

Mehr betriebliche Sicherheit – mit einem verlässlichen Partner an der Seite

Wussten Sie, dass SIGNAL IDUNA 1906 von selbständigen Handwerkern und Gewerbetreibenden gegründet wurde? Genau deshalb proklamiert die SIGNAL IDUNA für sich, die Ansprüche und Wünsche des Mittelstandes so gut wie kaum ein anderes Versicherungsunternehmen zu kennen. Manuel Attig fasst es treffend zusammen: „Profitieren Sie von unserer über 100-jäh-

rigen Erfahrung und versichern Sie Ihr Unternehmen mit uns.“

Speziell für die Mitglieder des FDPW wurde eine eigene Webseite eingerichtet: www.fdpw-versicherungsservice.de

Nutzen auch Sie die Vorteile dieses auf Ihre Bedürfnisse zugeschnittenen Rahmenvertrages und nehmen Sie Kontakt mit Ihrem FDPW-Versicherungsservice auf. ■

WEITERE INFORMATIONEN

SIGNAL IDUNA Generalagentur Attig

Tel.: +49 228-3-69-8750

ga-attig@signal-iduna.net

MEHR SICHERHEIT FÜR IHRE IT

Gefahren aus dem Netz gezielt abwehren.

Der Erpressungstrojaner „WannaCry“ hat im Mai die Welt in Atem gehalten. Er infizierte hunderttausende Rechner und richtete immensen Schaden an. Telefonnetze waren betroffen, Automobilproduktionen ruhten und sogar Operationen in Krankenhäuser mussten verschoben werden. Experten warnen, dass es immer neue Angriffe auf Sicherheitslücken geben wird. Ein Grund mehr, die IT im eigenen Unternehmen genauer unter die Lupe zu nehmen und den Fokus deutlicher auf das Thema „Sicherheit“ zu lenken.

Der Welt wird vernetzter und smarter und der Digitalisierungsprozess schreitet voran. Auch in Werkzeugschleifbetrieben sind eine leistungsfähige IT und die Nutzung des Internets mittlerweile unverzichtbar. Während das Hauptaugenmerk vor allem auf Geschwindigkeit, Effizienz, Vernetzung und Mobilität liegt, wird das Thema IT-Sicherheit gleichzeitig oft vernachlässigt. Das ist angesichts der vielfältigen Bedrohungen von außen fatal. Denn, soviel steht fest, je vernetzter, desto höher ist das Risiko.

Die Unternehmensgröße spielt keine Rolle, wenn es um Hacker, Cyberkriminalität und Virenangriffe geht – funktioniert die IT nicht mehr, liegen viele Geschäftsprozesse brach. Die Auswirkungen des aktuell kursierenden Erpressungstrojaners namens „WannaCry“, der unzählige Windows-Rechner infiziert, Inhalte verschlüsselt und Lösegeld erpresst hat, zeigen deutlich, dass es immer wieder Sicherheitslücken gibt, über die ein solcher Angriff sattfinden kann.

„Die Abläufe im modernen Handwerksbetrieb sind heutzutage ohne die Nutzung von Informations- und Kommunikationstechnologien kaum denkbar. Das durchzieht das ganze Unternehmen, von der Auftragsannahme bis zur Produktion an hochmodernen Maschinen“, so Stephan Sachweh, Geschäftsführer von der Pallas GmbH aus Brühl. Sei dieses Konstrukt gestört, entstünden Kosten, die sich vermeiden ließen.

Was man selbst machen kann

Jani Nakos, IT Berater von Pallas empfiehlt, sich zunächst auf grundlegende Sicher-

heitsregeln zu besinnen: „Das fängt damit an, Sicherheitsupdates bei Verfügbarkeit aufzuspielen. Damit man nichts verpasst, sollte man regelmäßig in den Windows-Update Einstellungen nachsehen und diese dann zeitnah einpflegen.“

Beide IT-Experten verweisen zusätzlich auf die Unverzichtbarkeit von Backups. Dabei sei es wichtig darauf zu achten, dass die Daten auf einem externen Speichermedium gesichert werden, wie zum Beispiel auf externen Platten. „Und diese sollten nach der Speicherung sofort vom Rechner beziehungsweise vom Netz getrennt werden“, so Jani Nakos, „sonst können sie natürlich auch befallen werden!“

Stephan Sachweh erinnert noch einmal daran: „Öffnen Sie nur E-Mails oder Anhänge von Ihnen bekannten Absendern und fragen Sie, falls Sie sich nicht sicher sind, immer nochmal persönlich nach, ob die Anhänge so richtig sind.“ Verdächtig seien zum Beispiel Dateitypen mit den Endungen .exe, .asf, .mov, .mpg und .pif.

