issa | INTERNATIONALE VEREINIGUNG FÜR SOZIALE SICHERHEIT | IVSS

Sektion für Maschinen- und Systemsicherheit

Sichere Passwörter

im Kleinbetrieb

Factsheet
Nº 2

Ein Beispiel aus der Praxis

Der Süßwarenhersteller „Keks und Schokolade“ stellt mit 16 Angestellten im Zweischichtbetrieb u.a. Schokoriegel mit einer Keksfüllung her. Eines Tages stellt die interne Qualitätssicherung fest, dass die produzierten Riegel eine ungewöhnliche Verfärbung aufweisen. Eine nähere Untersuchung ergibt, dass in den produzierten Riegeln eine zu große Menge Salz enthalten ist. Sofort wird die Produktion gestoppt. Dennoch ist die komplette Tagesproduktion betroffen. Die Maschine kann aufgrund von weiteren Untersuchungen für mehrere Tage nicht mehr verwendet werden.

Was war geschehen?

Nachforschungen zur Fehlerursache ergaben, dass die eingestellte Rezeptur während der laufenden Produktion geändert wurde. Die Maschine, die die Zutaten einwiegt, verfügt über einen Remote-Maintenance-Zugang. Dieser Zugang wurde nach der Installation der Maschine nicht deaktiviert, so dass die Maschine permanent mit dem Internet verbunden war. Der Betreibende hatte auch vergessen, das Standardpasswort für den Wartungszugang zu ändern.

Das Fazit

Offensichtlich wurde die Rezeptur über das Internet verändert. Die Firma war Opfer eines Hackerangriffs geworden. Die Geschichte klingt unglaubwürdig? Solche oder ähnliche Vorfälle kommen immer häufiger vor. Die steigende Bedeutung des Themas Cyber Security verdeutlichen aktuelle Berichte des Bundesamts für Sicherheit in der Informationstechnik (BSI). Danach besitzen Geräte und Maschinen mit Internetanbindung in deutschen Unternehmen immer noch viele Sicherheitslücken. Und täglich werden mehr als 350.000 neue Schadprogramme registriert. Keiner kann es sich heute noch erlauben, das Thema Cyber Security bei der Entwicklung oder dem Betreiben einer Maschine zu vernachlässigen.

Sind Sie sicher, dass so etwas bei Ihnen nicht vorkommen kann?

Eine Störung oder ein Ausfall von IT-Systemen kann sehr schnell zu Imageverlust, Produktionsausfall oder größeren Schäden, einschließlich Personenschäden, führen. Ein vernünftiger IT-Schutz ist dagegen schon mit verhältnismäßig einfachen Mitteln zu erreichen.

Deswegen: Ergreifen Sie wichtige Basismaßnahmen!

Basismaßnahmen für Maschinen oder Geräte mit Internetverbindung

Wählen Sie ein geeignetes Passwort

Die einfachsten Maßnahmen wären, alle nicht verwendeten Ports zu deaktivieren, hierzu zählen auch USB, Bluetooth oder W-LAN, und die Maschine nur mit dem Internet zu verbinden, wenn dieses erforderlich ist.

Ein geeignetes Passwort anstelle des voreingestellten Standard-Passworts ist in vielen Fällen das entscheidende Mittel, um sich gegen unerwünschte Zugriffe zu schützen.

Die neuesten Empfehlungen für ein gutes Passwort zielen nicht mehr auf Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen, sondern empfehlen ganze individuelle Sätze mit vielen Zeichen.

Eine Möglichkeit, ein zufälliges Passwort zu generieren, sind sogenannte Hash-Generatoren. Aus dem Satz „Ich gehe nach Hause." wird mit der SHA-256 Methode das Passwort:

„840de88a9e6e282089fc1ad5b49b5f6cdc4b4598810f8769af6ed4544b2c333d"

Da die Hashmethode einen definierten Algorithmus enthält, ist das Passwort bei allen Hashgeneratoren bei Eingabe desselben Wortes bzw. Satzes identisch.
Da man sich solche Passwörter nicht mehr merken kann, empfiehlt es sich die Passwörter in sogenannten Passwort-Tresoren zu hinterlegen (z.B. KeePass 2). Der Vorteil ist, dass man sich nur noch ein Master-Passwort für den Tresor merken muss, um auf alle gespeicherten Passwörter zuzugreifen.

Passwörter, die von Hackern bevorzugt getestet werden, um sich illegal Zugang zu verschaffen, sind mittlerweile bekannt. Wenn Sie Ihr eigenes Passwort testen wollen, können Sie das z. B. unter folgendem Link:
https://haveibeenpwned.com/Passwords

Wer ist verantwortlich?

