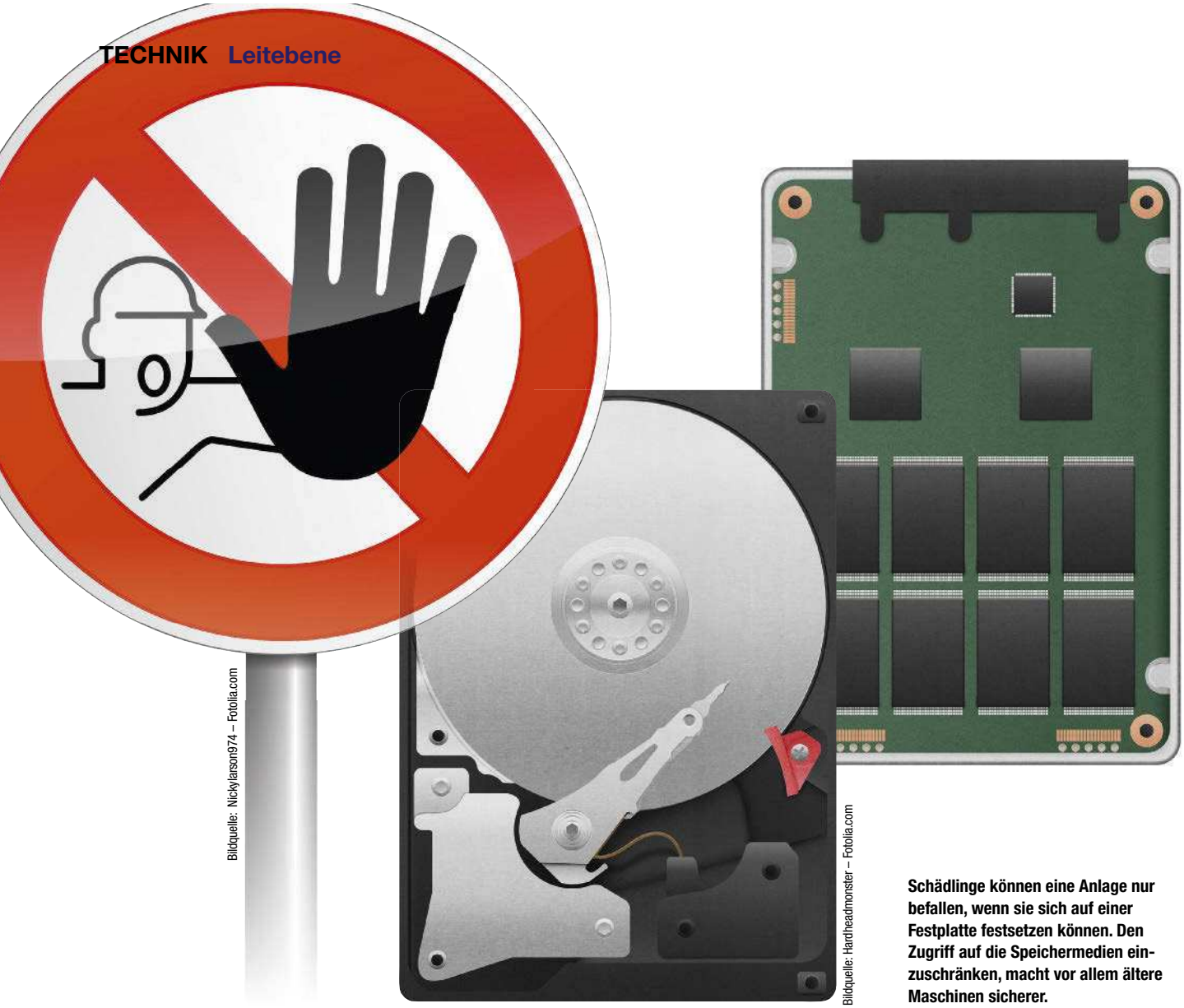


Bildquelle: Nickylarson974 – Fotolia.com

Bildquelle: Hardheadmonster – Fotolia.com

Schädlinge können eine Anlage nur befallen, wenn sie sich auf einer Festplatte festsetzen können. Den Zugriff auf die Speichermedien einzuschränken, macht vor allem ältere Maschinen sicherer.

Security

Kein Zugriff

Scada-Systeme und Industrial Control Systems (ICS) laufen häufig noch auf alter Hardware, die sich nur schwer oder gar nicht vor Cyber-Attacken schützen lässt. Doch es gibt eine einfache Schutz-Möglichkeit: den unautorisierten Zugriff auf die Festplatten sperren. Wo Daten nicht geschrieben und gelesen werden können, kann sich keine Schad-Software festsetzen und kein Hacker Daten absaugen.