„Natürlich ist ein Virenschoner unverzichtbar. Es gibt gute Systeme, die man schon für wenig Geld im Abo buchen kann“, ergänzt Jani Nakos. Diese böten zwar keinen hundertprozentigen Schutz aber in Kombination mit allen anderen Maßnahmen ergänzen sie ein gut funktionierendes Sicherheitsnetz.

Neues Angebot für FDPW Mitglieder

Die Angreifbarkeit der IT-Systeme von kleinen Werkzeugschleifbetrieben, ist eine Problematik, die auch im FDPW schon länger bekannt ist. Aus diesem Grund wurde nach einer praktikablen und einfachen Lösung gesucht, um die Mitglieder auch in dem Bereich IT-Sicherheit unterstützen zu können.

„Wir wissen einfach, dass das Thema IT-Sicherheit bei vielen unserer Mitgliedsbetriebe nicht im Vordergrund steht. Einfach aus dem Grund, weil dies nicht Tagesgeschäft ist. Dennoch ist fast allen bewusst, dass sie etwas unternehmen müssen, zumal die Bundesregierung bzw. die EU ein neues Datenschutzgesetz auf den Weg gebracht hat. So muss bis Mai 2018 jedes Unternehmen größer neun Mitarbeiter über einen Datenschutzbeauftragten verfügen, der unter der Verantwortung der

Unternehmensleitung dafür Sorge tragen muss, dass Daten geschützt sind und bleiben“, so FDPW Geschäftsführer Prof. Dr.-Ing. Wilfried Saxler. Deshalb habe man sich entschlossen, eine Kooperation mit dem Unternehmen für IT-Sicherheit Pallas GmbH einzugehen.

Über Pallas können Verbandsmitglieder zu FDPW-Sonderkonditionen das Internet-Schutz-Paket 3protect beziehen, welches zuverlässig drei Einfallstore für Angriffe aus dem Internet überwacht:

1. Emailschutz: Abwehr von Spam und Emailviren mit modernster IP-Reputation in Real-Time und mehrstufigem Spam- und Virenfilter, echte Security aus der Cloud

2. Webschutz: Schutz vor gefährlichen Webseiten und Webviren, klassischer Virenfilter und Real-Time URL-Filter gegen Gefahren sogar bei Deep Links, echte Security aus der Cloud

3. Netzwerkschutz: Abwehr von Angriffen auf das Firmennetzwerk durch eine führende Hardware-Firewall, vor Ort installiert und zentral überwacht.

Mitarbeiter von Pallas steuern den Betrieb und die Überwachung der Sicherheitslösung im Rahmen eines festdefinierten Leistungs- und Preispakets.

Durch eine schnelle Integration passend konfigurierter Hardware sowie die Nutzung dieses zentralen Managed Security Services, müssen sich die Betriebe nicht mehr um die Internet-Security kümmern. Pallas ist TÜV-zertifiziert und nach deutschem Datenschutz geprüft.

„Es war an der Zeit, das Dienstleistungsangebot des Verbandes durch ein solches Modul zu erweitern. Das mit uns abgestimmte Leistungspaket 3protect passt sehr gut zu unseren kleinen und mittelständischen Betrieben und ist auf ihre Bedürfnisse abgestimmt“, so Wilfried Saxler. ■

WEITERE INFORMATIONEN

FDPW Geschäftsstelle
info@fdpw.de

✓ Halten Sie Ihre Systeme auf neuestem Stand und spielen Sie regelmäßig Sicherheitsupdates auf.

✓ Aktueller Virenschutz ist unverzichtbar, so können Sie Infektionen vorbeugen.

✓ Machen Sie regelmäßig Backups auf externen Speichermedien und trennen Sie diese vom Netz. Prüfen Sie auch, ob Sie die Daten aus einer Sicherung Wiederherstellen können.

✓ Verwenden Sie nur sichere Passwörter und achten Sie darauf, sie regelmäßig zu ändern. Benutzen Sie ggf. einen Passwort-Manager, um möglichst viele verschiedene Passwörter zu verwalten.

✓ Öffnen Sie keine verdächtigen Mails beziehungsweise verdächtige Dateianhänge und Links. Selbst wenn die Mails von Ihnen bekannten Adressen stammen, bietet das keine Sicherheitsgarantie.

✓ Achten Sie darauf, dass Microsoft Office keine Makros ausführt.

✓ Starten Sie keine ausführbaren Dateien, die Ihnen nicht hundertprozentig vertrauenswürdig erscheinen.

✓ Lassen Sie keine Unbekannten „zu Wartungszwecken“ aus der Ferne auf Ihren Rechner zugreifen.

✓ Schulen Sie Ihre Mitarbeiter entsprechend, damit sich alle an die Regeln halten.



CHECKLISTE