Für die Sicherheit von Maschinen und Geräten im Internet sind Herstellfirma und Betreiber verantwortlich.

Der **Betreiber** muss die üblichen Vorsichtsmaßnahmen treffen, um das eigene Netzwerk vor Viren und anderen Bedrohungen zu schützen. Dazu gehören neben der richtigen Passwortwahl ein Virenscanner mit aktuellen Virensignaturen, eine Firewall und vor allem die richtige Einstellung des Routers. Wichtig ist auch, Betriebssystem und Anwenderprogramme regelmäßig auf dem neuesten Stand zu halten.
Eine Trennung zwischen dem Büro- und Produktionsnetz ist ebenfalls sehr sinnvoll.

Der **Hersteller** von Geräten und Maschinen mit Internetverbindung muss das maschineneigene Netzwerk ebenfalls absichern und die Möglichkeit vorsehen, nicht verwendete Ports zu deaktivieren.

Es sind Voraussetzungen für die Eingabe von Passwörtern geschaffen, die nicht durch wenige Versuche „erraten" werden können. Die Länge des Passworts ist nicht der einzige entscheidende Faktor für die Sicherheit.

Möglich ist auch die sogenannte Zwei-Faktor-Authentifizierung. Dafür gibt es mehrere Methoden. Beliebt ist ein (relativ) einfaches Passwort und ein einmalig gültiger, dynamischer Code. Diesen Code erhält man per SMS, E-Mail oder über eine entsprechende App bei jedem Anmeldeversuch auf sein Smartphone.

Möglich ist auch die verzögerte Eingabe eines Passworts nach einer Fehleingabe. Dazu sperrt das Programm die Passworteingabe nach einer Fehleingabe um einige Sekunden. Nach der zweiten Fehleingabe wird die Wartezeit verdoppelt, und so weiter. Damit kann schon bei relativ einfachen Passwörtern das Knacken des Passworts so zeitaufwändig werden, dass der Hacker aufgibt.

Auch die Verwendung biometrischer Daten (Fingerabdruck, Gesichtserkennung) wäre möglich, wird aber bisher in diesem Bereich selten angeboten.

Weitergehende Informationen

1 **Bundesamt für Sicherheit in der Informationstechnik:**
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

2 **Allianz für Cybersicherheit:**
https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Grundschutz-Profile/it-grundschutz-profile_node.html

3 **Webseite „Kompetenzzentrum Digitales Handwerk“:**
https://handwerkdigital.de/

8 Tipps zur Verbesserung der Cyber-Sicherheit in Ihrem Unternehmen

1. Halten Sie Betriebssystem, Anwendungsprogramme, Router und Firewall auf dem neuesten Stand und nutzen Sie Virenscanner mit täglich aktualisierten Virensignaturen.
2. Ersetzen Sie Standardpasswörter bei der ersten Benutzung durch eigene, sichere Passwörter.
3. Schützen Sie Ihre Passwörter gegen Zugriff durch Unbefugte.
4. Unterweisen und sensibilisieren Sie Ihre Mitarbeitenden im richtigen Umgang mit Computern, vernetzten Maschinen und Passwörtern.
5. Führen Sie ein effektives Berechtigungsmanagement ein, indem Sie festlegen, welche Mitarbeiter auf welche Systeme und Maschinenfunktionen Zugriff haben.
6. Achten Sie beim Kauf von Maschinen und Geräten mit Internetzugang darauf, dass diese die Voraussetzung für eine sichere Vernetzung mitbringen.
7. Deaktivieren Sie nicht verwendete Ports.
8. Schaffen Sie für Ihre Mitarbeitenden die Möglichkeit, Passwörter sicher zu speichern.

issa | INTERNATIONALE VEREINIGUNG FÜR SOZIALE SICHERHEIT | IVSS

Sektion für Maschinen- und Systemsicherheit

IVSS Sektion
Maschinen- und Systemsicherheit

Projektgruppe Digital Manufacturing

Dynamostraße 7–11 · 68165 Mannheim
Deutschland
Telefon: +49 (0) 621 4456 2213
Fax: +49 (0) 3212 1419 443

www.safe-machines-at-work.org

AUVA

BGN
Berufsgenossenschaft
Nahrungsmittel und Gastgewerbe

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

INAIL
ISTITUTO NAZIONALE PER L'ASSICURAZIONE CONTRO GLI INFORTUNI SUL LAVORO

suva

TECHNICAL UNIVERSITY OF KOŠICE

UNIVERSITY of GREENWICH