Wie ein Cyber-Angriff für mehr Sicherheit sorgen kann

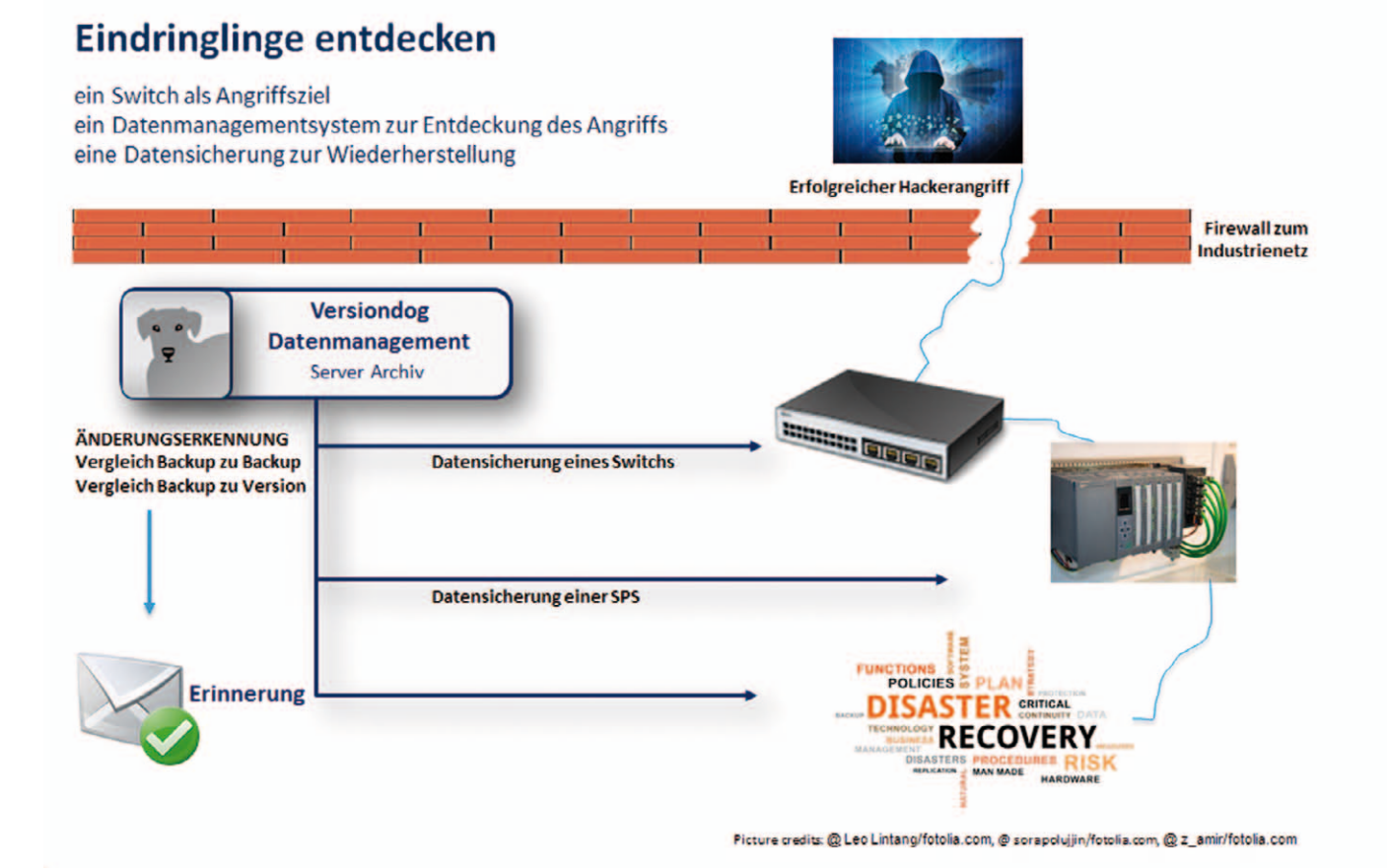

Bild 1: Das Honeypot-Szenario

Wenn man auf Angreifer in der virtuellen Welt frühzeitig reagieren will, muss man diese verstehen, deshalb kann es hilfreich sein, sich ihnen komplett auszuliefern. Zuerst wird die Firewall abgeschaltet, um das Netzwerk zu öffnen. Die Zugangsberechtigung wird abgeschaltet, so dass jeder Virus oder jede Malware ungebremst auf das System einschlägt. Jetzt schließen Sie die Augen und verabschieden sich von Ihren Daten - denn meistens sind es diese, worauf es die Angreifer abgesehen haben.

Selbstverständlich ist das in dieser Form nur ein Gedankenspiel, ein Szenario. Niemand würde real mit echten Daten so fahrlässig handeln, zumal es auch gesetzlich untersagt ist, aber man kann dieses Szenario auch vortäuschen. Eine Vorgehensweise, ähnlich dem oben Beschriebenen, um Hacker-Angriffe gezielt aufzuspüren, verbirgt sich hinter dem Begriff des „Honeypot-Szenarios“. Man öffnet die Tür, sichert sich aber gegen alle Schäden, die dabei entstehen könnten ab, damit nicht derjenige, der die Tür offen gelassen hat, haftet. Deshalb ist es zwingend ratsam, dieses Szenario nur gemeinsam mit dem IT-Berater des Unternehmens durchzuführen, um den Schutz der Daten zu jedem Zeitpunkt zu gewährleisten.

Welche Ziele verfolgen Angreifer?

