newsletter

Wirtschaftsförderung Kanton Schaffhausen

cyber security

sh.ch

«Ein Hackerangriff kann für ein KMU von existenzieller Bedrohung sein»

KMU geraten zunehmend in den Fokus von Cyber-Kriminellen. Im Interview spricht Candid Wüest, Leiter des neuen Cyber Protection Operation Centers von Acronis in Schaffhausen, über mangelndes Gefahrenbewusstsein bei KMU, Phishing-Attacken während der Corona-Pandemie und wie sich Unternehmen besser schützen können.

VON PASCAL SCHMIDLIN | LAYOUT BBF | FOTOS 4KP

Herr Wüest, die Digitalisierung bringt Herausforderungen im Sicherheitsbereich für Unternehmen mit sich. Erst kürzlich wurden die Server des Fitnesstracker- und GPS-Spezialisten Garmin erfolgreich angegriffen. Sind das Einzelfälle oder sind Hacker oft erfolgreich?

Candid Wüest: Sie sind leider definitiv erfolgreich. Und Cyberangriffe sind deshalb ein lukratives Geschäft geworden, das immer stärker wächst, da das Geld lockt.

Computerschädlinge und Cyberangriffe sind kein neues Phänomen und gibt es bereits seit den Anfängen des Internets. Warum sind Cyberkriminelle trotzdem erfolgreich?

Das hat verschiedene Gründe. Die Komplexität der Systeme hat in den vergangenen Jahren stark zugenommen mit global verstreuten Servern, Clouddiensten und so weiter. Das macht die korrekte Konfiguration für Unternehmen herausfordernd und führt dazu, dass sich Fehler einschleichen, die erfolgreiche Angriffe ermöglichen. Man kann aber die Systeme heute sehr sicher machen, das zeigt sich etwa bei Banken.

ÜBER CANDID WÜEST

Candid Wüest, (*1977), ist in Uhwiesen aufgewachsen und hat an der ETH Zürich Informatik studiert. Von 2003 bis 2020 war er beim Security-Spezialisten Symantec tätig und hat dabei unter anderem dessen Security Team in Dublin aufgebaut und geleitet.

Seit März dieses Jahres ist er beim Cyber-Protection-Unternehmen Acronis in Schaffhausen Leiter des EMEA Cyber Protection Operation Centers. Gemeinsam mit seinem Team analysiert er die aktuellen Gefahren im Netz und verbessert laufend die Sicherheitsprodukte von Acronis. Acronis setzt mit seinen innovativen Lösungen für Backup, Ransomware-Abwehr, Disaster Recovery, Storage und EFSS (Enterprise File Sync & Share) den Standard für Cyber Protection für Privatanwender sowie KMU und Grossunternehmen.

Inwiefern?
Banken werden kaum je erfolgreich angegriffen, obwohl sie ein scheinbar lukratives Ziel wären. Doch sie investieren stark in ihre Sicherheit, auch im Cyberbereich. Die Kehrseite ist jedoch, dass die Benutzerfreundlichkeit leidet. Um sich an der Arbeitsstation anzumelden, etwa mit dem eigenen Laptop, braucht es neben einem komplexen Passwort eine Smart-Card, die man ins Gerät steckt oder Fingerabdruck-Leser. Der 0815-Benutzer möchte das aber nicht, da er es bequem mag.

Welchen Gefahren sind Unternehmen heute besonders ausgesetzt?
Das sind zum einen die sogenannten Distributed-Denial-of-Service-Attacken (DDoS), bei denen die Server überlastet werden und schliesslich ausfallen. Dann Phishing-Mails, bei denen versucht wird, über gute Stories oder gefälschte Webseiten an Geld oder Passwörter zu kommen und zuletzt Ransomware, sogenannte Verschlüsselungstrojaner, die derzeit eine der grössten Gefahren darstellen. Dabei dringen Angreifer in das System ein, stehlen und verschlüsseln die kompletten Daten und erpressen die Unternehmen. Fast jeder dritte Cyberangriff in der Schweiz ist heute ein Ransomware-Vorfall. Damit sind wir weit über dem globalen Durchschnitt, was auf die finanzielle Lukrativität der Schweiz zurückzuführen ist. Kürzlich gab etwa Stadler Rail bekannt, Opfer einer solchen Attacke geworden zu sein.

