CYBER-SICHERHEIT: EIN FALL NICHT NUR FÜR INFORMATIKER

Bei Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen können Störungen oder Ausfälle erhebliche Folgen für die Sicherheit der Gesellschaft haben. Cyber-Experten beim Bundesamt für Sicherheit in der Informationstechnik schützen diese so genannten kritischen Infrastrukturen.

VON ELENA WEBER

ISABEL MÜNCH

Frau Münch, Sie sind Fachbereichsleiterin Präventive Cyber-Sicherheit und Kritische Infrastrukturen beim Bundesamt für Sicherheit in der Informationstechnik (BSI). Was genau sind denn „Kritische Infrastrukturen"?

Grob gesagt sind kritische Infrastrukturen all das, was für unsere Gesellschaft wichtig ist, um das normale Zusammenleben zu gewährleisten. Wir unterteilen die Bereiche der kritischen Infrastrukturen in neun Sektoren: Staat und Verwaltung, Finanz- und Versicherungswesen, IT und TK, Gesundheit, Ernährung, Transport und Verkehr, Medien und Kultur, Energie und den Sektor Wasser. Wir haben in Deutschland viele Institutionen typischerweise kleinteilig aufgebaut, sodass wir denken, der Ausfall einer einzelnen Einrichtung ist gar nicht so schlimm. Bis wir dann feststellen, wie vernetzt inzwischen alles ist. Wenn zum Beispiel die IT in einem Krankenhaus ausfällt, lässt sich das meistens überbrücken, aber gerade durch die zunehmende Vernetzung – Krankenhäuser sind ja bis in den OP hinein mit IT ausgestattet – können schnell auch umliegende Krankenhäuser betroffen sein. Das ist das, was wir unter kritisch fassen: Bereiche, bei denen Unregelmäßigkeiten die Versorgung oder Sicherheit der Bevölkerung gefährden.

Inwieweit nimmt die Bedrohung dieser Infrastrukturen durch die zunehmende Vernetzung und Digitalisierung denn zu?

Unsere IT-Abhängigkeit nimmt zu und damit auch die Wahrscheinlichkeit, dass irgendetwas mit der IT schiefgeht, sei es durch Hacker – professionelle wie Hobby-Hacker –, sei es durch unaufmerksame Mitarbeiter oder höhere Gewalt. Die Ursache ist erstmal egal. Wenn es zu Ausfällen kommt, müssen die Bereiche der kritischen Infrastrukturen so aufgestellt sein, dass die Auswirkungen dieser Ausfälle keine schwerwiegenden Folgen nach sich ziehen.

Wie sieht die Präventionsarbeit aus?

Zunächst machen wir uns Gedanken darüber, zu welchen Bedrohungen es überhaupt kommen könnte. Diese können im Bereich der Cyber-Sicherheit sehr unterschiedlich sein und entsprechend sind auch die erforderlichen Gegenmaßnahmen sehr unterschiedlich. Im Endeffekt müssen wir uns fragen: Was sind die kritischen Anlagen? Was sind die wesentlichen Bereiche, die geschützt werden müssen? Im nächsten Schritt schauen wir uns an, wovon diese Bereiche abhängen und auf welchen Systemen sie laufen. In der so genannten Gefährdungsanalyse tragen wir dann zusammen, was alles schiefgehen könnte und welche Maßnahmen ergriffen werden können, um Beeinträchtigungen oder Ausfälle zu verhindern. Außerdem muss entschieden werden, welche Maßnahmen angemessen sind, denn grundsätzlich kann man Sicherheit natürlich beliebig weit nach oben treiben. Das ist dann aber auch beliebig teuer.

Welchen Bedrohungen sind kritische Infrastrukturen denn ausgesetzt?