Im industriellen Umfeld hat das Thema Cybersecurity gerade eine sehr hohe Priorität. Doch warum und an welcher Stelle sollte man einen Cyberangriff überhaupt zulassen wollen? Um Prozesse vor ungewollten Eingriffen zu schützen, ist es wichtig, zu verstehen, welche Ziele die Angreifer verfolgen und wie sie dabei vorgehen. In einer Automatisierungsumgebung finden sich neben Steuerungen, Roboter, Antriebe, HMIs auch Switche. Diese haben im Netzwerk die Aufgabe, die Komponenten mit dem Server zu verbinden und Daten durchzulassen, die an anderer Stelle benötigt werden. Ein Switch überwacht Datenströme und die Kommunikation im Internet der Dinge, übergibt Befehle an Steuerungen oder sorgt dafür, dass niemand Befehle an ein Gerät aus der Produktion übermittelt, wenn er nicht die Berechtigung dafür hat.

Das macht den Switch zu einem klassischen Angriffsziel für Cyberattacken und zu einem optimalen Ansatzpunkt für das Honeypot-Szenario.

Ein Switch als Honeypot

Ein Switch in einem Industrienetz ist zuständig für die Anbindung von Netzwerkkomponenten wie beispielsweise Roboter, Antriebe oder eine SPS. Konfiguration und Firmware des Switches sind wichtige und absolut schützenswerte Daten:

1. Die Firmware eines Switchs gleicht einem Betriebssystem, das nur auf Grund von Herstellerangaben verändert wird.

2. Die Konfiguration eines Switchs beinhaltet die Grundeinstellungen,

Autoren:

Dr. Thorsten Sögding, Head of Business Development, AUVESY GmbH & Co. KG
Co-Autor: Stefan Schnackertz, Business Development, AUVESY GmbH & Co. KG

