IT-Sicherheit – Bedrohungslage durch Corona zugespitzt

13
PROZENT

der befragten Unternehmen hatten in den vergangenen **zwölf Monaten einen Sicherheitsvorfall**.

TÜV Cybersecurity-Studie 2019

Phishing, Schadsoftware, Trojaner, Ransomware, Datenklau und Identitätsdiebstahl, Cyber-Attacken aller Art – das sind Probleme, denen wir schon vor Corona am liebsten nie begegnen wollten. Leider sah die Realität immer schon anders aus – und das Problem hat sich durch die krisenbedingt eiligen organisatorischen Veränderungen und die beschleunigte Digitalisierung vehement verschärft. Welche Fehler am weitesten verbreitet sind, wo besondere Risiken liegen und was man tun kann, um sie möglichst zu vermeiden – darüber sprach das Wirtschaftsmagazin Pfalz mit Experten aus unserer Region.

Über digitale Angriffe berichteten 2018 und 2019 laut Bitkom 70 Prozent der deutschen Unternehmen. Schäden in Milliardenhöhe sind die Folge. Zu nennen sind neben Systemausfällen, einer geringeren Produktivität und nicht zugänglichen Diensten für Kunden häufig auch Schäden für die Reputation des Unternehmens oder andere Wettbewerbsnachteile, hieß es im vergangenen November bei der Vorstellung einer gemeinsamen Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des TÜV-Verbandes. Nicht zu vergessen sind aber auch mögliche Haftungsprobleme durch fahrlässigen Umgang mit Sicherheitsthemen.

Angela Wahl-Knoblauch, Prokuristin des IT-Dienstleisters Demando in Kaiserslautern

Die Corona-Krise hat die Bedrohungslage massiv zugespitzt. Die von heute auf morgen verordnete Arbeit im Homeoffice für große Teile einer nun örtlich verteilten „Remote-Belegschaft“ hat die Kreativität von Cyberkriminellen zusätzlich angefacht. Viele kleine und mittlere Unternehmen (KMU) sind darauf nicht genug vorbereitet. „Unternehmen, die noch nicht so gut auf mobiles Arbeiten vorbereitet waren, hatten mit erheblichen Anlaufschwierigkeiten zu kämpfen“, schildert Angela Wahl-Knoblauch, Prokuristin des IT-Dienstleisters Demando in Kaiserslautern, die Lage. Doch auch wenn die Krise die weitere Digitalisierung in den Unternehmen stark beschleunigt, müsse IT-Sicherheit immer den Vorrang vor schnellen Lösungen haben, um Schäden zu vermeiden.

Volker Bentz, Chef des IT-Systemhauses Brandmauer IT in Bellheim, warnt eindringlich, dass Cyberkriminelle die momentane Situation schamlos ausnutzen und Unternehmen, die keine ausreichenden Schutzmaßnahmen getroffen haben, zunehmend angegriffen werden. In einer Zeit, in der viele Unternehmen sowieso schon ins Trudeln geraten sind oder zumindest unter starkem Druck stehen, könne dies für manche den Ruin bedeuten.

Private Geräte im Homeoffice – Gefahr für Unternehmen

„Wir bekommen derzeit mit, wie Unternehmen auch aus unserer Region zunehmend Opfer von Cyber-Attacken und hier oft von Phishing oder Ransomware werden“, erzählt IT-Experte Bentz. Gerade in Corona-Zeiten habe sich die Situation stark verschlimmert.

Fotos: DEMANDO | BRANDMAUER IT | stock.adobe.com – Bits and Splits

Die plötzlich und unvorbereitet zu mehr Digitalisierung gezwungenen und auf diese Situation nicht eingestellten Unternehmen schicken ihre Leute teilweise ins Homeoffice. Im schlimmsten Fall sind diese mit einem USB-Stick ausgerüstet, auf dem sensible Daten vom Firmen-PC auf ein privates Gerät übertragen und dort bearbeitet werden. Entweder weil man über die damit verbundenen Gefahren nicht Bescheid weiß oder weil Lieferengpässe die Beschaffung von mobilen Endgeräten wie Notebooks, Laptops & Co. zur Ausrüstung der Homeoffices erschweren. Was da in Sachen Datenschutz teilweise aus dem Ruder gelaufen ist, wird nur schwer wieder einzufangen sein, glaubt der Fachmann.

„Oft sind die privaten Geräte lediglich mit kostenlosen Antivirus-Programmen ausgerüstet, die nur das Mindeste leisten, während eine gute Antivirensoftware im Jahr schon mal um die 35 Euro oder auch deutlich mehr kostet. Zwischendurch haben die Kinder der Remote-Mitarbeitenden auf demselben Gerät auf unsicheren Seiten gesurft, später werden hier dann Firmendaten bearbeitet." Das Computervirus, das man sich dabei eventuell eingefangen hat, wird bei der nächsten Kommunikation an das Firmennetzwerk weitergereicht.

Höchstes Augenmerk auf IT-Sicherheit legt man auch bei Demando – schon weil mit Energieversorgern auch Kritische Infrastrukturen zu den Kunden des IT-Dienstleisters mit eigenem Rechenzentrum gehören. Hier sind die Anforderungen an IT-Sicherheit – wie vom Gesetzgeber vorgeschrieben – besonders hoch, und kommunale Unternehmen schon von der Unternehmenskultur her nicht unbedingt auf mobiles Arbeiten oder Homeoffice-Betrieb eingestellt. In der Krise

Volker Bentz, Geschäftsführer des IT-Systemhauses Brandmauer IT GmbH in Bellheim

Unternehmer-Frühstück IT-Strategie

Wer IT-Fehlentscheidungen vermeiden und dauerhaften Nutzen aus IT-Investitionen ziehen möchte, sollte eine IT-Strategie entwickeln – auch im Mittelstand. Eine gelungene IT-Strategie sollte sich an den Bedürfnissen des Unternehmens orientieren und aktiv neue geschäftliche Chancen ermöglichen. Kommen Sie beim Unternehmer-Frühstück am 14. Oktober von 9 bis 11 Uhr bei der IHK Pfalz in Ludwigshafen mit einem ausgewiesenen IT-Experten ins Gespräch und entwickeln Sie erste Ideen für Ihre IT-Strategie. Weitere Informationen und Anmeldung unter

www.pfalz.ihk24.de, Nummer 149132941.

musste aber schnell gehandelt werden – der Notfallplan sah vor, dass ein Teil der 500 Mitarbeiter im Büro, die anderen von zuhause arbeiten mussten.

Die IT-Dienstleister waren in dieser Zeit extrem gefordert, das mobile Arbeiten unter Berücksichtigung aller bereits geltenden IT-Sicherheitsmaßnahmen zu ermöglichen. Daher wurden keine privaten Geräte zugelassen, nur Firmen-Hardware, die zentral gemanagt und überwacht wird. „Wir setzen Device-Lock-Management ein: Alle USB-Ports werden überwacht und zentral verwaltet, sodass zum Beispiel über USB-Sticks keine Schadsoftware ins Netzwerk kommt oder Daten abgezogen werden können. Mit der Ende-zu-Ende-Verschlüsselung übertragener Daten stellen wir sicher, dass nur die Kommunikationspartner eine Nachricht entschlüsseln können“, erläutert Wahl-Knoblauch wichtige Maßnahmen.

Fazit der IT-Experten: Private Geräte, die nicht unter der Hoheit der IT-Abteilung stehen, sollte man niemals ins Firmennetzwerk einbinden. Auch wenn das billiger ist oder schneller geht, als firmeneigene PCs oder Laptops zur Verfügung zu stellen. Der Virenschutz sollte von den zuständigen Administratoren konfiguriert und überwacht werden, sodass sofort professionell reagiert werden kann, wenn mal etwas passiert. Hard- und Software kann man übrigens auch mieten, wenn man nicht kaufen will. Oder man kann IT-Leistungen von vornherein outsourcen.

Wie man sich beraten und fördern lassen kann, wenn man Digitalisierungsprojekte starten oder die IT-Sicherheit verbessern will, neue Geräte oder Software anschaffen will oder mehr Homeoffice-Arbeitsplätze anbieten möchte, lesen Sie in unserem Beitrag über einschlägige Förderprogramme auf Seite 15. Die IHK Pfalz bietet zu dem Thema spezielle Förder-Sprechtage an, berät aber auch gern individuell.

Regelmäßige Updates und Backup – mehr als eine lästige Pflicht

Ein zu lässiger Umgang mit Themen wie Updates und Backup ist ein weiteres Problem. Schadsoftware („Malware“) schlägt besonders gern zu, wenn der PC über eine Sicherheitslücke angreifbar ist. Sind auf dem Rechner Programme wie PDF-Reader, Videoplayer und andere Zubehörsoftware installiert? Dann bitte genau hinsehen – denn wenn man diese nicht regelmäßig updatet, ist die Sicherheitslücke schon da. „Viele Nutzer klicken die Update-Hinweise weg, weil sie gerade unpassend kommen, und vergessen die Systemaktualisierung dann“, beobachtet Bentz, „das kann schlimme Folgen haben.“ Zum Beispiel eine Attacke mit sogenannter Ransomware, mit deren Hilfe Cyberkriminelle die IT-Systeme einer Organisation lahmlegen und die Unternehmen dann zur Zahlung eines Lösegeldes erpressen.

Eines der nach eigenen Angaben sichersten und modernsten Rechenzentren Europas und hohes Know-how der Mitarbeiter in den Bereichen IT-Betrieb, Anwendungslösungen, Betreuung und Beratung: Damit punktet Full-Service-IT-Dienstleister Demando in Kaiserslautern.

Foto: Demando / Ewa Weimer

Grafik: stock.adobe.com – Fotomay

Ein solcher Verschlüsselungsangriff kann laut Branchenkennern schon mal eine halbe Million Euro kosten.

Besonders wenn im Unternehmen kein regelmäßiges, korrektes Backup ausgeführt wird, die Daten also tatsächlich erstmal nicht zugänglich sind, geraten viele, wenn nicht gar die meisten Opfer in Versuchung, das Erpressungsgeld tatsächlich zu zahlen. Davon hält Bentz nicht viel. Nicht nur, weil man damit das Geschäftsmodell der Verbrecher am Laufen hält: Man kann ziemlich sicher sein, dass das Firmennetzwerk nicht mehr vertrauenswürdig ist. Im Falle eines erfolgreichen Angriffs muss die Integrität des Netzwerks wiederhergestellt werden. Das geht nur, wenn man alles neu und sauber installiert. Und das funktioniert am besten, wenn die Firmendaten nicht wirklich verloren sind, weil man das Thema Backup wichtig genug genommen hat. ■ *(Kira Hinderfeld)*

Coronabedingte Unsicherheit führt zu steigendem Informationsbedarf

Auch wenn grundsätzliche Aspekte der IT-Sicherheit wie die vernünftige Ausstattung von Homeoffices, regelmäßige Updates und kluge Backups berücksichtigt werden – die Corona-Krise sorgt für weitere Fallstricke. Daraus kann dann schnell ein Paradies für Cybercrime werden.

Besonders kritisch wird es, wenn aus Unwissenheit oder Sorglosigkeit die IT-Sicherheit im Hause sowieso schon nicht hundertprozentig ist und dann noch eine große persönliche Unsicherheit wegen Corona hinzukommt. „Die Menschen sind geradezu süchtig nach den aktuellsten Informationen über Corona-Wirtschaftshilfen, das Infektionsgeschehen, interaktiven Karten von Verbreitungsgebieten, neuen Erkenntnissen, Tipps und dergleichen“, beobachtet Volker Bentz von Brandmauer IT. Da werden schon mal Webseiten angeklickt, die man besser nicht besuchen sollte, und Mails geöffnet, die von Verbrechern verschickt worden sind. Leider haben sich die Cyberkriminellen auch weiterentwickelt. „Die früher stümperhaft gemachten Phishing-Mails sehen heute total seriös aus und sind manchmal selbst von IT-Fachleuten erst auf den zweiten Blick zu erkennen“, berichtet der Bellheimer IT-Spezialist.

Der Trend zu immer „besseren“ Spam-Mails setzt sich auch aus Sicht von Demando definitiv weiter fort: „Wir konnten auf unseren Systemen zum Beispiel für den Juli feststellen, dass 80 Prozent der eingehenden Mails bösartig waren. Jeden Monat werden also über eine Million solcher Mails von unseren Sicherheitssystemen erkannt und herausgefiltert. Diese Viren richten sich zumeist gegen Office-Anwendungen. „Emotet-Viren sind dabei weiterhin sehr beliebt bei den Angreifern“, beobachtet Angela Wahl-Knoblauch.

So warnt auch die Verbraucherzentrale zum Beispiel vor betrügerischen E-Mails angeblich von der Sparkasse und anderen Banken, worin Kunden zur Eingabe ihrer persönlichen Daten aufgefordert werden. Es wird behauptet, dass die Übermittlung dieser Daten notwendig sei, um in der Corona-Krise per Chat mit der Bank in Verbindung bleiben zu können oder in den Genuss von Vorteilen wie dem Wegfall der Kontoführungsgebühr zu kommen. Über einen Link werden Betroffene auf eine authentisch aussehende Eingabemaske geleitet, die die Daten nach der Eingabe direkt an Betrüger sendet, die dann das Konto leerräumen oder andere Straftaten begehen können. Aber auch bekannte Institutionen wie die WHO oder das RKI werden von Angreifern gern als vermeintliche Absender missbraucht, um Nutzer auf harmlos aussehende, aber veränderte Seiten zu locken, wo ihre Daten und Identitäten abgegriffen werden. ■ *(kh)*

Schutzmaßnahmen gegen Ransomware

Besonders perfide arbeitet der Trojaner „Emotet“ mit seinem hoch komplexen Angriffsweg. Vereinfacht gesagt, liest die auf Ihren Rechner gelangte Vorbereitungs-Software Kontakte aus, kapert den E-Mail-Verkehr und schickt Ihnen bekannt aussehende, also harmlos wirkende Dokumente samt dem eigentlichen Virus. Der wiederum verschickt dann weitere Malware – von Ihrem Rechner aus.

Wie man sich gegen „Emotet“ und andere Ransomware schützen kann, zeigt zum Beispiel der Ratgeber von Brandmauer IT unter

www.brandmauer.de

> Wir wollen als IHK **IT-Security Awareness** bei unseren Unternehmen schaffen.
>
> Christiane Huber, IHK Pfalz

Problembewusstsein schärfen – sich nicht als Opfer anbieten!

Zu glauben, das Problem treffe nur andere, nur weil kein Bekannter einen solchen Angriff erlebt hat, ist ein Fehler. Insbesondere weil es eine hohe Dunkelziffer von Betroffenen geben dürfte, die sich gar nicht outen.

Falko Faschon, Vorstandsvorsitzender der 4S IT-Solutions AG, Kaiserslautern.

Weg vom Papier und persönlichen Kontakten, hin zu digitalen Prozessen: Corona zwingt die Unternehmen dazu, immer stärker zu digitalisieren. Angesichts der derzeitigen steilen Zunahme von Malware wie Trojanern, Ransomware, DDoS- oder Phishing-Attacken in der Größenordnung von über 300.000 neuen Schadprogrammen pro Tag gewinnen die Themen Compliance und Sicherheit durch die Digitalisierung also eine ganz neue Dimension. Das Problembewusstsein ist aber derzeit noch unterentwickelt. „Wir halten es für eine ganz wichtige Aufgabe der IHK, bei diesem Thema stets am Ball zu bleiben, immer wieder auf die Probleme hinzuweisen und IT-Security Awareness bei unseren Unternehmen zu schaffen“, sagt Christiane Huber, bei der IHK Pfalz für Innovation und Digitale Wirtschaft zuständig. Das A und O für Unternehmen ist, sich permanent gut zu informieren und auch den Wissensstand der Mitarbeiter durch Information und Schulung up-to-date zu halten.

Je schwerer man es einem Cyberkriminellen macht, Sicherheitsmaßnahmen zu überwinden, desto mehr Zeit muss er dafür investieren – und desto weniger rentiert es sich für ihn. Aus Sicht von Experten sind dabei Security-Awareness-Trainings für die Mitarbeiter genauso wichtig wie ein guter, aktueller Virenschutz. Ein einziger sorgloser Mitarbeiter reicht, um ein Unternehmen zu gefährden. „‚Ich wollte nur mal ausprobieren, was passiert, wenn ich da klicke‘, hat mir ein User sorglos erzählt“, so Volker Bentz von Brandmauer IT. Von den Kriminellen werde oft auf die menschliche Neugier gesetzt, und das funktioniere leider zu oft sehr gut.

Hier setzt das Angebot der 4S IT-Solutions AG in Kaiserslautern an. Mit dem Ziel, das Sicherheitsbewusstsein und den Wissensstand von Mitarbeitern in Unternehmen zu erhöhen, bietet das Systemhaus unter anderem Phishing-, Social-Engineering- und Awareness-Kampagnen an, um Fehlverhalten aufzuspüren und gezielt zu bekämpfen. Dabei werden Angriffsszenarien in Unternehmen nachgestellt, die Ergebnisse analysiert und in Optimierungsansätze für die eingesetzte IT-Technik und die Ausbildung des Personals überführt. „Wir wollen erreichen, dass die Mitarbeiter perspektivisch als erste Verteidigungslinie – quasi als Firewall – gegen Angriffe fungieren können“, blickt Vorstandsvorsitzender Falko Faschon in die Zukunft.

■ *(kh)*

Foto: stock.adobe.com – vegefox.com | Harald Krähler

(Un)Sicherheitsfaktor Mensch

Das größte Risiko für die IT-Sicherheit sitzt 50 Zentimeter vor dem Bildschirm. Das zumindest behaupten viele Experten. Die gute Nachricht: Der menschliche Faktor lässt sich absichern – auch und speziell im Homeoffice.

„Die drei wichtigsten Faktoren für IT-Sicherheit heißen Datensicherung, Datensicherung und Datensicherung“, resümiert Gunnar Schwarz, Inhaber von Schwarz-IT in Waldfischbach-Burgalben, keineswegs im Scherz. Er weiß aus Erfahrung mit seinen Firmenkunden, dass jede hausgemachte IT-Panne nur halb so wild ist, wenn man ein Backup hat, oder besser noch zwei an jeweils unterschiedlichen Aufbewahrungsorten.

Sorglosigkeit öffnet Tür und Tor

Noch immer herrschen bei IT-Sicherheit Naivität und Unsicherheit auf Seiten der Anwender – was nicht sichtbar ist, gerät schnell in Vergessenheit. „Wer keine Security Awareness – also ein Bewusstsein für Sicherheit – trainiert, muss verstärkt mit dem Sicherheitsrisiko Mensch rechnen“, betont der westpfälzische IT-Experte. Nach seiner Erfahrung ist es tatsächlich häufig die fehlende oder ungeprüfte Datensicherung und der unbedachte Umgang damit, der zu Sicherheitslücken führt. Dazu kämen Fehlbedienungen wie das sorglose Herunterladen von Internet-Inhalten oder das Öffnen von Spam-Mails. „Vorsatz ist in der Praxis selten, meist führt Unachtsamkeit zu Systemversagen.“

Sicherheitslücken tun sich laut Schwarz nicht erst im Tagesgeschäft auf, häufig ist bereits die IT-Systemstruktur anfällig, etwa wenn es keine stringente Berechtigungsstruktur gibt und Mitarbeiter Zugriff auf Daten haben, auf die sie keinen haben sollten, und dort größeren Schaden anrichten können. „Hier kann der Arbeitgeber organisatorisch viel abfangen“, so Schwarz. Er rät außerdem zu regelmäßigen Schulungen und Webinaren. Die Mitarbeiter sollten sich zum Beispiel sicher sein, welche Daten sie an Dritte weitergeben dürfen und welche nicht: „Denken Sie etwa an die gefälschte E-Mail vom Chef, der angeblich auf einer Geschäftsreise Bargeld braucht.“

