

Traditionelle Data Security beschränkt sich in der Regel auf die Zugriffskontrolle der jeweiligen Anwendungssysteme. Dies wird ergänzt durch Firewalls, Gateways und Intrusion Detection Systeme, die ein unerlaubtes Eindringen in die IT-Infrastruktur verhindern. Obwohl diese Schutzmechanismen ein hohes Maß an Kontrolle besitzen, bieten sie keine absolute Sicherheit. Schwachstellen werden ausgenutzt, um Zugänge zu Informationen zu schaffen, deren unkontrollierte Nutzung schädlich für das Unternehmen sein kann.

Die Achillesferse traditioneller Sicherheits-Mechanismen, bezogen auf die Sicherheit von Daten, ist die Tatsache, dass Informationen in einer direkt lesbaren Form vorliegen. Die Zugriffe auf die Informationen werden für Unbefugte lediglich verweigert, die Daten sind eigentlich nur versteckt. Diese Tatsache lässt viel Spielraum für einen Angreifer, die Sicherheits-Mechanismen zu umgehen.

In einer sicheren Umgebung werden sensible Daten generell durch Verschlüsselung in einem nicht-lesbaren Format gehalten. Die Umwandlung in einen lesbaren Kontext wird durch eine von Betriebssystem oder Datenbank getrennten Berechtigungsebene kontrolliert. Diese Erweiterung der Zugriffskontrolle eliminiert die Gefahr des Datendiebstahls durch Schwachstellen in den Anwendungs-, Datenbank- und Betriebssystemen.

Die Ingrian DataSecure Plattform gewährleistet Datensicherheit durch ein mehrstufiges Berechtigungs-System, kombiniert mit einer industriennormierten Verschlüsselung sensibler Daten. Die zentralisierte zusätzliche Zugriffskontrolle kann sich über mehrere Anwendungen und Datenbanken erstrecken. Durch die Anbindung an existierende Verzeichnis-Systeme wie LDAP ist eine schnelle Integration in die bestehende Sicherheits-Architektur möglich. Die zeitgesteuerte Nutzungs-Einschränkung liefert die notwendige Flexibilität, großzügige Berechtigungen für „superuser“ (z.B. Datenbank- oder Anwendungs-Administrator) zu erlauben und gleichzeitig vor Missbrauch zu schützen. Die Policy-basierte Management Oberfläche deckt alle Anforderungen für eine sichere Schlüsselverwaltung ab und macht die Implementierung einer komplexen PKI Infrastruktur überflüssig. Das Ganze wird von einer umfassenden Revision ergänzt, so dass jederzeit unerlaubte Zugriffe transparent werden.

Die zentrale DataSecure Appliance wird über eine sichere Netzwerkverbindung mit dem Datenbank Server verbunden. Die DataSecure Plattform führt die zusätzliche Authentifizierung aus, übernimmt die Verschlüsselungsaufgaben und entlastet damit den Datenbank Server. Diese physische Trennung von der Datenbank Plattform bietet darüber hinaus eine erhöhte Sicherheit gegenüber datenbankinternen Lösungen. Man spricht dabei von einer Trennung der Sicherheitsmechanismen von den Angriffszielen.

Der Kern dieser Architektur ist, dass der Zugriff auf die Daten von der DataSecure Plattform nicht verhindert wird, stattdessen wird die Umwandlung von verschlüsseltem in unverschlüsseltes Format verhindert. Der Vorteil dieser Vorgehensweise lässt sich anhand eines einfachen Beispiels darstellen: Administrative Benutzerkonten haben in der Regel fast uneingeschränkten Zugriff auf alle Daten in der Datenbank. Diese Regelung ist zwar notwendig für den Betrieb des Datenbank-Systems, der Missbrauch dieser Benutzerkonten ist jedoch eines der größten Sicherheitsrisiken in Datenbank Systemen. Mit der Ingrian DataSecure Plattform haben diese Benutzerkonten nach wie vor die notwendigen Zugriffsberechtigungen auf Datenbank Objekte, jedoch sind die betroffenen Spalten (z.B. Konteninformationen oder Lohn/Gehälter) nicht lesbar. Wenn ein Angreifer versucht, über administrative Benutzerkonten auf Daten zuzugreifen, weigert sich die DataSecure Plattform, die Spalten zu entschlüsseln. Administrative Operationen können wie gewohnt durchgeführt werden. Sollte sich jemand unbefugten Zugang über die administrativen Konten verschaffen, sind die Daten trotzdem sicher, und der fehlgeschlagene Versuch, Daten zu entschlüsseln, wird protokolliert und ist somit nachvollziehbar.

Die Implementierung von DataSecure ist transparent für Anwendungen und unterstützt Standardlösungen wie PeopleSoft. Sie erlaubt eine schnelle und effektive Absicherung bestehender Datenbanksysteme und unterstützt DB2, SQL Server und Oracle. Die zusätzliche Kontrolle ist nicht auf Datenbanken beschränkt. Durch Unterstützung von Standard APIs wie z.B. JCE, MSCAPI und XML ist die Erweiterung der Sicherheit auf der Ebene der Applikation gegeben; so kann auch jedes andere Datenhaltungssystem in das Sicherheitskonzept aufgenommen werden. Integriertes Load Balancing, Health Checking und Connection Pooling garantieren eine ausfallsichere und performante Integration in bestehende Systeme. Die modulare und einfach skalierbare Architektur erlaubt auch kleineren Unternehmen einen wirtschaftlichen Einsatz dieser Technologie.