WIRTSCHAFT

ZWISCHEN NORD- UND OSTSEE

IHK Schleswig-Holstein
Flensburg·Kiel·Lübeck

AUSGABE FLENSBURG
11/2022 · NOVEMBER

Titelthema:

Wirtschaftsfaktor Häfen

Digital in die Vorreiterrolle

Wirtschaft im Gespräch:
Markus Mettler

Schwerpunkt aktuell:
Cyberangriffe auf Unternehmen

Schwerpunkt aktuell

Gefahren abwehren

Trotz Spamfiltern oder Firewalls verüben Hacker jeden Tag gezielte **CYBERANGRIFFE AUF UNTERNEHMEN**, greifen sensible Daten ab oder blockieren ganze Produktionsabläufe durch digitale Sabotage. Drei Experten geben Ratschläge, wie sich Betriebe schützen können.

VON MAJKA GERKE

Die Auswirkungen einer Cyberattacke können massiv sein. Die IHKs in Deutschland sind im Sommer selbst Ziel eines gezielten Angriffs geworden – einige Onlineservices der Kammern sind auch heute noch lediglich eingeschränkt nutzbar. Nach Erkenntnissen von IT-Forensikern und des Bundesamts für Sicherheit in der Informationstechnik wurde der Angriff auf die IHK-Organisation von extrem professionellen Hackern ausgeführt. Durch die Abschaltung des Internetzugangs konnte eine Ausbreitung des Angriffs sowie ein Datenabfluss verhindert werden. Deshalb möchte die IHK Unternehmen dabei unterstützen, sich vor Cyberattacken zu schützen. Angriffe werden häufig mit einfachen Mitteln ausgeführt.

Was ein falscher Klick alles anrichten kann, weiß Frank Barthel genau. Der Fachmann und seine Mitarbeiter der FB datentechnik GmbH in Travemünde betreuen hauptsächlich kleinere Betriebe. Darunter sind nicht nur Unternehmen, die er vorsorglich in Sachen

FOTO: STOCK.ADOBE.COM/ARTEMISDIANA

IT-Sicherheit betreut, sondern auch solche, bei denen der Ernstfall schon eingetreten ist. „Das geht meist blitzschnell. Man liest gestresst eine Mail, klickt, ohne nachzudenken, auf einen mitgeschickten Anhang und schon ist es passiert“, sagt Barthel. Wenn dann durch Ransomware, also Schadprogramme, die die Systeme verschlüsseln, der ganze Betrieb lahmgelegt wird und die Erpresser drohen, erst gegen Zahlung eines Lösegelds alles wieder freizuschalten, kann der Schaden für das Unternehmen hoch werden.

Gut, wenn man seine Daten extern gesichert hat, das System auf den Stand vor dem Angriff bringen kann und damit die Schadsoftware aushebelt. „Die stärkste Waffe ist eine funktionierende Datensicherung“, sagt Barthel. Er rät seinen Kunden generell zu mehr Schutzmechanismen wie der Installation von Firewalls, Spamfiltern und Endpointschutz, zu regelmäßigen Softwareupdates sowie zu passenden Authentifizierungsmöglichkeiten und starken Passwörtern. Diese Sicherheitsanforderungen sind auch Teil von Richtlinien wie der VdS 10005, die Cyberversicherungen als Grundlage für ihre Versicherungsbedingungen dienen. „Viele KMU erkennen oft nicht, dass IT kein Unterstützungsprozess ist, sondern zu den Kernprozessen zählt und damit der zentrale Dreh- und Angelpunkt eines Unternehmens ist“, sagt Barthel.

Schadsoftware wird immer intelligenter, die Gefahren aus dem Internet größer. Auch Unternehmen im Norden müssen sich verstärkt gegen Cyberangriffe wehren. 153 Millionen neue Schadcodes seien in den vergangenen zwölf Monaten festgestellt worden, sagt Janek Maiwald, technischer Vorstand der Deutschen Gesellschaft für Cybersicherheit (DGC) mit Hauptsitz in Flensburg. „Aktuell sehen wir eine ansteigende Tendenz von Angriffen“, erklärt er.

75 Prozent der Malware werden per Spam und Phishingkampagnen versendet und unwissentlich vom Empfänger aktiviert. Der Großteil der betroffenen Unternehmen erkenne nicht, was alles ankomme, weil die Menge rasant zunehme, sagt Maiwald. Meist dauert es bis zu sieben Monate, bis der Angriff auf die Systeme überhaupt auffällt. Oft ist es dann schon zu spät, den Schaden abzuwenden. Die Größe der Betriebe ist für die Cyberkriminellen dabei unerheblich, allerdings gibt es Branchen, die gefährdeter sind und permanent angegriffen werden. Dazu gehören unter anderem DAX-Unternehmen, aber auch Behörden oder für die Gesellschaft elementare Bereiche wie Krankenhäuser oder Energieversorger. Gezielt werden Infrastrukturen und Applikationen der Betriebe ausspioniert, um Hintertüren in die Systeme zu finden und Daten abzugreifen oder Viren einzuschleusen. Der Einsatz von automatisierten Securitylösungen hilft da sehr. „Das funktioniert in Deutschland besser als in anderen Ländern“, meint Maiwald. Die DGC hilft ihren Kunden, Sicherheitslücken aufzudecken und den Schutz der Infrastrukturen sicherzustellen. Ihre Mitarbeiter scannen Systeme und Netzwerke, zeigen, wo Schlupflöcher auftreten, und überwachen die IT-Sicherheit ihrer Kunden.

Das schwächste Glied in der Kette der Cybersicherheit ist für Thomas Holst der Mensch. Der Geschäftsführer der BT Nord Systemhaus GmbH in Husum betreut KMU in technischen und organisatorischen Maßnahmen der Cybersicherheit. Einer der Schwerpunkte des Unternehmens ist das Thema Sensibilisierung der Mitarbeiter. „Wir klären auf, welche Gefahren es gibt, wie man sich schützt und an wen man sich wenden kann, wenn doch was passiert ist“, sagt er. Das Problem ist real, immerhin zehn bis 25 Prozent aller Phishingmails kommen beim Empfänger an, auch durch gut gesicherte Systeme.

„Man sollte jede E-Mail doppelt und dreifach prüfen, bevor man auf einen mitgeschickten Link klickt“, sagt er. Neben dem Erhalt von Ransomware lauern aber noch mehr Gefahren. Eine davon ist Social Engineering. Dabei wird versucht, das Vertrauen von Personen zu erschleichen, damit diese Daten oder Passwörter verraten. Eine weitere Betrugsmasche ist der CEO-Fraud. So nennt man es, wenn Mitarbeiter unter Verwendung von falschen Identitäten dazu gebracht werden, Geld zu überweisen. „Sind die Mitarbeiter aufgeklärt, wie die Gefahren gelagert sind, sind sie viel aufmerksamer in Bezug auf das, was sie preisgeben. Human Firewall nennt man das“, sagt Holst. ■

HILFE FÜR UNTERNEHMEN

Hilfestellung gibt auch die Transferstelle für IT-Sicherheit im Mittelstand (TISiM). Hier bekommen KMU, Freiberufler und Selbstständige Angebote zur IT-Sicherheit und Hilfe bei der Umsetzung. Mit einer eigenen Anwendung, dem Sec-O-Mat, bekommen Unternehmen passgenaue Umsetzungsvorschläge für ihre IT-Sicherheit.

Mehr unter: www.tisim.de

Autorin: Majka Gerke, freie Journalistin, redaktion@ihk-sh.de
Mehr unter: www.fb-it.de, www.dgc.org, www.btnord.de