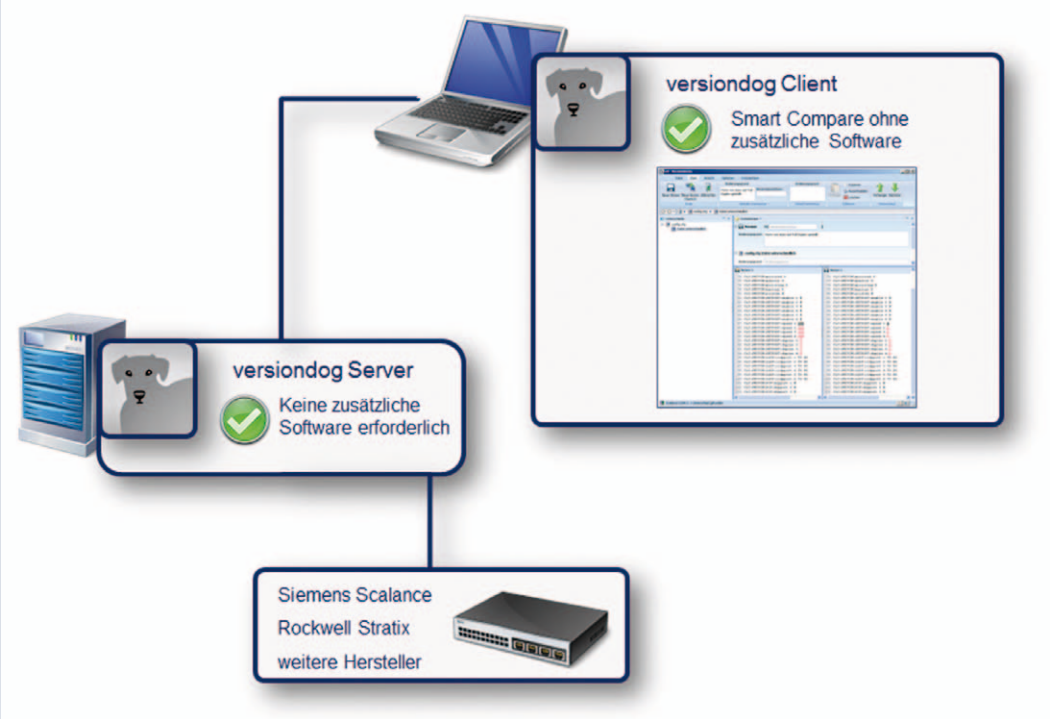

Bild 2: Switch-Management mit dem Datenmanagementsystem versiondog

also über welchen Port darf welcher Netzwerkverkehr an eine angeschlossene Komponente gesendet und im Gegenzug von der Komponente empfangen werden. Diese Daten sind entscheidend für eine reibungslose Kommunikation mit der Komponente über den Switch.

Angreifer, die einem Netzwerk schaden möchten, können die Netzwerkkommunikation eines Switches umgehen, um erfolgreich Daten zu manipulieren. Nicht selten wird dafür der Switch manipuliert, damit er fehlerhafte Daten sendet oder empfängt bzw. Ports öffnet oder schließt, um dem Angreifer eine schnelle Verbindung zu einer Komponente zu ermöglichen.

Da durch das "Honeypot-Szenario" ein Cyberangriff oder dessen Vorbereitung rechtzeitig entdeckt werden soll, wird ein Switch – als beliebtes Angriffsziel- ohne echte Funktion im Industrienetz installiert und eingerichtet. Er soll nur so aussehen, als wäre er ein attraktives Ziel (Honeypot). Die eigenen Mitarbeiter sind in solche Szenarien eingeweiht und kennen diesen Switch. Sie werden selbst keine Änderung durchführen, sondern nur überwachen. Mit Hilfe eines Datenmanagementsystems wird der Switch in regelmäßigem Abstand auf ungewollte Veränderungen überprüft. Hierbei werden die Konfigurationsdaten des Switches durch eine regelmäßige und automatische Datensicherung überwacht. Werden Änderungen und damit ein Angriff erkannt, meldet das Datenmanagementsystem Alarm. Die Mitarbeiter können sich den ohne Schaden erfolgten Angriff im Detail ansehen und damit mögliche Folgen des bevorstehenden Cyberangriffs verhindern.

