IHK Das Magazin der IHKs Bodensee-Oberschwaben und Ulm

die WIRTSCHAFT

zwischen Alb und Bodensee

2| 2025
Ausgabe:
IHK Bodensee-Oberschwaben

Phishing, Ransomware, Trojaner & Co.

So schützen Sie Ihr Unternehmen vor Cyber-Kriminellen und Hacker-Angriffen


ThinkPad

Cyber-Sicherheit: Schutz vor Phishing, Ransomware & Co.

Cyber-Angriffe treffen Unternehmen unabhängig von ihrer Größe. Ob Ransomware, Phishing oder Angriffe auf Lieferketten – die Bedrohungen werden komplexer, und die Schäden sind gravierend. Um IT-Infrastruktur effizient zu schützen, braucht es einen ganzheitlichen strategischen Ansatz, der ein Bewusstsein für die Gefahren schafft und maßgeschneiderte technische Lösungen implementiert. Am Ende geht es nicht nur um Daten, sondern um Vertrauen.

Angela Lembcke, Sales Manager bei der SITS Deutschland GmbH in Ulm, weist darauf hin, dass die Mitarbeitenden auf allen Unternehmensebenen regelmäßig im Rahmen von Awareness-Kampagnen geschult werden sollten, um sie für IT-Sicherheit zu sensibilisieren.

Bild: Armin Buhl, Photodesign Armin Buhl

Norbert Hofmann ist ein großer Mann, breites Kreuz, eine echte Kante. Und wie er da so steht, wirkt er wie eine Fleisch gewordene Firewall, unüberwindbar für Cyber-Angriffe aller Art. Ein Antipode gegen die digitalen Teufeleien aus dem Darknet, gegen die Hacker dieser Welt. Tatsächlich ist Hofmann Experte für IT-Security mit mehr als 40 Jahren Berufserfahrung sowie Gründer und Geschäftsführer der meco IT GmbH in Weingarten. Er betreut mit seinem Team kleine und mittelständische Unternehmen zu IT-Sicherheit und -Infrastruktur. Und manchmal sind er und seine Mitarbeiter auch Retter in großer Not – dann, wenn der Ernstfall eingetreten ist.

Bild: Rolf Schultes, Drumlin Photos

Norbert Hofmann, Geschäftsführer von meco IT in Weingarten, betreut mit seinem Team vor allem kleine und mittelständische Unternehmen in Sachen IT-Sicherheit.

Zunehmende Professionalisierung in der Cyber-Kriminalität

Rund 39 Millionen infizierte Systeme, sogenannte Abuse Reports, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) im vergangenen Jahr allein in Deutschland dokumentiert – Tendenz steigend. Dabei sei der deutschen Wirtschaft 2024 ein Schaden in Höhe von 178,6 Milliarden Euro entstanden, rund 30 Milliarden Euro mehr als im Vorjahr, berichtet Bitkom, der Branchenverband der deutschen IT- und Digitalwirtschaft. Laut einer weiteren BSI-Analyse werden täglich mehr als 300.000 neue Schadprogrammvarianten entdeckt – ein alarmierender Hinweis auf die zunehmende Professionalisierung der Cyber-Kriminellen. Monströse Zahlen, die aufschrecken. „Es geht schon lange nicht mehr um die Frage, ob meine IT-Infrastruktur attackiert wird, sondern nur noch um das Wann und Wie", mahnt meco-IT-Chef Hofmann.

Hintertür ins System

„Ransomware und Phishing-Kampagnen bleiben die häufigsten und gefährlichsten Angriffe", weiß René Karcher, Geschäftsführer der SecuritySquad GmbH in Frickingen. Der Mann war einst beim Bundesnachrichtendienst beschäftigt und weiß genau, wie es in den Eingeweiden des globalen Cyberspace ausschaut und welche Gefahren dort lauern: „Solche Attacken richten oft erhebliche Schäden an und haben in den letzten Jahren signifikant zugenommen." SecuritySquad ist nach eigenen Angaben darauf spezialisiert, widerstandsfähige digitale Infrastrukturen vor allem für KMUs, Behörden und andere Organisationen zu schaffen.

Ransomware ist Schadsoftware, die heimlich eingeschleust wird. Sie eröffnet eine Hintertür ins System, Angreifer können sich in aller Ruhe umsehen, manchmal monatelang. Und wenn sie nicht rechtzeitig entdeckt werden, macht es irgendwann Klick, und alle Daten sind verschlüsselt, oft auch in den Backups. Phishing-Attacken kommen als E-Mails von scheinbar vertrauenswürdigen Absendern und zielen darauf ab, vertrauliche Informationen wie Passwörter abzuschöpfen. Die Daten werden manchmal im Darknet zum Kauf angeboten, oder es folgt eine Lösegeldforderung. Oder beides.