Sichere Passwörter einfach generieren

Auch ein „Werkzeugkasten“ für den IT-Notfall hilft laut Schwarz in akuten Situationen. „Für unsere Kunden haben wir Leitfäden entworfen, was zum Beispiel bei Virenbefall zu tun ist.“ Ebenso gibt es eine detaillierte Anleitung, wie Mitarbeiter sichere Passwörter generieren können: Sie sollten einmalig für die betreffende Anwendung sein, nicht eines für alle. Da sie Groß- und Kleinbuchstaben, Zahlen sowie Sonderzeichen enthalten sollten, bildet man am besten einen Satz, den man sich leicht merken kann, und nimmt die Anfangsbuchstaben der Wörter: 3KEmS# steht für „Drei Kugeln Erdbeereis mit Sahne#“. Darin kann man dann sogar Abkürzungen etwa für Onlinebanking (OB) oder PC für Anmeldung am PC verstecken: 3KEOBms# oder 3KEPCmS#. Damit hat man unterschiedliche Passwörter, an die man sich leicht erinnern kann. ■ *(mara)*

Fan in- und externer Datensicherung: Gunnar Schwarz, Inhaber von Schwarz-IT, in Waldfischbach-Burgalben.

Firmenfoto

Tipps für mehr IT-Sicherheit

- Einen IT-Sicherheitsbeauftragten oder externen Berater einsetzen
- Komplexe Passwörter ohne persönlichen Bezug wählen
- Wo möglich, Mehrfaktor-Authentifizierungen nutzen
- Regelmäßig Updates vornehmen
- Backup: regelmäßig vornehmen und prüfen, Zweitkopie außer Haus
- Vorsicht bei dubiosen Mails und Anfragen
- Informationen von in- und externen Sicherheitsexperten praktisch umsetzen
- Dokumentation inklusive Notfallplanung ständig aktualisieren

Keran Sivalingam ist KI-Trainer im Mittelstand-4.0-Kompetenzzentrum Kaiserslautern.

Künstliche Intelligenz – gut oder böse?

Künstliche Intelligenz (KI) ist oft im Spiel, wenn es um Schadsoftware geht, und zwar einerseits bei der Automatisierung und Personalisierung von Cyberangriffen und auf der anderen Seite bei deren Abwehr beziehungsweise zur Identifizierung von Schadsoftware oder Anomalien in Datenströmen. KI kommt aber auch in modernen Authentifizierungsverfahren zum Einsatz, etwa bei der Gesichts- oder Spracherkennung.

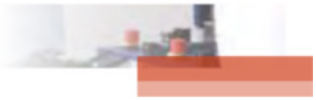
„Phishing-Mails werden immer besser und schwerer zu entdecken“, sagt Keran Sivalingam, KI-Trainer beim Mittelstand-4.0-Kompetenzzentrum Kaiserslautern (siehe dazu auch Seite 17). Seine wichtigste Aufgabe ist es, kleine und mittlere Unternehmen über die Nutzungsmöglichkeiten von KI zu informieren und für die diversen Problematiken zu sensibilisieren. Dazu lädt das Kompetenzzentrum Pfälzer Unternehmen – oft in Zusammenarbeit mit der IHK, aber auch mit Wirtschaftsförderungen, Handwerkskammern und weiteren Multiplikatoren – zu Vorträgen und Schulungen über aktuelle Themen ein.