Vorteile eines Datenmanagementsystems

versiondog ist ein Datenmanagementsystem, das im Industrienetz eines produzierenden Unternehmens installiert wird und automatisch Daten sichert und überwacht. Daneben sollten alle Lösungen für die Daten- und Netzwerksicherheit wie Firewalls, IDS- oder IPS-Systeme unabhängig von versiondog installiert sein. Sie bilden weitere entscheidende Barrieren gegen Cyberangriffe und werden durch versiondog nicht ersetzt. Bei einem Switch liegt das Hauptaugenmerk auf der Veränderung der Portfreigaben, die einem Hacker das Tor zur Automatisierungskomponente öffnen, um weiteren Schaden anzurichten.

Die Datensicherung, deren Dokumentation (wer hat was, wann, wo und warum geändert) und die Versionskontrolle sind deshalb weitere wichtige Bausteine einer Cybersecurity Strategie. Nach einer Datensicherung wird das gesamte Datenpaket mit dem letzten Stand verglichen. Ein Datenmanagementsystem überwacht alle Datensätze – die im Falle des „Honeypot-Switches" gleich sein sollten – und erkennt jede Änderung im Code eines Programmes. Wenn Änderungen im Programmcode gefunden werden, meldet versiondog dies dem Systemadministrator, der die Änderungen klassifiziert. Wenn ein Angriff entdeckt wird, kann der Systemadministrator schnell reagieren und ein Disaster Recovery mit einer „sauberen" Version vom Server des Datenmanagementsystems durchführen.

Defense in Depth

Cyberangriffe auf die Produktion sind zur Realität geworden und wegen der Komplexität von Anlagen ist nur eine mehrstufige Verteidigungsstrategie wirklich effizient (Defense in Depth). Das Honeypot-Szenario ist ein Baustein von vielen – ein Stück Sicherheit mehr, um Mensch, Natur und Umwelt zu schützen.

■ *AUVESY GmbH & Co. KG*
www.versiondog.de

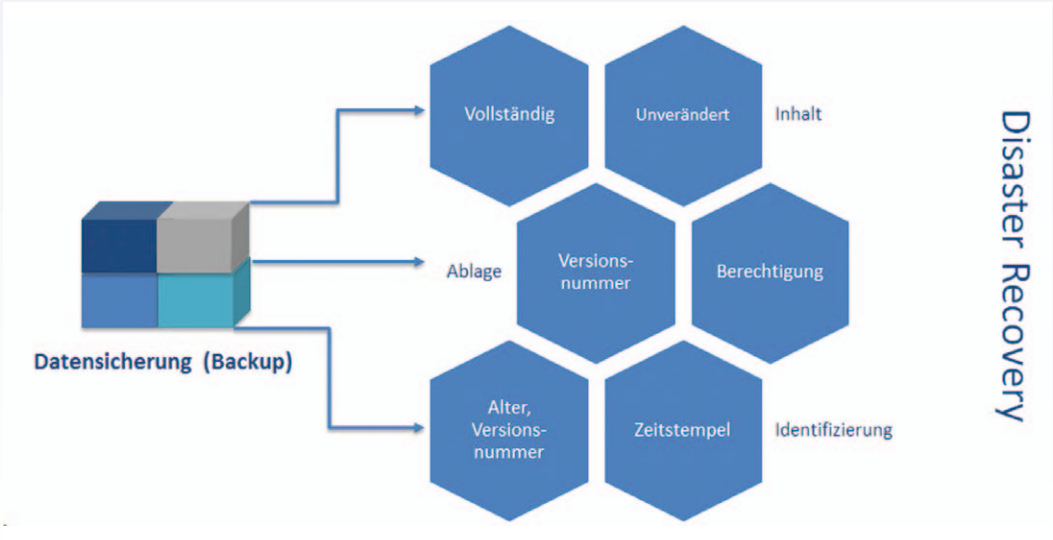

Bild 3: Darstellung der Klassifizierung einer Datensicherung in der Produktion nach Inhalt, Ablage und Identifizierung für ein Disaster Recovery, Copyright by Auvesy GmbH & Co. KG