Im Industrieumfeld greifen bewährte Sicherheitsmaßnahmen wie Application Whitelisting und regelmäßige Betriebssystem-Updates aufgrund des administrativen Zusatzaufwands nicht. Der Software-Hersteller Abatis hat deswegen Abatis HDF entwickelt. Diese Software setzt dort an, wo bewährte Sicherheitsmaßnahmen wie Antivirus, lokale Firewalls, Whitelisting und regelmäßige Betriebssystem-Updates nicht mehr helfen. HDF steht für Hard Disk Firewall, die lokal auf dem zu schützenden System installiert wird. Sie ermöglicht, bislang ungesicherte oder schwach gesicherte ältere Systeme vor Schad-Software und Hackerangriffen zu schützen – und zwar ohne den Einsatz von Virensignaturen, Heuristiken und Scanner-Durchläufen. Die Festplatten-Firewall dreht den Spieß um und nutzt eine Schwachstelle jeder Malware: Jeder Schadcode benötigt einen Schreibzugriff auf den Datenträger. Aber wie unterscheidet die Festplatten-Firewall zwischen schädlichen Schreibzugriffen und ungefährlichen? Die Antwort: Sie unterscheidet gar nicht – weil sie es nicht muss. Auch sie verwendet im Prinzip eine Positiv-Liste, in der die erlaubten Schreib-

Technik im Detail

Das Grundproblem

Scada-Systeme lassen sich über einen langen Zeitraum hinweg auch mit alten Betriebssystemen wie Windows NT4, Windows 2000 oder Windows XP Embedded betreiben. Doch dies erweist sich sicherheitstechnisch als großer Nachteil. Denn diese älteren Systeme sind anfällig für Schad-Software oder Hacking-Attacken. Aber genau solche Angriffe kommen in den vergangenen Jahren immer häufiger vor. 2014 war es die Malware-Familie Havex, die für Aufsehen sorgte, weil sie vor allem Scada- und Industrial-Control-Systeme im Visier hatte. Die Mehrheit der von Havex attackierten Firmen ist in Europa ansässig, vor allem in Deutschland, Frankreich und Belgien. Ziel der Hacker war es, über kompromittierte Systeme an sensible Daten zu kommen oder gar die Kontrolle über die Anlagen zu erlangen.

Sicherheitslücken in Industrienetzen können heutzutage relativ leicht entstehen, zum Beispiel wenn ein Wartungstechniker versehentlich mit einem verseuchten USB-Stick arbeitet. Da die Systeme in der Regel untereinander vernetzt sind, breitet sich der Schadcode dann schnell und unbemerkt auch auf andere Anlagenteile aus. Störungen und Produktionsausfälle, physische Schäden durch Sabotage oder Industriespionage sind die möglichen Folgen.

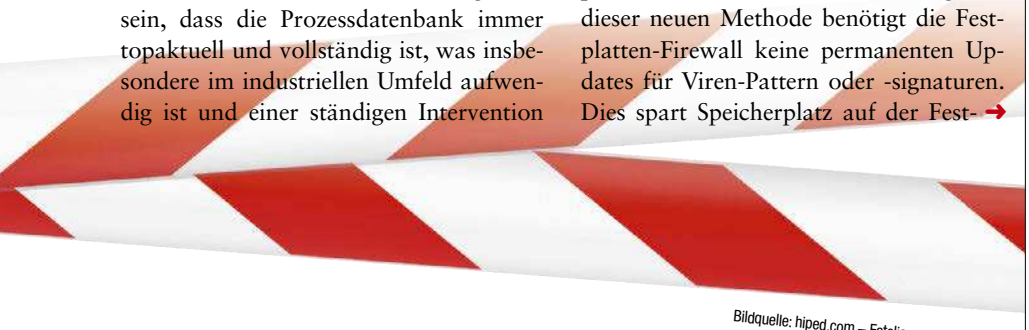
Hinzu kommt: Im April 2014 stellte Microsoft den Support für sein Betriebssystem Windows XP ein. Die IT-Sicherheit von Unternehmen, die gezwungen sind, nach wie vor alte Betriebssysteme einzusetzen, ist seitdem gefährdeter als zuvor, weil für diese Betriebssysteme keine Sicherheits-Updates mehr bereitgestellt und neue Sicherheitslücken somit nicht mehr geschlossen werden. Allerdings sehen viele Unternehmen von einem Wechsel des Betriebssystems aus verschiedenen Gründen ab, unter anderem weil auf der oft älteren Hardware der Steuerungssysteme neue Betriebssysteme wie Windows 8.1 nicht funktionieren.

zugriffe hinterlegt sind. Es gibt jedoch entscheidende Unterschiede zum klassischen Whitelisting-Verfahren – auch Process-Whitelisting genannt. Bei der klassischen Methode werden alle guten Prozesse in einer zentralen Datenbank eingepflegt und mithilfe von Prüfsummen identifiziert und klassifiziert. Die Prüfsummen der laufenden Prozesse werden mit der Datenbank abgeglichen. Stimmen die Prüfsummen nicht überein stuft die Datenbank den Prozess als gefährlich ein und blockiert ihn.

