunkt kontrolliert werden. Dabei sollte kein Dritter in der Lage sein, diese Überprüfung zu beobachten oder zu belauschen. Eine einfache Idee wäre natürlich, den Benutzer zu fragen, ob er diese Kontrollstation kennt (Zertifikatprüfung). Allerdings funktioniert dieser Ansatz in der Praxis nicht. Meistens bestätigen die Benutzer einfach jede Art von Rückfrage. Also

„Beachten wir die Härtungsmaßnahmen, lässt es sich sicherer in SAP Town leben."

Torsten Lutz, Senior IT Security Consultant bei der Syss GmbH

müssen wir ein eindeutiges und fälschungssicheres Merkmal der Kontrollstation (Zertifikat, Public Key) an alle Transporter verteilen. Zudem baut sich jeder unserer Benutzer einen eigenen kleinen „Tunnel“ (Verschlüsselung) auf unserer Zufahrt auf, der ihn vor neugierigen Blicken schützt.

Auskünfte über Rechte in SAP Town: Was dringt nach außen? Wer darf was?

Fährt der Transporter zum ersten Mal nach SAP Town und will von der öffentlichen Auskunft/Registrierung den für ihn vorgesehenen Weg erfragen, ergeben sich zwei potenzielle Probleme:

- Es gibt zum einen die öffentliche Auskunft, die für alle verfügbar sein muss, und zum anderen eine interne Auskunft, die ausschließlich Anfragen von innerhalb des Gebäudekomplexes beantworten soll.
- Auch Anfragen von innerhalb des Gebäudekomplexes können potenziell von einer Abteilung kommen, die eigentlich keine Berechtigung hat, diese Informationen abzufragen.

Um sich gegen ungewollten Abfluss von Informationen abzusichern, muss die interne Auskunft zusätzlich Listen der berechtigten Abteilungen führen (Access Control Lists; insbesondere in den Dateien reginfo, secinfo und ms_acl_info). Befindet sich die interne Auskunft nicht hinter dem Zaun, werden interne Informationen plötzlich öffentlich verfügbar. Und falls es ein Einbrecher hinter den Zaun schaffen sollte, natürlich auch.

Da die Registrierung innerhalb desselben Gebäudes wie die öffentliche Auskunft verortet ist und daher nicht durch einen Zaun (Firewall) geschützt werden kann, benötigt sie zwei Listen: Eine, die definiert, welche Abteilungen sich grundsätzlich anmelden dürfen, und eine, die festlegt, welche Sicherheitsfreigaben diese besitzen.

In puncto Auskünfte über SAP Town ist außerdem das zentrale Datenarchiv (Datenbank), in dem alle Informationen gespeichert sind, äußerst wichtig. Dringt ein Einbrecher dort ein, werden alle anderen Kontrollmaßnahmen hinfällig. Deshalb gehört das Datenarchiv auf jeden Fall hinter den Zaun, und der Zugriff darauf muss streng geschützt werden (Verwendung sehr komplexer Passwörter).

Ähnliches gilt für Rechte: Wichtig für die Sicherheit in SAP Town ist, dass wir keine unnötig hohen Rechte erteilen (Berechtigungsobjekte). Deshalb sollten wir sichergehen, dass die Administration unsere Benutzer und deren Privilegien möglichst restriktiv gestaltet (Principle of Least Privilege; Profil „SAP_ALL“ nur für Ausnahmefälle wie Notfall-User oder Firefighter). Dies ist übrigens insbesondere für die Zufahrt zu SAP Town, die primär für automatisierte Vorgänge gedacht ist (RFC), relevant: Normale Transporter dürfen nicht berechtigt sein, sie zu befahren (Whitelist, Callback-Prüfung).

Stadtplanung und Architektur: Wie wird SAP Town saniert?

Im Rahmen der komplexen Bau- und Umbaumaßnahmen während der Konzeption und Umsetzung von SAP Town werden leider immer wieder unbewusst Hintertüren eingebaut, die einem Einbrecher oder Bewohner unberechtigt Zugriff auf Informationen verschaffen können. Die Fehler können sehr alt oder erst durch den Bau neuer Stadtviertel (Funktionen) entstanden sein. Wir sollten also SAP Town konsequent sanieren (sicherheitsrelevante Aktualisierungen). Um zu vermeiden, dass hierbei die Funktionalität beeinträchtigt wird, ist es hilfreich, Bauarbeiten erst einmal zu simulieren (Testumgebung), um Änderungen auf ihre Auswirkungen prüfen zu können. Und auch das Fundament (Betriebssystem) von SAP Town sollte gründlich gepflegt werden (OS-Updates).

Beachten wir diese Härtungsmaßnahmen, lässt sich in unseren SAP Towns sicherer leben. ■

SySS GmbH:
www.syss.de