

Physikalische Zutrittskontrolle im Einsatz bei der GfK-Gruppe

HANDVENEN-ERKENNUNG SCHÜTZT DIE SAP-SYSTEME

Der Grad für den Schutzbedarf der Daten eines Unternehmens ist von vielen Faktoren abhängig. Dabei lassen sich für die Zutrittskontrolle in das Rechenzentrum, in dem die sensiblen SAP-Applikationen und -Daten liegen, über Techniken wie die Handvenen-Erkennung zuverlässig schützen. Die Gesellschaft für Konsumforschung (GfK) hat diese Technik im Einsatz; implementiert wurde das von der PCS Systemtechnik.



Quelle: PCS

Die „Intus PS Handvenenerkennung“ schützt die Tür zum Rechenzentrum

Das Herz eines jeden Unternehmens ist heute das Rechenzentrum und dort laufen alle von SAP gesteuerten Prozesse mit den unternehmensweiten Daten zusammen – von den Mitarbeiterstammdaten bis zur Produktionsplanung. Schützt ein Unternehmen dieses Rechenzentrum, dient das nicht nur dem eigenen Firmeninteresse, sondern ist sogar vom Bundesdatenschutz-Gesetz zwingend vorgeschrieben: Im Paragraph 9 ist festge-

legt, dass technische und organisatorische Maßnahmen zu treffen sind, um den Schutz personenbezogener Daten zu gewährleisten.

Die Sicherheitsverantwortlichen in den Unternehmen sind aufgefordert, durch organisatorische Regelungen und Maßnahmen dafür Sorge zu tragen, dass personenbezogene Daten weder unbefugt genutzt noch – mit entsprechender krimineller Energie – gehackt werden können.

Im Interesse des Unternehmens ist es daher neben der logischen Zugangsberechtigung mit physikalischer Zutrittskontrolle das Rechenzentrum innerhalb des Firmengeländes zusätzlich abzusichern.

Sicherheitsniveaus unterscheiden sich

Für den Zutritt zu weniger sicherheitskritischen Bereichen bieten berührungslose RFID-Ausweise ein ausreichendes Sicher-

heitsniveau. RFID gilt für die Zutrittskontrolle als eine Möglichkeit der Identifizierung, die ein hervorragendes Preis-Leistungsverhältnis bietet und darüber hinaus einen hohen Komfort bereithält. Die Mitarbeiter-Stammdaten für die Zutrittskontrolle werden hierbei seitens SAP über die zertifizierte Schnittstelle (HR-PDC) verschlüsselt an ein Subsystem, zum Beispiel DEXICON Enterprise, übergeben.

Ein dem Mitarbeiterausweis zugeordnetes Standard-Zutrittsrecht ergibt sich aus der im Infotyp 0050 geführten SAP-Gruppierung, auch „BDE-Gruppe“ genannt. Bei RFID-Ausweisen sollte ein Unternehmen auf den Einsatz neuester Technologien setzen. Denn diese Leseverfahren bieten weiterentwickelte Speicherkapazitäten kombiniert mit hohen Übertragungsgeschwindigkeiten und ein „Karten-Hack“ wird dadurch weitestgehend ausgeschlossen. Derzeit bieten „Mifare DESFire EV1“ oder „Legic advant“ den bestmöglichen Schutz in Kombination mit einem sehr ergonomischen Handling.

Investition in das Sicherheitskonzept

Der erste Schritt zur Unternehmenssicherheit ist neben der physikalischen Zutrittskontrolle ein umfassendes Sicherheitskonzept, das organisatorisch definiert, ob beispielsweise die Mitarbeiterausweise überhaupt das Gebäude verlassen dürfen, was im Falle von verlorenen beziehungsweise nicht mehr auffindbaren Karten erfolgen muss und welche Personen von Fremdfirmen (wie zum Beispiel das Reinigungspersonal) welche Zutrittsrechte erhalten sollen und dürfen. Diese Aufgabe lässt sich nicht leicht verwirklichen, aber gefordert ist an dieser Stelle der Kompromiss zwischen Unternehmenssicherheit und Mitarbeiterkomfort.