Gefahr droht auch von innen

Doch es droht auch Gefahr von innen – Risiko Schatten-IT: „Häufig nutzen Mitarbeiterinnen und Mitarbeiter private Anwendungen auf ihrem Bürorechner oder eigene Geräte, die nicht in das Sicherheitskonzept des Arbeitgebers integriert sind", stellt Angela Lembcke, Sales Manager bei der SITS Deutschland GmbH in Ulm, fest. Das Unternehmen ist auf Cyber-Sicherheit für große Mittelständler und Konzerne mit ihren teils globalen und komplexen Netzwerken spezialisiert. Mit Blick auf international aufgestellte Unternehmen zählt Lembcke auch Attacken auf die verschiedenen Lieferketten zu den größten Bedrohungen: „Solche Supply-Chain-Attacken auf Zulieferer oder Partnerunternehmen zielen darauf ab, den Angreifern Tür und Tor in die Systeme großer, eigentlich gut geschützter Unternehmen zu öffnen." Noch eher selten sind Schäden durch Attacken auf IoT-Geräte oder Deep Fakes und sogenannte Robo Calls, die vor allem durch die Verbreitung von Künstlicher Intelligenz einfacher werden, wie im Bitkom-Bericht nachzulesen ist.

> „Unternehmen sollten Gefahren realistisch einschätzen und in effiziente Schutzmaßnahmen investieren."
>
> Norbert Hofmann, Geschäftsführer der meco IT GmbH in Weingarten

IT-Sicherheit beginnt im Kopf

Die gute Nachricht: Es gibt Mittel und Wege, Unternehmen sowie IT-Infrastruktur und Daten effizient zu schützen. Aber wie? „IT-Sicherheit beginnt im Kopf", erklärt Hofmann. Viele Entscheider und Führungskräfte kleiner und mittelständischer Unternehmen (KMUs) gehen seiner Erfahrung nach immer noch davon aus, sie seien für Cyber-Attacken nicht interessant genug. Doch das Gegenteil ist der Fall: Gerade KMUs geraten immer mehr ins Visier der Angreifer, belegt die BSI-Dokumentation.

> „Ransomware und Phishing-Kampagnen bleiben die häufigsten und gefährlichsten Angriffe.“
>
> René Karcher, Geschäftsführer der SecuritySquad GmbH in Frickingen

Auch, weil die Angreifer die Schwachstellen von KMUs kennen: „Kleinstunternehmen fehlen nicht nur das technische Wissen, sondern oft auch die finanziellen Mittel, um grundlegende IT-Schutz- und Sicherheitsmaßnahmen effektiv umzusetzen“, erläutert IT-Experte Hofmann. Mittlere Unternehmen seien in der Regel zwar besser aufgestellt, „haben aber häufig keine ausreichend spezialisierten IT-Abteilungen und stoßen gerade bei komplexeren Anforderungen schnell an ihre Grenzen“. Vor allem aber sieht er eine Diskrepanz zwischen Eigenwahrnehmung und Realität: „Viele Geschäftsführer unterschätzen auf der einen Seite die Abhängigkeit ihres Unternehmens von einer funktionierenden IT-Infrastruktur. Und überschätzen auf der anderen Seite ihre IT-Sicherheit“, stellt Hofmann fest. Daher fordert er Unternehmensführer dazu auf, „ihr Bewusstsein für die Bedrohungen aus dem Cyberspace zu schärfen, die Gefahren realistisch einzuschätzen und in effiziente Schutzmaßnahmen zu investieren“.

Philipp König, Geschäftsführer der SSIG-IT GmbH in Blaubeuren, bläst ins selbe Horn. „IT-Sicherheit sollte nicht als Luxus verstanden werden, sondern als integraler Bestandteil einer verantwortungsbewussten Unternehmensführung“, betont er. Bereits nach einem einstündigen Impulsgespräch könnten erste Möglichkeiten skizziert und gemeinsam die Richtung bestimmt werden, das soll die Hemmschwelle senken. Die Mission seines Unternehmens: auch kleineren Unternehmen und Mittelständlern professionelle und erschwingliche IT-Sicherheitslösungen bereitzustellen.

