CORONAVIRUS
INFO-SERVICE FÜR BETRIEBE

INFOPOINT

Wie man Betriebe vor Cyberattacken schützen kann

Dass in Zeiten virus-bedingter Lockdowns nicht nur der Mensch, sondern auch die IT verstärkt Schutz braucht, zeigt eine Vielzahl brisanter Cyberrisiken. Im Rahmen der WKOÖ-Webinar-Reihe „Digital vernetzt & ausspioniert" teilte IT-Sicherheitsspezialist FH-Prof. Kolmhofer deshalb sein Wissen mit zahlreichen Interessierten.

20.01.2021, 14:11

© ADOBE STOCK

Die Bedeutung von Cybersicherheit für Betriebe wächst mit neuen Lockdown-bedingtenAnforderungen.

Anfang letzten Jahres begann ein bis dato zumeist unbekannter, mikroskopisch kleiner Virus die Sicherheit von Menschen rund um den Globus in Frage zu stellen. Das hatte weitreichende Konsequenzen: Spätestens seit den ersten Lockdowns übertrug sich die Sicherheitsthematik schnell auch auf IT-Systeme. Plötzlich musste aufgrund neuer Anforderungen vieles improvisiert werden, Notfallpläne waren aber oft nicht ausreichend vorhanden. Es wurde vermehrt im Homeoffice gearbeitet, bis dahin geordnete IT-Verhältnisse wurden teils obsolet, es kam verstärkt zu Ausfällen von Personal, externen Dienstleistern und mehr – ein Nährboden für vielfältige Formen von Cyberkriminalität, auch in Oberösterreich. Es gilt daher mehr denn je, Betriebe gegen Angriffe auf die IT zu wappnen.

WKOO-Webinar für mehr Sicherheit in Betrieben

Aus diesem Grund luden WKOÖ, Branchenverbund Consulting, IT-Cluster, FHOÖ, und JKU LIT Open Innovation Center im Rahmen der On- und Offline-Serie „Digital vernetzt & ausspioniert" Cyber-Security-Experten Professor Robert Kolmhofer von der FH Hagenberg zu einem interaktiven Webinar ein. Kolmhofer ist Leiter des Departments Sichere Informationssysteme und allgemein beeideter und gerichtlich zertifizierter Sachverständiger der Informatik und Nachrichtentechnik. Zudem leitet er die UNINETit consulting GmbH Hagenberg/Linz, die u. a. ein Spezialist für IKT-Consulting, Informationssicherheit, Cyber Security, IT/OT Security und ISO27001/TISAX ist. Nicht nur das mehr als gute Feedback der 241 angemeldeten TeilnehmerInnen der Veranstaltung lässt auf hohe Aktualität des Themas schließen. Auch die Ergebnisse der brandneuen Studie „Global Digital Trust Insights Survey 2021" von PwC belegen den starken Bedeutungszuwachs von Cybersicherheit. Die Umfrage spiegelt die Ansichten von 3.249 Führungskräften aus Wirtschaft und IT weltweit wider.

Cyberrisiken von Kunden, Lieferanten, Cloud-Diensten & Plattformen

Laut Kolmhofers Vortrag ist es während der Lockdowns letzten Jahres in Oberösterreich bereits zu einigen Fällen von Cybersicherheitsbedrohungen für Industrie und Dienstleister gekommen. Dies betraf v. a. mittelgroße Betriebe, in denen Professionalität der IT-Abteilungen und Cyber-Security-Strategien nicht zeitgleich mit verwendeter IT „mitgewachsen" sind, schilderte er. Unternehmen nutzen Netzwerke, Datenbanken und Cloudservices. Durch Updates kann manipulierte Software (z.B. mit Trojaner verseucht) so verteilt werden und landet leicht in vielen tausenden Unternehmen. Cloud Provider, Netzwerkprovider und sogar Softwarehersteller (Entwicklerkonten kompromittiert, Diebstahl von Sourcecode, ...) waren bereits Opfer solcher Attacken, wie der Referent mitteilte. Endkunden und sogar Regierungsbehörden sowie deren Provider und Dienstleister wurden angreifbar. Es hat Monate gedauert, bis ein solcher Angriff erkannt, analysiert und dann letztendlich gestoppt werden konnte, so Kolmhofer.

