# PRESSEMITTEILUNG

**Unternehmensdaten schützen: PROXESS veröffentlicht Whitepaper zu Cybersecurity und integriert umfassende Sicherheitsfunktionen mit 3-fach-Authentifizierung in sein DMS**

Mit dem dreistufigen Sicherheitsprogramm seiner Dokumentenmanagement-Lösung schafft PROXESS den Spagat zwischen Anwenderfreundlichkeit, umfassendem Schutz und revisionssicherer Aufbewahrung von Dokumenten – TÜV-geprüft, gemäß gesetzlicher Vorgaben und mit zusätzlicher Smart-Card-PIN-Autorisierung für Supervisor. Doch zum umfassenden Schutz von Unternehmensdaten bedarf es auch einer Cybersecurity-Strategie für die übrige IT-Infrastruktur des Unternehmens. So bietet PROXESS aktuell ein kostenloses Whitepaper zum Thema mit Guideline zur Abwehr von Cyberattacken.

Der Softwareanbieter und Experte für Dokumentenmanagement bietet mit seiner Lösung PROXESS 10 ein skalierbares DMS mit Schnittstellen zu zahlreichen ERP-, CRM-, HR- und FiBu-Systemen sowie Office-Anwendungen und E-Mail-Programmen. Entsprechend sammeln sich im PROXESS-System vertrauliche Dokumente und sensible Daten, die vor unberechtigten Zugriffen geschützt werden müssen – intern wie auch extern. Dass dieser umfassende Schutz, inklusive revisionssicherer Archivierung nach GoBD*-Richtlinie, gleichzeitig benutzerfreundlich auf die entsprechenden Rollen im Unternehmen zugeschnitten sein kann, beweist das Dokumentenmanagementsystem von PROXESS.

Die Lösung kombiniert detaillierte, qualitative Zugriffsberechtigungen bis auf Benutzerebene mit der Verschlüsselung von Datenbank und Dateien sowie der Protokollierung von Änderungen, um Manipulationsversuche am System aufzudecken. Dabei hat der Supervisor – meist ein Mitglied der Geschäftsleitung – die zentrale Rolle im Sicherheitskonzept von PROXESS. Ausgestattet mit einer PIN-geschützten Smart-Card vergibt er Berechtigungen an Benutzer oder delegiert diese Aufgabe an sogenannte „Bereichsadministratoren“ – einfach und schnell, ohne dass weitreichende IT-Kenntnisse von Nöten sind. Die von ihm ernannten Bereichsadministratoren sind wiederum in der Lage, Benutzerverwaltung und Zugriffsberechtigungen innerhalb ihrer Abteilung vorzunehmen. Diese wird durch die Integration von Windows Active Directory zusätzlich erleichtert. Darüber hinaus ermöglicht das Dokumentenmanagementsystem eine lückenlose IT-Administration inklusive Verwaltung der Archivstrukturen, Datenbanken, Datensicherungen sowie Hardwarekomponenten, ohne dass der Administrator Zugriff auf Archivinhalte oder Einsicht in die Dokumente hat.

Unkompliziert und zuverlässig erfüllt die PROXESS-Lösung so unterschiedliche Zugriffs- und Sicherheitsbedürfnisse. Die Installation eines aufwendigen Nebensystems – beispielsweise zum Schutz besonders sensibler Dokumente – ist dazu nicht nötig.

Doch nicht nur intern stoppt die DMS-Lösung Unbefugte zuverlässig. Intelligente Verschlüsselungsverfahren stellen sicher, dass auch von außen keine Gefahr droht. Mittels symmetrischer und asymmetrischer Verschlüsselungsverfahren nach AES (Advanced Encryption Standard) werden Dateiinhalte geschützt und sind so auch gegen „Dictionary-Angriffe“ immun. Weiterhin protokolliert das System nicht nur alle vorgenommenen Änderungen, sondern auch die Dokumentenzugriffe – so ist die Integrität der archivierten Daten jederzeit gewährleistet.

Die DMS-Lösung aus dem Hause PROXESS schützt sensible Daten mit ihren intelligenten Sicherheitsfunktionen sowohl auf Ebene der Benutzer und Datenbank als auch des Dateisystems – ohne aufwendige Administration oder die Installation eines Zweitsystems. Doch die Sicherheit des DMS allein reicht nicht aus, denn es ist nur ein Baustein der gesamten IT-Infrastruktur eines Unternehmens. Um Cyberattacken zuverlässig und vor allem ganzheitlich zu verhindern, hat PROXESS ein Whitepaper erstellt, das erläutert, wie Unternehmen ihre komplette IT-Struktur optimal vor Angriffen schützen und welche Maßnahmen im Falle einer Attacke zu ergreifen sind. Dazu haben Experten wie Heinz Pretz, Leiter Softwareentwicklung und Kundenservice der PROXESS GmbH; Silvana Rößler, Head of Security Incident Response & Digital Forensics bei der networker, solutions GmbH sowie Dirk Kordus, Chief Claims Officer und Matthias Neumann, Chief Underwriting Officer von der COGITANDA Group ihr Fachwissen zusammengetragen. Das Whitepaper „Vernetzte Welt – sichere Welt? Wie Sie Ihr Unternehmen vor Cyberattacken schützen können“ steht Interessierten hier kostenlos zum Download zur Verfügung.

*GoBD: Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff