IT- & DATENSICHERHEIT

Die Mitarbeiter für Cybercrime sensibilisieren

Der Regensburger Cybersecurity-Kongress soll künftig zu einer festen Einrichtung werden.

Von Gerd Otto

Worst Case: Wenn Sicherheitslücken den Angreifern im Netz Tür und Tor öffnen. Foto: NicoElNino-stock.adobe.com

REGENSBURG. Der 1. Regensburger Cybersecurity-Kongress ist – darin waren sich alle Experten einig – angesichts der Brisanz des Themas keineswegs zu früh gekommen. Vielmehr waren die Veranstalter rund um den IT-Sicherheitscluster e. V., die Digitale Gründerinitiative Oberpfalz (DGO), die OTH Regensburg, das Polizeipräsidium Oberpfalz sowie die Handwerkskammer Niederbayern-Oberpfalz und die IHK Regensburg für Oberpfalz/Kelheim, überzeugt, dass Cybercrime künftig einen enorm hohen Stellenwert für Wirtschaft und Gesellschaft bekommen werde.

Impuls für Technologiestandort

Aus dem Blickwinkel Regensburgs und der gesamten Region Ostbayern verknüpfte der Referent für Wirtschaft, Wissenschaft und Finanzen, Prof. Dr. Georg Stephan Barfuß, angesichts dieser Herausforderung mindestens zwei Aspekte, die ihm als besonders zukunftsträchtig erschienen. Angesichts der zunehmenden Gefahren kommt es ihm vor allem darauf an, bei den Bürgern und den Unternehmen für eine höhere Sensibilisierung zu sorgen und konkrete Gegenmaßnahmen anzustoßen.

Gleichzeitig aber plädiert Barfuß in seiner Eigenschaft als Wirtschaftsreferent der Stadt auch dafür, am Standort Regensburg und in der Region Firmen zu fördern, die einen technologischen Beitrag gegen die Cyberkriminalität leisten können. Hier gehe es in hohem Maße um Innovationsfähigkeit. Ihm sei es nach eigenen Angaben besonders wichtig, die Ideengeber zusammenzuführen, die Kräfte zu bündeln – und den Regensburger Cybersecurity-Kongress zu einer festen Einrichtung werden zu lassen. Ein intensiver Erfahrungsaustausch und eine permanente technologische wie auch gesellschaftspolitische Auseinandersetzung seien die Basis dafür, Antworten auf die enormen Herausforderungen zu finden.

Die Lage der IT-Sicherheit in Deutschland erläuterte Prof. Dr. Jürgen Mottok von der Fakultät Elektro- und Informationstechnik der OTH Regensburg. Sein Appell an die Unternehmen lautete, die Kosten für IT-Sicherheit in der Kalkulation nicht zu vernachlässigen. Nicht von ungefähr habe das Allianz-Risk-Barometer bei einer Umfrage unter Risikomanagementexperten Cybervorfälle bereits weltweit noch vor Betriebsunterbrechung, Naturkatastrophen oder Feuer und Explosion als besonders hohe Geschäftsrisiken eingestuft. Vor diesem Hintergrund und der Tatsache, dass der Mensch sich tatsächlich als die größte Schwachstelle erweist, appelliert Mottok an ein ausgeprägtes Sicherheitsbewusstsein.

Fragenkatalog abarbeiten

Nur, wenn alle Mitarbeiter erkennen und akzeptieren, dass die Informationssicherheit ein bedeutender Faktor für den Erfolg eines Unternehmens oder einer Institution ist, könne ein solches Risiko erfolgversprechend bekämpft werden: „Die Belegschaft muss jedenfalls für relevante Gefährdungen sensibilisiert werden." Deshalb sollten sich die Unternehmen eine Checkliste erarbeiten, um anhand eines solchen Fragenkatalogs eine Kultur des Sicherheitsbewusstseins zu entwickeln. Neben der Selbsteinschätzung der Mitarbeiter in puncto Security gehe es nicht zuletzt um eine regelmäßige Schulung zu sicherheitsrelevanten Themen und die Frage, in welchem Maße die Mitarbeiter eigenverantwortlich an Themen der IT-Sicherheit beteiligt werden. Konkret spricht sich Jürgen Mottok auch für eine sorgfältige Aufbewahrung und den zusätzlichen Schutz vertraulicher Informationen und Datenträger aus.

Wichtig sei auch ein Verhaltenskodex rund um sicherheitsrelevante Fragen. Vor Wartungs- und Reparaturarbeiten durch Mitarbeiter von Fremdfirmen sollten vertrauliche Informationen sorgfältig behandelt und verwahrt werden. Außerdem müsse der Kenntnisstand der eigenen Mitarbeiter in Sachen IT-Sicherheit regelmäßig überprüft werden. Neben der Überlegung, wie Sicherheitsvorgaben kontrolliert und Verstöße dagegen „geahndet" würden, komme es ganz grundsätzlich darauf an, den Mitarbeitern klare Verhaltensregeln zu vermitteln.

Vorsorge kein Kostentreiber

Am Beispiel eines Angriffs auf die Ransomware der Pöllath GmbH in Erbendorf wurde im Rahmen einer Podiumsdiskussion der Ablauf einer solchen Attacke auf ein Unternehmen besprochen. Wie Thomas Moosmüller, Geschäftsführer der Breakin Labs GmbH, erläuterte, werden vor allem kleine und mittlere Unternehmen sowie Start-ups immer häufiger als Ziel von Cyberangriffen ausgewählt.

In diesem Zusammenhang bedauerte es Moosmüller, dass die IT-Sicherheit als Kostentreiber betrachtet und deshalb vernachlässigt werde. „IT-Sicherheit bringt keinen operativen Erfolg und kostet nur Geld", sei dabei eine häufige Aussage mittelständischer Unternehmen.

Viele Geschäftsführer wähnen sich jedoch in falscher Sicherheit. Mossmüller, dessen Unternehmen erst kürzlich zum Partner des BSI-Projekts „Allianz für Cyber-Sicherheit" ernannt worden war, empfiehlt regelmäßige, quartalsweise oder jährliche Penetrationstests, damit der Stand der aktuellen IT-Sicherheit verbessert werden kann.

Kriminalhauptkommissar Daniel Dünzinger von der Kriminalpolizei Oberpfalz verwies auf die hohe Dunkelziffer bei Cybercrime und appellierte an die Adresse der Unternehmen, zum einen die Schulung der Mitarbeiter zu intensivieren und andererseits zeitnah den Kontakt mit der Kriminalpolizei zu suchen.

Cyberkriminalität im engeren Sinne wird von der Polizei als hochtechnische Straftat eingestuft, die deshalb auch hochtechnische Ermittlungsarbeit aufseiten der Polizei erfordert. Insgesamt gehe es hier um einen hochkomplexen, kriminellen Wirtschaftszweig mit eigenen Wertschöpfungsketten.

Wissen wandert in falsche Hände

Erpresser können allzu leicht ihrem einträglichen Geschäftsmodell nachgehen.

Gastbeitrag von
Dr. Matthias Kampmann, Leiter F&E
beim IT-Sicherheitscluster

Dr. Matthias Kampmann
Foto: Sophia Wiesbeck

Der Klick, der alle Steine ins Rollen bringt, geht schnell: Man erhält eine E-Mail, die täuschend echt wie die eines Geschäftspartners aussieht. Ein Link darin führt auf Server von Cyberkriminellen. Es geht weiter im Büroalltag vor dem Bildschirm und am Telefon. Es kommt ein Anruf, der nächste und übernächste. Das Mikromanagement gerät aus den Fugen, die E-Mail aus dem Blick. Ein halbes Jahr später sind plötzlich alle Festplatten in der Organisation verschlüsselt. Die Lösegeldforderung steht an.

Dies ist keine Fiktion. Das Beispiel erzählt die Geschichte eines mutigen Unternehmers: Josef Pöllath leitet einen Betrieb für Tore, Türen und deren Antriebe in Erbendorf nahe Weiden. Sein Unternehmen mit gut 60 Mitarbeitern ist digitalisiert. Es ist vorbildlich aufgestellt. Seine Server betreut Josef Pöllath selbst. Aber ganz gleich, auf welchem Wege die erpresserische E-Mail in sein Netz gekommen ist: Plötzlich war sie da. Geschichten wie die von Josef Pöllath gehören in deutschen Unternehmen zum Alltag. Es wird jedoch viel zu häufig darüber geschwiegen, die Erpresser agieren nach einem einträglichen Geschäftsmodell. Denn wenn man das Lösegeld verweigert und lediglich das Back-up einspielt, kann es sein, dass die Ganoven damit drohen, die Daten, die abgeflossen sind, öffentlich zu machen. Rufschädigung ist vorprogrammiert, Wissen wandert in falsche Hände, und mögliche Klagen ziehen schwerwiegende Folgen nach sich. Was schafft Abhilfe? Das IT-Sicherheitscluster empfiehlt erst einmal eine Aktion zur Bildung von Aufmerksamkeit und zur Erfassung der Istlage, etwa mit der ISA+ Informations-Sicherheits-Analyse, die kostenlos über die Homepage des Clusters erhältlich ist. Es gibt eine Reihe von Werkzeugen, mit denen man seine Wahrnehmung für gefährliche E-Mails trainiert.

Doch dabei kann man nicht stehen bleiben. Genauso wenig reicht es, einfach neue Geräte, etwa eine Firewall zu kaufen. Informationssicherheit adressiert erst einmal den Menschen: Was mache ich mit dem USB-Stick, den ich auf dem Parkplatz vor dem Unternehmen gefunden habe? Wohin gehört mein Firmenlaptop nach Feierabend? Was muss ich tun, wenn wirklich Daten abgeflossen sind? All diese Fragen beantworten Regelwerke, die man als Informationssicherheitsmanagementsystem (ISMS) definiert.

Informationssicherheit kostet Zeit und Ressourcen. Wenn sie gelebt wird, haben Erpresser weniger Chancen und vor Gericht kehrt sich beispielsweise die Beweislast um. Selbst wenn man niemals zu 100 Prozent vor Cyberattacken oder Angriffen auf die Schutzziele des Unternehmens gefeit sein wird: Gut aufgestellt zu sein, sichert Kapital, Wertschöpfungsketten und natürlich auch Arbeitsplätze.