Wo liegen die größten Sicherheitsrisikos für Betriebs-IT?

Kolmhofer schilderte weiter, wo die größten Risiken für die IT-Sicherheit von Betrieben liegen. Outsourcing von Kern IT-Services beispielsweise kann dazu führen, dass betriebsintern im Krisenfall kein ausreichendes IT-Know-How vorhanden ist. Dadurch wird die Ressourcenverfügbarkeit von Externen abhängig. Fehlende Datensouveränität gefährdet somit die Verfügungsgewalt über eigene Daten. Als weitere Risikoquelle nannte der Security-Experte die Nutzung von Privatgeräten im Homeoffice. Diese verfügen oft über keine aktuellen Virenscanner und schlechte bis keine Passwortsicherheit. Über VPN haben Angreifer uneingeschränkten Zugang zu Endgeräten im Betrieb, und es kann zu unkontrollierter Nutzung von Services (Cloud, ...) kommen. Nicht minder gefährlich sind laut Kolmhofer schlechte IT „Lösungen" im B2B und B2C-Bereich. Hierbei sind „offene" Remote-Zugänge, fehlende Passwortsicherheit und Multi Faktor-Authentifizierung sowie die Nutzung von Cloud- und Webservices ohne Securityprozesse sehr problematisch.

Empfehlungen zur Schließung von Sicherheitslücken

Kolmhofer empfiehlt u. a. „Insourcing" von Kern-IT, Stärkung von eigenen IT-Abteilungen und Unterstützung im Fachkräftebedarf, sorgfältige Dienstleisterauswahl sowie Planung von Notfallprozeduren. Zudem ist der Expertenmeinung nach höhere Informationssicherheit durch eine Business Impact Analyse als Basis für IT-Security-Maßnahmen sehr sinnvoll. Dabei wird eine Bewertung des Geschäftsprozesses zur Festlegung der Wiederanlaufparameter vorgenommen. Es stellt sich diesbezüglich die Frage, welche Ausfälle das Unternehmen am härtesten treffen würden, um dahingehend resilienter werden zu können. Notfallmanagement ist die unumgängliche Basis für sicheren Geschäftsbetrieb, so Kolmhofer.

Weiter rät er zu strikter Trennung von Enterprise Netzwerken und Produktionsnetzwerken zur Verhinderung einer Ausbreitung von Angriffen im Netzwerk. In der Praxis ist diese Trennung noch selten anzutreffen, in einigen Industrieunternehmen aufgrund von Vorfällen aber in ersten Ansätzen vorhanden, teilte der Experte mit. Generell empfiehlt Kolmhofer, den Stand der eigenen Technik mit aktuellen Standards abzugleichen. Dies ist z. B. mit Hilfe von BSI-IT-Grundschutz Katalogen und BSI-Grundschutz-Kompendium, Standards des Deutschen Bundesamts für Sicherheit in der Informationstechnik, dem Österreichischen Informationssicherheitshandbuch und der Handreichung von TeleTrust zum „Stand der Technik" möglich, schloss er seinen Vortrag.

www.wk-events.at/ooe/it-security/home

Das könnte Sie auch interessieren

Es muss auch in die Energieinfrastruktur investiert werden

Die Sparte Industrie der WKO Oberösterreich steht dem geplanten Ökostromausbau grundsätzlich positiv gegenüber und bekennt sich zu den äußerst ambitionierten klima- und energiepolitischen Zielen. › mehr

Gut beraten in die Zukunft

Im Rahmen der Veranstaltung „Future of Consulting" wartete der Branchenverbund Consulting mit Unterstützung der Aussenwirtschaft Austria und des Export Centers OÖ mit brandaktuellem Wissen zum Thema Innovation und Transformation auf. Seine Expertise brachte u. a. Innovations-Spezialist Prof. Gassmann von der Uni St. Gallen ein. › mehr