Je nach Größe und Sensibilität des Unternehmens muss für Rechenzentren oder andere sicherheitskritische Bereiche, wie etwa die Entwicklungsabteilung, darüber hinaus der Einsatz von Hochsicherheitssystemen erwogen werden. Aktuell kommt an diese Stelle häufig eine biometrische Lösung zum Einsatz, die den Zutritt mittels Ausweis oder PIN-Code ergänzt und dadurch möglichst unverwechselbar macht. Bei der Biometrie spielt der zu-



RFID-Karten und -Tags zur komfortablen Zutrittskontrolle

nächst favorisierte Fingerabdruck inzwischen eine untergeordnete Rolle, da ihm in der Praxis die Akzeptanz der Mitarbeiter fehlt und er aus diesem Grund primär in Komfortanwendungen bei der Zeiterfassung zum Einsatz kommt.

Die Handvenen-Erkennung reglementiert den Zutritt

Für die GfK-Gruppe in Nürnberg stellte sich die Frage: Gibt es neben RFID-Lesern und Fingerprint eine bessere Technologie, um die vertraulichen Daten zu schützen? Denn die Zutrittsüberwachung des Rechenzentrums ist für die GfK-Gruppe von existentieller Bedeutung, denn die Gesellschaft für Konsumforschung handelt und vertreibt grundlegendes Wissen in Form von sensiblen Daten und Informationen, die die Industrie, Handel, Dienstleistungsunternehmen und Medien benötigen, um Marktentscheidungen zu treffen.

Weltweit ist die GfK Nummer 4 der Marktforschungsunternehmen. Im Jahr 2009 betrug der Umsatz der GfK-Gruppe 1,16 Milliarden Euro. Das ist Grund genug, um das Rechenzentrum und die darin enthaltenen Daten effektiv vor allen eventuellen Angriffs- und Manipula-

tionsversuchen, aber auch vor Diebstahl, zu schützen.

An diesem neuralgischen Punkt entschied sich die GfK für eine neue Technik, die zusätzlich zum Mitarbeiterausweis beziehungsweise dem personenbezogenen PIN-Code mit hochsicheren biometrischen Merkmalen bei der Zutrittskontrolle arbeitet und deswegen nicht manipulierbar ist: die Handvenenerkennung. Der „Intus PS Handvenen-Leser“ vom Münchner Spezialisten PCS erkennt mit Hilfe eines Infrarot-Sensors und einer integrierten Kamera das menschliche Handvenen-Muster, das sich innerhalb der Handinnenfläche befindet.

Diese Technik ist bei jedem Menschen nutzbar, einfach in der Anwendung, hygienisch und trotzdem hochsicher, denn die Position sowie die Struktur sowie das Muster der Venen sind bei jedem Individuum unterschiedlich. Ein unbemerktes Erfassen des biometrischen Merkmals wird hierbei zuverlässig verhindert.

Sowohl bei der Speicherung der Referenzmuster, der so genannten Templates, als auch beim Transfer an andere Systeme sorgt die integrierte Verschlüsselung dafür, dass keine unberechtigten Zugriffe erfolgen können. Die Handvenenerkennung des Intus PS arbeitet mit extrem hoher Genauigkeit und Sicherheit. Die Falsch-Akzeptanz-Rate (FAR) liegt bei 0,00008 Prozent, die False-Rejection Rate (FRR) bei 0,01 Prozent und gilt defacto als fälschungssicher.

Bei einem Zutrittsversuch wird das aktuelle Handvenenmuster mit dem in der Datenbank gespeicherten Mustern verglichen und der Mitarbeiter so eindeutig und unverwechselbar identifiziert. Nur wenn die Identität des Mitarbeiters eindeutig verifiziert ist, öffnet sich die Tür zum Rechenzentrum. Mit diesem modernen Sicherheitspaket trotzt die GfK allen Hack- und Betrugsversuchen moderner Datenräuber und schützt so physikalisch das Rechenzentrum. Diese Technologie wurde bereits mehrfach ausgezeichnet – zuletzt im Juli 2010 mit dem Bayrischen Sicherheitspreis für herausragende innovative Sicherheitsprodukte der betrieblichen Sicherheit, verliehen vom BVSU unter der Schirmherrschaft des Bayerischen Staatsministeriums des Inneren. (Ute Hajek, PCS Systemtechnik/rh) ©