Ganzheitlicher Ansatz für effizienten Schutz

Die vier Experten sind sich einig: Für einen effizienten Schutz der IT-Infrastruktur von Unternehmen braucht es einen ganzheitlichen Ansatz. Am Anfang steht eine fundierte Risikoanalyse: Wo sind die Schwachstellen, was sind die Kronjuwelen des Unternehmens?

Bild: Rolf Schultes, Drumlin Photos

René Karcher, Geschäftsführer der SecuritySquad GmbH in Frickingen, kennt als ehemaliger Angestellter des Bundesnachrichtendiensts die Gefahren, die im Cyberspace lauern, genau.

IN KÜRZE

Ihre IHK-Ansprechpartner IT-Sicherheit

Bei Fragen rund um IT-Sicherheit, CyberSicherheitsCheck, NIS-2 und verwandte Themen kommen Sie gerne auf uns zu!

- **IHK Bodensee-Oberschwaben,**
  Melanie Riether,
  Tel. 0751 409-299,
  riether@weingarten.ihk.de
- **IHK Ulm,**
  Gernot Schnaubelt,
  Tel. 0731 173-179,
  schnaubelt@weingarten.ihk.de

Leitfaden zur Cyber-Sicherheit im Unternehmen

Wie können sich Unternehmen vor Hacker-Angriffen schützen? Wie können Mitarbeiter für mögliche Gefahren aus dem Netz sensibilisiert werden? Und wohin wendet man sich im Notfall? Ein Leitfaden der IHK Bodensee-Oberschwaben gibt einen Überblick über mögliche Risiken und Handlungsfelder im Bereich IT-Sicherheit.

www.ihk.de/bodensee-oberschwaben, Nr. 1941832

Infos rund ums Thema Informationssicherheit

Auch auf der Website der IHK Ulm gibt es zahlreiche Informationen zu Datensicherheit, Awareness, Passwort-Management und anderen verwandten Themen.

www.ihk.de/ulm, Nr. 6174294

Bild: Gonzalo, stock.adobe.com

Bild: Armin Buhl, Photodesign Armin Buhl

> Es braucht eine effiziente Backup-Strategie mit klar definierten Prozessen – und ein solides Patch-Management.
>
> Philipp König, Geschäftsführer der SSIG-IT GmbH in Blaubeuren

Philipp König ist überzeugt davon, dass IT-Sicherheit nicht als Luxus verstanden werden sollte, sondern als integraler Bestandteil einer verantwortungsbewussten Unternehmensführung.

René Karcher von SecuritySquad beispielsweise setzt dabei auf ein strategisches IT-Sicherheitsmanagement. Ein solches Information Security Management System (ISMS) bilde die Grundlage für eine systematische und langfristige Sicherung der IT-Infrastruktur. Dazu gehören für ihn ein umfassendes Sicherheitskonzept mit alltagstauglichen Richtlinien sowie regelmäßige Audits und die kontinuierliche Anpassung des ISMS an neue Bedrohungen. SITS Deutschland spricht analog von einem 360-Grad-Ansatz und verfolgt eine Sicherheitsstrategie, die sämtliche Geschäftsprozesse integriert, erklärt Angela Lembcke. Dazu zählen beispielsweise eine umfassende Risikobewertung, die Integration von Sicherheitsmaßnahmen in alle Unternehmensbereiche und eine konsequente Überwachung.

Veraltete Systeme: offene Einladung für Angreifer

Konkret geht es um eine ganze Reihe für den Schutz einer IT-Infrastruktur elementarer, vorbeugender Maßnahmen. Ganz wichtig: „Es braucht eine effiziente Backup-Strategie mit klar definierten Prozessen, die vorschreiben, wann Backups erstellt und auch getestet werden müssen“, erklärt König. Wesentlich sei auch ein solides Patch-Management. Heißt: Software und Betriebssysteme müssen regelmäßige aktualisiert werden – die Updates schließen bekannte Sicherheitslücken. Rechner mit veralteter Software, für die es keinen Support und damit auch keine Patches mehr gibt, gehören unbedingt vom Netz, befindet Angela Lembcke: „Veraltete Systeme sind eine offene Einladung für Angreifer.“

Darüber hinaus hält meco-IT-Geschäftsführer Hofmann etwa Netzwerkpläne, Inventarlisten oder Konfigurationsdateien sowie einen Passwort-Manager und gut gepflegte, umfassende IT-Dokumentationen für zwingend notwendig. „Gerade im Notfall, wenn alles schnell gehen muss, braucht es einen guten Überblick über die Infrastruktur“, erklärt er. Daher sollten gut durchdachte Notfallpläne, die genau regeln, was nach einem Angriff zu tun ist, sowie Wiederanlaufpläne dabei helfen, nach Ausfällen schnell und geordnet zu reagieren.

