issa | INTERNATIONALE VEREINIGUNG FÜR SOZIALE SICHERHEIT | IVSS

Sektion für Maschinen- und Systemsicherheit

Cyber Security

im Kleinbetrieb

Factsheet
Nº 1

Ein Beispiel aus der Praxis

Die Bäckerei-Konditorei „Süß und Knusprig“ stellt mit 10 Angestellten Pralinen her. Eines Tages geht an der Verpackungsmaschine die Folien-Schweißeinheit ohne Vorwarnung in Flammen auf. Und das noch während der Pause! Glücklicherweise wird das Feuer schnell bemerkt und der Brand kann noch in seiner Entstehungsphase gelöscht werden. Dennoch ist der Schaden erheblich.

Was war geschehen?

Nachforschungen zur Brandursache ergaben, dass die Solltemperatur der Schweißeinheit auf einen viel zu hohen Wert eingestellt war: oberhalb der Entzündungstemperatur der Folie! Dies führte zum Brand. Nachdem Elektronikversagen ausgeschlossen werden konnte, stellte der Experte fest, dass die Maschine dauerhaft mit dem Internet verbunden war. Ein Mitarbeiter von „Süß und Knusprig“ hatte die Maschine über den Router verbunden, da er die empfohlene Fernwartung (Remote Maintenance) nutzen wollte – damit hatte der Hersteller die Maschine beworben und eine Reparatur binnen 24 h versprochen. Der Mitarbeiter hatte aber vergessen, das voreingestellte Passwort zu ändern.

Das Fazit

Die Bäckerei „Süß und Knusprig“ war Opfer eines Hackerangriffs geworden, denn offensichtlich war die Solltemperatur über das Internet manipuliert worden. Die Geschichte klingt unglaubwürdig? Solche oder ähnliche Vorfälle kommen immer häufiger vor. Die steigende Bedeutung verdeutlichen aktuelle Berichte des Bundesamts für Sicherheit in der Informationstechnik (BSI). Danach besitzen Geräte und Maschinen mit Internetanbindung in deutschen Unternehmen immer noch eine hohe Anzahl an Sicherheitslücken. Und täglich werden mehr als 350.000 neue Schadprogramme registriert.

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 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

Ziehen Sie den Stecker

Die einfachste Maßnahme ist es, den Stecker zu ziehen und die Internetverbindung zu unterbrechen, wenn sie nicht benötigt wird. Weil das in der Praxis oft nicht möglich ist, muss der Zugang auf andere Weise gesichert werden.

Wählen Sie ein geeignetes Passwort

Ein geeignetes Passwort ist in vielen Fällen das entscheidende Mittel, um sich gegen unerwünschte Zugriffe zu schützen. Zeichenfolgen wie „0000“, „12345“ oder „qwertz“ sind natürlich nicht geeignet.

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. Ein gutes Passwort wäre demnach z. B.:

WennMorgenSchönesWetterIstGeheIchMitDemHundGassi

Wichtig ist, dass die Sätze individuell und einfach zu merken sind. Denn ein Passwort, das man sich nicht merken kann, führt zum Schummeln. Das Passwort klebt dann am Bildschirm oder liegt in der Schublade. Auch der regelmäßig erzwungene, nervige Wechsel des Passworts wird nicht mehr gefordert.

Es gibt sogenannte „Blacklists“ mit Passwörtern, die von Hackern bevorzugt getestet werden, um sich illegal Zugang zu verschaffen. 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 Hersteller und Betreiber verantwortlich

Der Betreiber, also Sie, muss die üblichen Vorsichtsmaßnahmen treffen, um das eigene Netzwerk von Viren und anderen Bedrohungen frei zu halten. 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.

Der Hersteller von Geräten und Maschinen mit Internetverbindung muss das interne Netzwerk ebenfalls absichern. Bei der Anschaffung einer Maschine sollten Sie darauf achten, dass dies umgesetzt ist. Sie erkennen das beispielsweise an folgenden Merkmalen:

Es sind Voraussetzungen für die Eingabe von Passwörtern geschaffen, die nicht durch wenige Versuche „erraten" werden können. Die Sicherheit muss dabei nicht unbedingt über die Länge des Passworts erzeugt werden.

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/

6 Tipps zur Verbesserung der Cyber-Sicherheit in Ihrem Unternehmen

1. Halten Sie soweit möglich Betriebssystem, Anwendungsprogramme, Router und Firewall auf dem neusten 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 Mitarbeiter im richtigen Umgang mit Computern und vernetzten Maschinen.
5. Führen Sie ein effektives Rechtemanagement 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.

issa | INTERNATIONALE VEREINIGUNG FÜR SOZIALE SICHERHEIT | IVSS

Sektion für Maschinen- und Systemsicherheit

IVSS Sektion
Maschinen- und Systemsicherheit

Dynamostraße 7–11
68165 Mannheim
Deutschland
Telefon: +49 (0) 621 4456 2213
Fax: +49 (0) 621 4456 2190

www.safe-machines-at-work.org