Klassisches Whitelisting versus Festplatten-Whitelisting

Dieses Verfahren hat mehrere Nachteile: So ist die Wahrscheinlichkeit, dass auch ungefährliche Prozesse geblockt werden, relativ hoch. Denn Anwendungen ändern sich regelmäßig, zum Beispiel durch Updates. Hier ändern sich wiederum auch deren Prüfsummen, und unbekannte Prüfsummen werden bei Whitelisting-Verfahren standardmäßig geblockt. Ein weiterer Nachteil: Es muss sichergestellt sein, dass die Prozessdatenbank immer topaktuell und vollständig ist, was insbesondere im industriellen Umfeld aufwendig ist und einer ständigen Intervention eines Administrators bedarf. Zwangsläufig wird die Datenbank größer und größer, was zunehmend Speicherressourcen frisst. Nicht zuletzt ist das klassische Whitelisting-Verfahren langsam, da bei jeder Aktion Datenbankabfragen erfolgen müssen – schon wenn ein PC oder System gestartet wird oder ein neuer Prozess anläuft.

Der größte Unterschied zur HDF-Methode ist: Die Festplatten-Firewall blockiert niemals Prozesse. Das bedeutet, alle Anwendungen können immer ausgeführt werden, auch wenn sie selbst oder deren Prozesse unbekannt sind. Stattdessen geht die Festplatten-Firewall einen anderen Weg. Sie blockiert die Schreibzugriffe von Prozessen auf Datenträger wie Festplatten oder USB-Sticks und verhindert so, dass verseuchte Anwendungen Malware auf den Datenträger schreiben. Dieses Verfahren ist wirksam, da eine Schad-Software niemals erfolgreich arbeiten kann, wenn sie sich nicht auf einem lokalen Datenträger kopieren oder dort Manipulationen vornehmen kann. Aufgrund dieser neuen Methode benötigt die Festplatten-Firewall keine permanenten Updates für Viren-Pattern oder -signaturen. Dies spart Speicherplatz auf der Fest- →



Bildquelle: hiped.com – Fotolia.com

platte. Ebenso wenig sind Scandurchläufe oder das Überwachen des Arbeitsspeichers auf Schadcodes notwendig – beides Schutzverfahren, die verhältnismäßig viel Prozessor- und Speicherlast erzeugen, was sich gerade auf älteren Systemen schnell negativ bemerkbar macht. Sogenannte False Positives gehören ebenso der Vergangenheit an wie das Ausnutzen von Zero Day Exploits.

Festplattenzugriffe zentral verwalten

Für die zentrale Konfiguration steht die ‚Central Management Console' zur Verfügung, die zum Beispiel auf einem Windows Server installiert werden kann. Ergänzend wird auf dem zu schützenden System ein Kommunikations-Agent installiert. So ermöglicht die Konsole das Aktivieren und Deaktivieren des HDF-Schutzes. Die Konsole zeigt den Status der verschiedenen Clients und gespeicherte Log-Files an. Über die Benutzerverwaltung lassen sich unterschiedliche Benutzerrollen vergeben: Beispielsweise kann ein Administrator Richtlinien verwalten, Rechte vergeben, Benutzer anlegen oder die Festplatten-Firewall permanent deaktivieren, während ein Support-Mitarbeiter den Schutz nur temporär für die Installation einer neuen Software deaktivieren darf.

Ein Nebeneffekt: Datenträger-Schreibvorgänge erfolgen bei den meisten Betriebssystemen und Anwendungen fast permanent. Dadurch gehört der lokale Datenträger neben dem Prozessor zu den größten Energieverbrauchern im System. Aufgrund der geringeren Schreibvorgänge auf die ausschließlich für den Betrieb benötigten Verzeichnisse sinkt der Energieverbrauch. *(mf)*

Autor

Erik Stengert
ist Produktmanager HDF bei der Secion GmbH in Hamburg.

infoDIREKT **776iee0215**

www.all-electronics.de
Link zum Unternehmen

Steuerung

Internet-Fernwartung ohne Projektänderungen

Deltalogic: In der aktuellen Version unterstützt die Fernwartungs-Software Accon-Teleservice IE alle gängigen Windows-Betriebssysteme einschließlich 64-Bit-Systeme. Die Software ermöglicht den zuverlässigen Fernzugriff auf S7-Steuerungen, ohne Änderungen am Projekt. Gerade bei Fernwartungslösungen über das Internet ist es meist aufwendig, den Adressraum mehrerer Teilnehmer zu verwalten. Die Herausforderung besteht darin, dass im Falle der S7-Steuerung aufgrund des verwendeten TCP/IP-Protokolls hinter einem Router nur ein Teilnehmer über die eindeutig definierte Port-Adresse zu erreichen ist. In diesem Fall hilft die Software. Da sie eine Aufschlüsselung für die korrekte Weiterleitung aller Portnummern und IP-Adressen an interne Portnummern enthält, ermöglicht sie den direkten Zugriff auf verschiedene S7-Steuerungen – die Projektierungsdaten können unangetastet bleiben. Ein transparenter Austausch von Daten ist sowohl für einzelne Teilnehmer als auch für komplette Netzsegmente möglich. Der Router übersetzt dann automatisch die Portnummern und IP-Adressen, sodass nun mehrere Teilnehmer von außen über dessen IP-Adresse erreichbar sind.

infoDIREKT **706iee0115**

www.all-electronics.de
Link zum Produkt

Bildquelle: Deltalogic