Stadler Rail hat jedoch gesagt, man werde nicht bezahlen und könne die gestohlenen Daten dank eines Backups retten.
Das ist korrekt, aber auch das hat Zeit und somit Geld gekostet. Zudem darf der Image-Schaden nicht ausser Acht gelassen werden, etwa wenn die Hacker als Konsequenz des Nichtbezahlens die gestohlenen Daten im Web veröffentlichen. Sind da Kundendaten, wie Kreditkarteninformationen oder Passwörter dabei, kann auch schnell bei Dritten Schaden entstehen. Zudem haben wir festgestellt, dass in drei von zehn Fällen das Backup nicht funktioniert, da es nie getestet worden ist, gerade bei KMU. Die merken dann erst wenn es zu spät ist, dass es nicht funktioniert.

Von aussen scheint es lukrativ, dass sich Cyberangreifer auf grosse Unternehmen konzentrieren, da es dort mehr zu holen gibt. Laut einer Studie von Cisco sind aber 43% aller Cyberangriffe gegen KMU gerichtet. Weshalb?
Die Systeme von Grossunternehmen sind in der Regel besser gesichert, als diejenigen von KMU. Letztere verfügen oft nicht über eine eigene IT und setzen wenig Ressourcen für Cyber-Sicherheit ein. Hinzu kommt der Irrglaube, dass sie nicht Ziel von Cyberkriminellen werden, da sie ja unbekannt und somit nicht attraktiv für Hacker sind. Das ist jedoch ein Irrglaube. Hacker greifen KMU nicht bewusst an, sondern durchsuchen exponierte Systeme wie Webserver nach Schwachstellen. Dabei ist ihnen egal, wem dieser gehört. Diesem Umstand sind sich viel zu wenige KMU bewusst.

«DER MENSCH IST OFT DAS SCHWÄCHSTE GLIED. REGELMÄSSIGE INTERNE SCHULUNGEN SIND WICHTIG, UM SO DAS BEWUSSTSEIN FÜR DIE GEFAHREN IM NETZ ZU SCHÄRFEN UND DIE METHODEN DER BETRÜGER AUFZUZEIGEN.»

Fehlt also ein generelles Bewusstsein für die Gefahren von Cyberangriffen?
Bei grossen Unternehmen nicht, aber bei kleineren Unternehmen schon. Ein Hackerangriff kann für ein KMU von existenzieller Bedrohung sein. Da werden schnell einige Zehntausend oder gar Hunderttausend Franken gefordert, um die Daten wieder freizugeben. Hinzu kommt, dass der Betrieb lahmgelegt ist, solange die Systeme gesperrt sind. Ausserdem besteht keine Garantie, dass nach dem Bezahlen des Lösegeldes wirklich alle Daten freigegeben werden.
Mit dem Schaffhausen Institute of Technology entwickeln wir deshalb derzeit Online-Kurse, um Unternehmen aber gerade auch regionale KMU in diesem Bereich zu schulen und auf die Gefahren aufmerksam zu machen. So soll die Chefebene mehr mit dem Thema in Berührung kommen, um gute Risikoabwägungen zu machen und korrekte Entscheide fällen zu können.