Technische Lösungen bleiben wichtig, und Firewalls, Verschlüsselungen und Multi-Faktor-Authentifizierung sind heute Standard. SecuritySquad hat außerdem automatisierte Tools wie Schwachstellenscanner sowie manuelle Penetrationstests im Portfolio, um regelmäßig Schwachstellen und Sicherheitslücken zu identifizieren. Innovative Werkzeuge wie Threat-Intelligence-Plattformen oder automatisierte Anomalie-Erkennung könnten ebenfalls dabei helfen, potenzielle Gefahren frühzeitig zu erkennen und gezielt abzuwehren, ist Karcher überzeugt.

Technik ist nur Teil der Lösung

„Aber Technik allein reicht nicht aus“, warnt Angela Lembcke von SITS Deutschland, die sogar eine Darknet-Schulung besucht hat, um zu verstehen, wie die Marktplätze im „dunklen“ Teil des Internets funktionieren, und daher einen ganz besonderen Blick auf die Dinge hat. Sie ergänzt: „Die Mitarbeitenden auf allen Unternehmensebenen sollten im Rahmen sogenannter Awareness-Kampagnen regelmäßig geschult werden, um ihre Sinne zu schärfen gegen die Bedrohungen aus dem Netz.“ Um Freund von Feind unterscheiden zu können. „Denn Mitarbeitende“, fügt René Karcher hinzu, „sind oft die erste Verteidigungslinie gegen Angriffe aus dem Netz.“

Solche Kampagnen könnten beispielsweise aus spielerischen Elementen bestehen wie einem internen Phishing-Test und interaktiven Workshops. „Simulierte Phishing-Mails sind dabei besonders effektiv“, weiß SSIG-IT-Chef König. Karcher empfiehlt neben solchen Schulungsmaßnahmen auch die Einführung sogenannter Zero-Trust-Modelle, die davon ausgehen, dass niemandem im Netzwerk vertraut werden kann und daher bei Zugriffen automatisch eine ständige Verifizierung anfordern.

Bei Hackerangriffen ist schnelles Handeln gefragt

Sollte es trotz aller vorbeugenden Maßnahmen doch zu einem Hackerangriff kommen, ist schnelles Handeln gefragt: Krisenteams sollten einen kühlen Kopf bewahren, ihren Notfallplan aktivieren und professio-

nell vorgehen: Um rechtliche Konsequenzen zu vermeiden, muss der Vorfall innerhalb von 72 Stunden an zuständige Stellen gemeldet und Kunden und Geschäftspartner müssen umfassend informiert werden. „Vor allem sollten die betroffenen Systeme sofort vom Netz genommen und isoliert, Daten gesichert und IT-forensische Analysen eingeleitet werden“, betont Security-Experte Karcher. Darüber hinaus liegt die Priorität auf der Wiederherstellung essenzieller Systeme – ein zentraler Schritt, um den Betrieb schnellstmöglich wieder aufzunehmen und den potenziellen finanziellen und Imageschaden einzugrenzen. Und darauf, Vertrauen wieder aufzubauen, das womöglich verloren gegangen ist, weil etwa sensible Unternehmensdaten – Stichwort DSGVO – betroffen sind.

IT-Sicherheit geht alle an

Die EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2), die nun wohl erst im Laufe dieses Frühjahrs in nationales Recht umgesetzt werden wird, schreibt es ohnehin vor: Unternehmen müssen ihre Maßnahmen zum Schutz vor Cyber-Angriffen intensivieren, strengere Sicherheitsstandards etablieren und ihre IT-Systeme stets auf dem neuesten Stand halten und anpassen. Denn die Bedrohungsszenarien entwickeln sich weiter: „Cyber-Angriffe werden zunehmend spezialisierter, und Angreifer setzen verstärkt auf KI-gestützte Werkzeuge“, befürchtet IT-Profi-Hofmann. „Auf diese neuen Bedrohungen müssen sich Unternehmen künftig einstellen.“ Andererseits entwickeln sich spezifische KI-Anwendungen auch zu einer mächtigen Waffe im Kampf gegen die Gefahren aus dem Internet. Schon heute gibt es automatisierte Systeme, die Bedrohungen in Echtzeit erkennen und abwehren. Unternehmen müssen daher auf aktuelle Technologien setzen und zukunftsfähig planen.