Identitätsdiebstahl ist ein großes Problem, von dem die meisten schon gehört haben dürften: Die Schadsoftware gibt sich zum Beispiel für den abwesenden Chef aus und leitet Gelder um. Oder sie bestellt als vertrauter Absender teure Produkte bei einem Lieferanten, die dann niemals im Unternehmen ankommen. Möglich wird dies dadurch, dass sensible Daten von Cyberkriminellen ausgelesen werden – sehr oft, indem die Sorglosigkeit von Mitarbeitern ausgenutzt wird, die ein harmlos wirkendes Bild anklicken oder auf einer gehackten Internetseite landen. Ganz perfide: Bot-Netzwerke kapern fremde Rechner und nutzen sie, um andere anzugreifen. Dass der eigene Rechner betroffen ist, merkt man oft daran, dass er unerklärlich langsam wird oder man Mails von der eigenen Adresse mit eigenartigem Inhalt erhält. Auch DDoS-Attacken sind mit KI nochmal deutlich gefährlicher geworden. Besonders für produzierende Unternehmen, die in der Produktion zum Beispiel Cloud-Server nutzen, können diese Angriffe existenzbedrohend sein. Sivalingam empfiehlt, sich mit dem Hersteller der jeweiligen Produktionsanlage über geeignete Schutzmaßnahmen auszutauschen. ■ *(kh)*

Blick in das Mittelstand-4.0-Kompetenzzentrum Kaiserslautern. Mehr zum Angebot des Zentrums auf Seite 17.

Fotos: Firmenfoto/A. Sell

Neue Transferstelle **IT-Sicherheit im Mittelstand**



Das Bundeswirtschaftsministerium hat mit der Transferstelle IT-Sicherheit im Mittelstand (TISiM) eine neue, spezialisierte Anlaufstelle für IT-Sicherheit geschaffen. Die Pilotphase läuft seit Mitte September, der offizielle Startschuss fällt zum Jahreswechsel.

Für die pfälzische Wirtschaft ist die IHK Pfalz regionale Anlaufstelle. Die TISiM bündelt bundesweit Angebote zur IT-Sicherheit – kostenfrei und unverbindlich. Mit einem Sicherheitscheck wird der Bedarf ermittelt und eine Empfehlung ausgesprochen. Das Ergebnis ist ein individueller Aktionsplan. Anbieter von IT-Sicherheitslösungen können ihre Angebote bei der TISiM anmelden. ■ *(kh)*

www.tisim.de

Lassen Sie sich **fördern!**

Unternehmen, die ihre IT-Sicherheit verbessern wollen oder Digitalisierungsprojekte starten, sollten die wichtigsten Förderprogramme kennen. Wichtig zu wissen: Förderprogramme sind immer an Kriterien gebunden, einige richten sich an Unternehmen mit bis zu 100 Mitarbeitern, andere an solche mit bis zu 249 oder bis zu 499 Mitarbeitern. Weitere Kriterien sind zum Beispiel der Jahresumsatz und wie lange das Unternehmen bereits am Markt ist. Besonders wichtig ist, Projekte erst zu beginnen, nachdem sie beantragt und genehmigt wurden. Die IHK Pfalz bietet eine persönliche, telefonische oder virtuelle Orientierungsberatung zu Förderprogrammen an. ■ *(kh)*

Das rheinland-pfälzische **BITT-Programm** fördert bis zu 15 Beratertage mit bis zu 50 Prozent der Kosten, insgesamt bis zu 6.000 Euro. Beispiele sind technologieorientierte Beratungen oder Beratungen bei der Einführung spezieller EDV und Informationstechnik.

Seit September fördert das Programm **Digital jetzt** Investitionen in digitale Technologien. Voraussetzung ist ein Digitalisierungsplan, der den aktuellen Stand, die Ziele und das Gesamtvorhaben darlegt.

unternehmensWert:Mensch plus stellt mit einer Förderquote von bis zu 80 Prozent den Menschen in den Mittelpunkt. Die regionale Erstberatungsstelle ist an der Hochschule für Wirtschaft und Gesellschaft in Ludwigshafen. Das Programm kann auch von Kleinstunternehmen genutzt werden. Beispiele sind personalpolitische oder arbeitsorganisatorische Veränderungsprozesse im Rahmen des digitalen Wandels.

Das Bundesprogramm **go-digital** fördert mit bis zu 30 Tagen die drei Module Digitale Markterschließung, Digitalisierte Geschäftsprozesse und IT-Sicherheit. Beispiele sind der Aufbau einer professionellen, rechtssicheren Internetpräsenz, eines Web-Shops, die Einführung von E-Business-Software-Lösungen oder die Optimierung von betrieblichen IT-Sicherheitsmanagementsystemen.