Ein Hacker könnte beispielsweise versuchen, einen so genannten Denial-of-Service-Angriff gegen eine kritische Anlage zu fahren, indem er IT-Systeme so überlastet, dass sie nicht mehr arbeiten können. Das ist ein sehr beliebter Angriff. Der Klassiker sind natürlich Computerviren. Diese gelten eher als ungezielte Angriffe, das heißt, ein Hacker streut den Virus in die Breite und zufällig erwischt es dich. Inzwischen haben wir aber immer mehr gezielte

FOTOS // PRIVAT, GETTY IMAGES/SOLARSEVEN

Angriffe, die mit ähnlichen Mechanismen arbeiten wie die Computerviren, das heißt, es werden Schwachstellen auf den Rechnern ausgelotet, indem Mails verschickt werden, mit denen der Empfänger dazu gebracht werden soll, auf die Anhänge oder einen Link zu klicken, damit er die entsprechende Schadsoftware herunterlädt und aktiviert, ohne es zu merken. Angreifer versuchen also gezielt anzugreifen und dabei unentdeckt zu bleiben. Für uns bedeutet das: Wir müssen auf Massenangriffe ebenso vorbereitet sein wie auf diese gezielten Angriffe. Aber wir müssen uns beispielsweise auch Gedanken machen, ob hier bei uns in Bonn bei Hochwasser die Rechenzentren hoch genug liegen und geschützt sind.

Wie sehen in diesem Bereich die Berufschancen für Absolventen aus?

Alle, die sich gerade mit dem Cyber-Raum beschäftigen, sind momentan gesucht wie warme Semmeln. Unternehmen und Behörden haben inzwischen verstanden, wie wichtig IT-Sicherheit heutzutage ist, und entsprechend werden viele IT-Sicherheitsfachleute eingestellt. Die Bundeswehr hat beispielsweise die neue Waffengattung „Cyber“ eingeführt. Und so geht das überall. Egal, wo wir hinschauen: Es ist verstanden worden, wie wichtig das Thema Cyber-Sicherheit ist. Jeder Mittelständler sucht inzwischen nach einem Mitarbeiter, der für die IT-Sicherheit zuständig ist. Daraus ergibt sich das Phänomen, das spezialisierte Studiengänge wie IT-Sicherheit regelrecht ausverkauft sind, und es gibt Studiengänge, bei denen wir versuchen, das Interesse für dieses Thema zu wecken. Beispielsweise in der Psychologie oder Politologie. Denn wir brauchen auch Leute, die sich in die Verhaltensmuster der Angreifer hineindenken können. Wir beschäftigen aber auch Betriebswirtschaftler. Beim BSI sind zahlreiche neue Stellen entstanden, auch, weil sich immer etwas ändert. An das, was wir heute untersuchen, haben wir vor fünf Jahren noch gar nicht gedacht. Und so wird es weitergehen. Wir werden auch in fünf Jahren Herausforderungen haben, die wir uns jetzt noch gar nicht vorstellen können.

Welche Beschäftigungsmöglichkeiten bietet der Fachbereich Präventive Cyber-Sicherheit und Kritische Infrastrukturen Absolventen?

Gerade im Bereich IT-Sicherheit denken viele zuerst an Informatiker. Tatsächlich haben wir hier aber eine riesige Bandbreite an Beschäftigungsmöglichkeiten. Klischeehaft gesagt: Wir brauchen den Nerd, der im dunklen Kämmerlein sitzen will und am liebsten nachts vor sich hinarbeitet, genauso wie Menschen, die gerne mit anderen Menschen zusammenarbeiten wollen. Man kann in Sachen Cybersicherheit wirklich Absolventen fast aller Fachrichtungen gebrauchen.

Welche Voraussetzungen müssen Absolventen mitbringen, um am BSI arbeiten zu können?

Bewerber im öffentlichen Dienst brauchen ein abgeschlossenes Studium. Deswegen empfehle ich, zuerst etwas zu studieren, was einem Spaß macht, und dann zu schauen, wie man es einbringen kann. Mein Tipp an Absolventen: Geht mit offenen Augen und gesundem Menschenverstand durch die Welt und stellt lieber ein paar Fragen mehr, als die erstbeste Firma in der Nachbarschaft zu nehmen. Lieber etwas mehr rumschauen und dafür dann etwas finden, was den eigenen Neigungen entspricht. Man arbeitet ja nicht nur für fünf Jahre. Daher sollte man sich etwas aussuchen, was auch Spaß macht. Und ich kann garantieren: IT-Sicherheit macht jahrelang Spaß!