Daten und Vertrauen

Alles in allem wird deutlich: „IT-Sicherheit geht uns alle an“, resümiert Norbert Hofmann. Entscheider müssen erkennen, dass es nicht um Panikmache, sondern um Vorsorge geht. Dabei sollte IT-Sicherheit nicht als einmalige Maßnahme betrachtet werden, sondern als ein dynamischer Prozess, der regelmäßig überprüft und optimiert wird. Ein gut geschultes Team, klare Prozesse und der bewusste Umgang mit Technik schaffen die Basis für ein sicheres Arbeiten. Denn am Ende geht es um mehr als um Daten – es geht um Vertrauen.

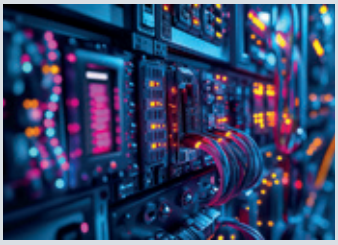
René Kius lebt und arbeitet als freier Journalist in Ravensburg

IN KÜRZE

IT-Security – Wie schütze ich mich vor Hackerangriffen?

Im Rahmen einer kostenfreien Online-Veranstaltung am 18. März von 19 bis 20:15 Uhr informiert Torsten Seeberg von der Zentralen Anlaufstelle Cybercrime (ZAC) des Landeskriminalamts Baden-Württemberg darüber, wie Unternehmen und Gewerbetreibende sich wirksam vor Angriffen aus dem Internet schützen können. Veranstalter ist die Wirtschaftsförderungs- und Standortmarketinggesellschaft Landkreis Sigmaringen (WIS).

Info und Anmeldung:
https://wirtschaftsradar.net/veranstaltungen/it-security-wie-schuetze-ich-mich-vor-hackerangriffen-2



Schutz für Kritische Infrastrukturen

Die KRITIS-Regulierung verpflichtet Betreiber Kritischer Infrastrukturen in Deutschland zu Cybersecurity und Pflichten in KRITIS-Anlagen. Damit soll die Versorgung der deutschen Gesellschaft und Wirtschaft durch kritische Dienstleistungen in KRITIS-Sektoren geschützt werden. Die Regulierung ändert sich ab 2025 in Deutschland und EU-weit deutlich. Ob Ihr Unternehmen davon betroffen ist und wie Sie sich auf die Regulierung vorbereiten können, lesen Sie hier:

https://www.openkritis.de/it-sicherheitsgesetz/index.html

NIS-2: Was tun?

Das Gesetz hat am 24. Juli 2024 das Kabinett passiert. Ein Beschluss des Deutschen Bundestags steht noch aus, ein Inkrafttreten des Gesetzes steht daher erst noch bevor.
So können sich Unternehmen darauf vorbereiten:

https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-was-tun/NIS-2-was-tun_node.html

Cybersicherheitsagentur Baden-Württemberg

Auf der Website der Cybersicherheitsagentur Baden-Württemberg gibt es aktuelle Sicherheitshinweise, Empfehlungen, Angebote und Anlaufstellen für Fragen rund um die IT-Sicherheit.

www.cybersicherheit-bw.de

Notfallnummer für den Ernstfall

Bei einem Hackerangriff können sich Unternehmen, staatliche Stellen und Kommunen rund um die Uhr an die von der Cybersicherheitsagentur betriebene Hotline Cyber-Ersthilfe BW wenden. Dort erhalten Betroffene Unterstützung bei der Einordnung des Vorfalls, eine erste Hilfestellung sowie Hinweise zu Anlaufstellen, an die man sich wenden kann.

Tel. 0711 137-99999

Landeskriminalamt und Polizei

Opfer eines Cyberangriffs sollten schnellstmöglich Anzeige bei der Polizei erstatten. Ansprechpartner für Unternehmen ist die Zentrale Ansprechstelle Cybercrime (ZAC) des Landeskriminalamts Baden-Württemberg. Dort erhalten Betroffene wichtige Hinweise, um den Angriff bestmöglich einzugrenzen und zu bewältigen. Darüber hinaus verfügen Landeskriminalamt und Polizei über exklusive rechtliche Befugnisse, um beispielsweise ausgespähte Daten oder erlangte Vermögenswerte sicherzustellen und einen weiteren Schaden zu verhindern.

Zentrale Ansprechstelle Cybercrime (ZAC),
Tel. 0711 54012444 (rund um die Uhr),
cybercrime@polizei.bwl.de,
https://lka.polizei-bw.de/zac