versiondog Factsheet:

versiondog – Switch-Integration – das „Honeypot Szenario“

versiondog – erhöht die Sicherheit der industriellen Automatisierung

versiondog ist die führende Software für Versions- und Datenmanagement in der automatisierten Produktion. Das System unterstützt Unternehmen dabei, Daten zu sichern und Versionen optimal zu verwalten.

versiondog schafft überall dort Ordnung, wo Projektdaten kontinuierlich geändert und zentral zur Verfügung gestellt werden müssen. Die Software erhöht die Sicherheit und Wirtschaftlichkeit der Produktion.

Außerdem sorgt versiondog für ein optimales Zusammenspiel unterschiedlicher Robotertypen, Feldgeräte, Steuerungen, Antriebssystemen, Programmiersprachen, Dateiformaten und Software-Anwendungen.

Das Datenmanagementsystem sorgt für Datentransparenz und -verfügbarkeit, wodurch Kosten und Aufwand reduziert, Risiken minimiert werden.

Datenmanagement als Teil der Cyber Security-Strategie

In der industriellen Automatisierung ist die Cybersicherheit ein zentrales Thema. Um Cyberangriffe frühzeitig zu erkennen, ist es essenziell, Änderungen an industriellen Steuerungen schnell festzustellen, um dann prüfen zu können, ob diese gewünscht waren. Da versiondog Änderungen in den Softwareversionen von Automatisierungsgeräten überwacht, lassen sich alle Änderungen, die nicht dokumentiert wurden, im Programmcode entdecken und auf unautorisierte Zugriffe prüfen.

Hat ein Cyberangriff stattgefunden, ist die schnellste Lösung, den Datensatz auf den vorherigen, nicht kontaminierten Stand zurückzusetzen. Aus diesem Grund ist es wichtig, regelmäßig eine Datensicherung durchzuführen. Der Instandhalter kann dann eine „saubere“ Datensicherung aus dem Server-Archiv nehmen und diese wieder auf die Steuerung aufspielen. Dieser Vorgang nennt sich Disaster Recovery und setzt das Automatisierungsgerät wieder auf seinen letzten, manipulationsfreien Zustand zurück.

Damit ist versiondog ein wichtiges Teilstück in der gesamten Cyber Security Strategie vieler Konzerne - in der Produktion auch Defense-in Depth Strategie genannt.

Das „Honeypot Szenario“

Ein weiteres Teilstück einer Cyber Security Strategie ist der „Honeypot“. Das industrielle Netzwerk wird aus Gründen der Übersichtlichkeit sowie der vereinfachten Administration typischerweise in unterschiedliche Ebenen unterteilt, die sich an den Datenströmen und Aufgaben orientieren. In der Maschinenebene werden Endgeräte wie Steuerungen, Feldgeräte oder HMI-Panels mit Industrial Ethernet Protokollen wie PROFINET über Switche verbunden. Ein Switch gehörte häufig zu den frühen Angriffszielen für Cyberattacken, da er über die Portsteuerung den Zugriff auf ein Automatisierungsgerät ermöglicht. Wird ein Port durch einen Cyberangriff geöffnet oder geschlossen, kann die Verbindung zu einem Endgerät getrennt oder ein unerlaubter Zugriff auf ein Gerät gewährt werden, was in beiden Fällen mit hohen Risiken einhergeht.

Das Ziel des „Honeypot Szenarios“ ist es, einen Cyberangriff oder dessen Vorbereitung rechtzeitig zu entdecken. Dafür benötigt es einen im Industrienetz installierten und eingerichteten Switch. Dieser erhält keine echte Funktion, sieht aber so aus, als wäre er attraktiv (Honeypot). Alle Verantwortlichen sind angehalten, selbst keine Änderung an diesem Switch durchzuführen, sondern diesen nur zu überwachen. versiondog überprüft den Switch auf ungewollte Veränderungen und meldet Alarm, wenn eine Anomalie entdeckt wurde. Die Mitarbeiter können reagieren und mögliche Folgen des Cyberangriffs verhindern. Mit einer regelmäßigen, automatischen Datensicherung überwacht das Datenmanagementsystem versiondog die Konfigurationsdaten eines Switches und erkennt Änderungen sofort.