KONTAKT

Christiane Huber

0621 5904-1530
christiane.huber
@pfalz.ihk24.de

Weitere Infos zum Thema IT-Sicherheit und Digitalisierung:

www.pfalz.ihk24.de/ihk-hub.

Oder klicken Sie sich in unsere XING-Gruppe „IHKhub – Unterstützung im digitalen Wandel".

IT-Dienstleistungen outsourcen – aber sicher!

Viele Unternehmen würden gerne externe IT-Dienstleistungen in Anspruch nehmen. Doch wie findet man einen guten Dienstleister und woran erkennt man ihn?

Die große Mehrheit der Unternehmen in Deutschland setzt bei ihrer IT auf externe Dienstleister. Insbesondere kleinere Unternehmen greifen bei Bereitstellung, Betrieb und Wartung ihrer IT-Infrastruktur oder zur Lösung alltäglicher IT-Herausforderungen auf externe IT-Experten zurück. Doch gerade für diese Unternehmen, die zudem häufig über keine eigenen IT-Fachkräfte verfügen, ist es wichtig, auf vertrauenswürdige Dienstleister zu setzen und die Prozesse mit Dienstleistern klar zu regeln.

Unter www.ihk.de/it-sicherheits-kriterien finden Interessierte einen Kriterienkatalog, der kleineren Unternehmen ohne eigene Sicherheitsexpertise bei der Auswahl eines vertrauenswürdigen IT-Dienstleisters hilft. Er gibt zudem erste Anregungen für die Aufnahme sicherheitsrelevanter Fragestellungen in Dienstleistungsvereinbarungen und erleichtert die Beurteilung, ob die internen Prozesse und Lösungen des IT-Dienstleisters unter dem Aspekt der IT-Sicherheit als vertrauenswürdig und verlässlich gelten können.

Den richtigen Dienstleister finden

Für kleine und mittlere Unternehmen (KMU), die keine eigene Stabsstelle für komplexe IKT- sowie IT-Sicherheits-Dienstleistungen schaffen oder dauerhaft unterhalten wollen und solche Dienstleistungen lieber zukaufen möchten, lohnt sich ein Blick in den „InnovationsMarkt Pfalz“ unter www.pfalz.ihk24.de/innovationsmarkt-pfalz.

Durch übersichtlich gestaltete Einträge erhalten Unternehmen mit Leistungsangebot und Kontaktdaten die wichtigsten Informationen über einen potenziellen Partner auf einen Blick. Pfälzer Experten können sich zudem in die neue Ausgabe online eintragen. ■ *(kh)*

Die beliebtesten **Cyber-Angriffe**

Nach den Ergebnissen der TÜV-Cybersecurity-Studie, die Ende 2019 veröffentlicht wurde, hatte gut jedes achte Unternehmen (13 Prozent) in den vergangenen 12 Monaten vor der Befragung einen IT-Sicherheitsvorfall.

Jedes vierte betroffene Unternehmen (26 Prozent) berichtet von **Phishing-Angriffen**, bei denen – in der Regel per E-Mail – Schadsoftware in die Organisation eingeschleust wird. An zweiter Stelle steht **Ransomware** (19 Prozent), mit deren Hilfe Cyberkriminelle die IT-Systeme einer Organisation lahmlegen und die Unternehmen dann erpressen.

Ein weiteres verbreitetes Phänomen ist **Social Engineering** (9 Prozent). Mitarbeiter werden gezielt manipuliert, um sich Zugang zu den IT-Systemen des Unternehmens zu verschaffen.

Weitere Angriffsszenarien sind **Man-in-the-Middle-, Passwort-** und **DDoS-Angriffe**. Diese sogenannten **Denial-of-Service-Attacken** bestehen aus einer Vielzahl von gezielten Anfragen, die einen Dienst lahmlegen.

Bei **Malware as a Service** bieten Cyberkriminelle ihr verbrecherisches Geschäftsmodell mittlerweile Unternehmen zum Kauf an, um deren Konkurrenten zu schädigen. Oder sie erpressen Geldzahlungen, um ein Internetangebot wieder nutzbar zu machen. ■ *(kh)*