Aber braucht es nicht auch Schulungen von Mitarbeitenden?
Das ist natürlich zentral. Der Mensch ist oft das schwächste Glied, was sich etwa bei Phishing-Mails zeigt. Man kennt ja die Betrugsversuche mit angeblichen Lottogewinnen oder Erbschaften, bei denen eine Vorauszahlung verlangt wird. Regelmässige interne Schulungen sind wichtig, um so das Bewusstsein für die Gefahren im Netz zu schärfen und die Methoden der Betrüger aufzuzeigen. Aber man muss sich als Unternehmen bewusst sein, absolute Sicherheit gibt es nicht und es wird immer jemanden geben, der eine solche Mail trotz aller Warnsignale öffnet und den Link anklickt.

Die Corona-Pandemie hat auf einen Schlag Millionen von Menschen weltweit ins Homeoffice versetzt. Hatte das auch einen Einfluss auf das Verhalten von Kriminellen im Internet?
Ja, das hatte es. Viele Angestellte kamen im Homeoffice mit neuen Produkten wie Zoom oder Microsoft Teams für Videokonferenzen in Kontakt. Plötzlich tauchten Phishing-Mails mit angeblichen Links zu Videokonferenzen auf. Das Homeoffice hat aber auch noch andere Gefahren offengelegt.

JEDEN TAG

300'000

NEUE SCHAD-PROGRAMME IM NETZ.

Cand[illegible]est, Leiter des EMEA Cyber Protection Operation Centers beim Cyber-Protection-Unternehmen Acronis in Schaffhausen.

Welche denn?

Viele Firmen haben keine Notebooks für ihre Mitarbeitenden. Die haben sich dann von zu Hause aus mit ihren Privatgeräten eingeloggt. Das stellt ein erhebliches Sicherheitsrisiko dar, da zum einen vertrauliche Daten plötzlich auf diesen Geräten landen und zum anderen mit diesen Geräten auch unsichere Seiten angesurft werden, etwa durch andere Familienmitglieder, was das Infektionsrisiko steigert. Hier braucht es bessere Vorgaben der Unternehmen und sichere Verbindungen, etwa über VPN und wenn möglich mit einer Zwei-Faktor-Authentifizierung für sensible Dienste, etwa über einen SMS-Code neben dem eigenen Passwort.

Viele KMU verfügen nicht über eigene IT-Abteilungen. Was empfehlen Sie diesen?

Diese Expertise kann heute relativ günstig bei IT-Dienstleistern hinzugekauft werden. So können die Systeme aktuell gehalten und Sicherheitsrisiken minimiert werden. Denn die Frage ist nicht ob, sondern wann ein System angegriffen wird. Jeden Tag gibt es 300 000 neue Schadprogramme im Netz, da ist es nur eine Frage der Zeit.

Was sind die wichtigsten Regeln für KMU, um sich gegen Angriffe im Netz zu schützen?

1. Immer das System aktuell halten, um Lücken zu schliessen. 2017 legte der Virus Wannacry fast eine Million Server lahm. Dabei nutzte er eine Schwachstelle, die nicht nur längst bekannt war, sondern für die bereits seit zwei Monaten ein Patch verfügbar war.
2. Eine starke Authentifizierung durch starke Passwörter, unterschiedliche Passwörter und wenn möglich eine Zwei-Faktor-Authentifizierung für kritische Services, wie etwa E-Mails.
3. Die Konfiguration von Diensten – etwa bei Cloud-Services wie Dropbox – regelmässig auf deren Sicherheit überprüfen. Wenn hier die Expertise fehlt, diese unbedingt extern einkaufen.
4. Regelmässige Backups der Daten machen und prüfen, ob diese auch funktionieren.
5. Security-Software wie Anti-Viren-Lösung auf allen Geräten installieren und stets aktuell halten. Damit können erfolgreiche Angriffe minimiert werden, denn Schadsoftware ist meist darauf ausgelegt, möglichst schnell in ein System einzudringen. Ist es besser geschützt als die andern, wird auf das nächste Ziel übergegangen.

«HACKER GREIFEN KMU NICHT BEWUSST AN, SONDERN DURCHSUCHEN EXPONIERTE SYSTEME WIE WEBSERVER NACH SCHWACHSTELLEN.»