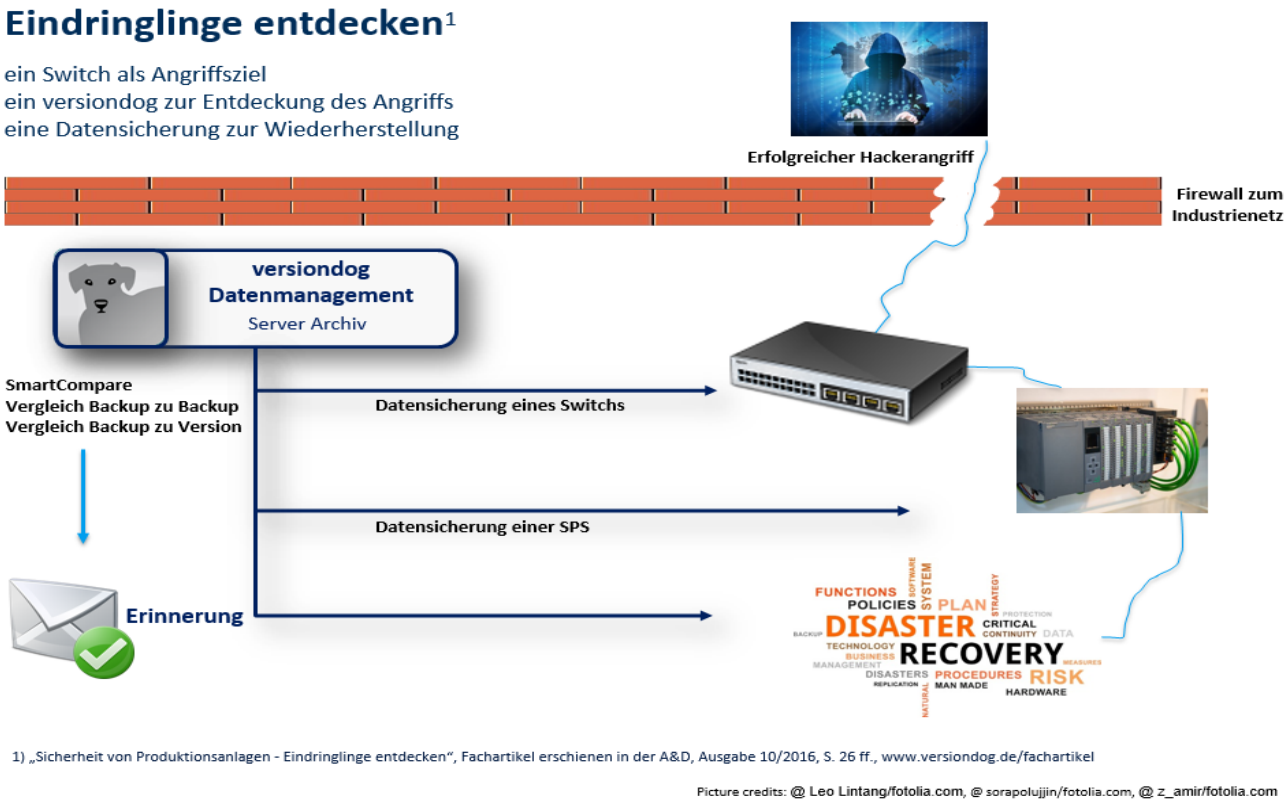


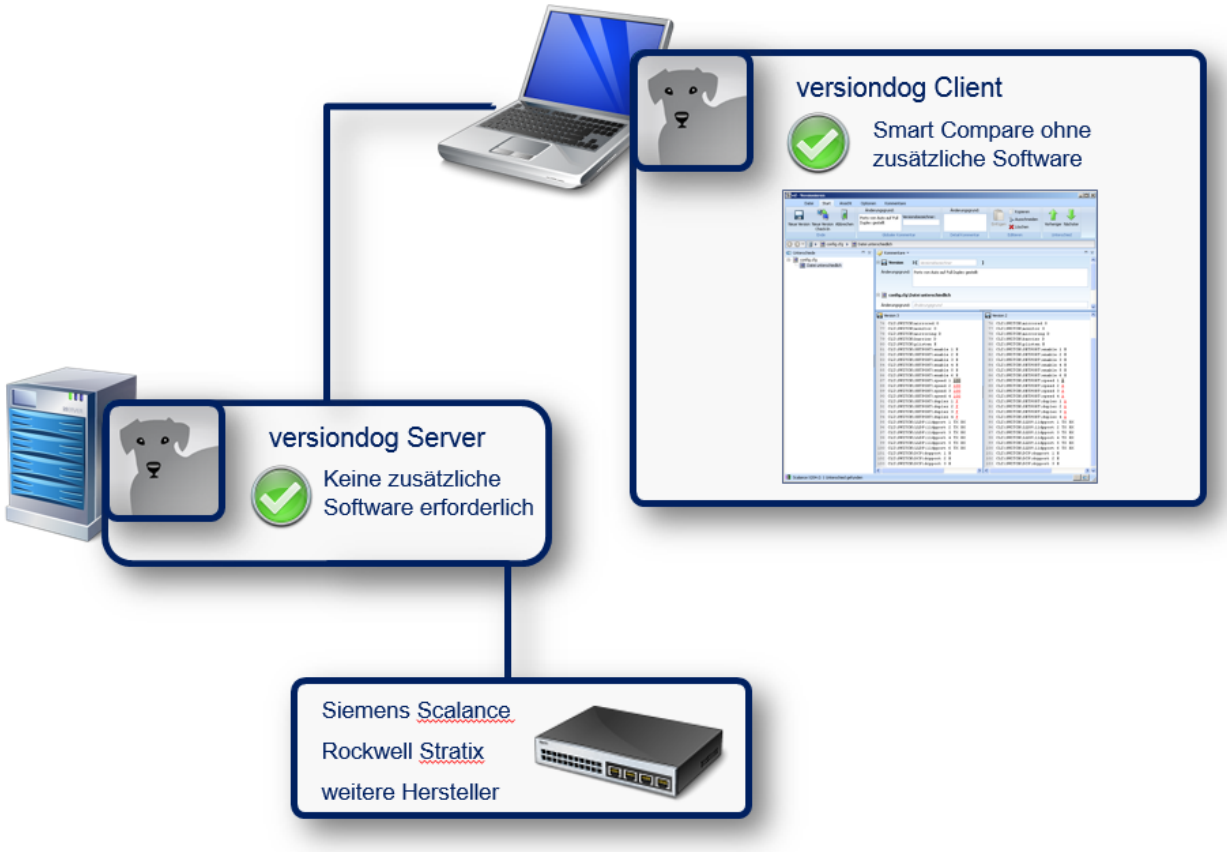
Abbildung 1: Honeypot Szenario. Ein Switch im Industrienetz, bei dem keine Änderungen im Programmcode vorkommen, wird regelmäßig von versiondog auf ungewollte Änderungen überwacht und wenn bei einem Datenvergleich unautorisierte Änderungen entdeckt werden, wird der zuständige Systemadministrator informiert.

AUVESY.

versiondog Switch-Integration

Wie unterstützt versiondog die Sicherheit Ihrer Daten?

- versiondog verifiziert zyklisch und automatisch die freigegebenen Versionen
  - ✓ mehrmals täglich
  - ✓ mit Alarmmeldungen
  - ✓ bei Abweichungen textuelle und/oder grafische Darstellung der Unterschiede
  - ✓ für fast alle Geräte der Automatisierungstechnik
- versiondog detektiert Unterschiede in Steuerungsprogrammen und stellt sie dar.
- versiondog überwacht die Systemkonfiguration von auf Windows und Linux basierenden Systemen.
- versiondog stellt sicher, dass versionierte Stände nicht verändert werden können.
- versiondog stellt Software-Stände (Versionen) ohne „Kontamination“ bereit für ein „sauberes“ Disaster Recovery.



AUVESY.

versiondog Switch-Integration

Leistungsmerkmale

Backup, Versionskontrolle und Dokumentation von Softwareprojekten	✓
SmartCompare für alle Komponenten in der automatisierten Produktion	✓
Vergleich Backup zu Backup oder Backup zu Version	✓
Nachvollziehbarkeit der Änderungen, gewollt oder ungewollt	✓
Wer hat wann was wo und warum geändert?	✓
Meldewesen bei nicht dokumentierten Änderungen	✓
Schnelles und sicheres Disaster Recovery	✓

Systemvoraussetzungen

versiondog Release	ab 5.0

Mehr Informationen

AUVESY GmbH & Co KG
Tel. +49 (0)6341 6810-440
E-Mail info@versiondog.de
Web www.versiondog.de