CYBERKRIMINALI
UND
CYBERSECURI

OBR d.LFV Michael Jost *)

Kürzlich wurde die FF St. Ruprecht an der Raab Opfer eines Hackerangriffs. Auch der LFV Steiermark wurde schon zweimal Ziel von Cyberattacken und zeigt, dass auch gemeinnützige Organisationen jederzeit mit Angriffen rechnen und ihre Cybersecurity aufrüsten müssen.

Angriffe wie dieser finden im Internet auf der ganzen Welt täglich zu tausenden statt und verursachen nach Auskunft einer Studie einen weltwirtschaftlichen Schaden von ca. einer Billion Dollar (820 Mrd. Euro) pro Jahr. Die Schäden durch diese kriminellen Aktivitäten summieren sich damit auf mehr als 1% der globalen Wirtschaftsleistung. Die COVID-19 Pandemie und die damit verbundenen Home-Office-Aktivitäten vieler Unternehmen haben den Cyberattacken noch einen zusätzlichen Turbo verliehen. Viele Laptops sind über nur gering gesicherte Leitungen mit der Unternehmenszentrale verbunden und bieten so leichte Angriffsflächen für Cyberkriminelle.
Die Cyberkriminalität schreitet extrem schnell voran, lt. einem Bericht von RiskBased Security wurden 2019 weltweit 7,5 Milliarden Datensätze gestohlen, das sind um 112% mehr als im Jahr davor. Die am meisten betroffenen Stellen des Datendiebstahls sind medizinische Dienste, Unternehmen und Behörden. Aufgrund der rasant fortschreitenden Entwicklung der Cyberkriminalität geht man davon aus, dass die Ausgaben für Cybersicherheitslösungen weltweit bis 2022 auf 133 Mrd. US-Dollar steigen werden.

Der Autor
OBR d.LFV Michael Jost ist Dienststellenleiter des LFV Steiermark und Sonderbeauftragter für EDV im Landesfeuerwehrverband.

TÄT

TY

Cybercrime - Was sind die Motive?
Es gibt viele Motive für Cyberkriminalität, allen voran natürlich sind es natürlich finanzielle Gründe. Eine sehr häufige Form der Cyberkriminalität ist die Erpressung durch Verschlüsselung der Daten. Ein weiteres Motiv für Cyberkriminelle ist der Spaß an der Herausforderung. Viele Hacker sind am Anfang ihrer kriminellen „Karriere" jünger als 16 Jahre und agieren weniger aus krimineller Absicht, sondern weil sie sehr intelligent und neugierig sind und es einfach können.

Auch emotionale Gründe wie Wut oder Rache können dazu führen, dass Cyberkriminelle vor allem in sozialen Netzwerken aktiv werden und dort nach potenziellen Opfern suchen. Angebliche Verwandte im Ausland in finanzieller Not oder Internet-Bekanntschaften auf Plattformen für Partnersuchen sind oft Cyberkriminelle, die ihren Opfern sehr geschickt auf verschiedenste Weisen Geld entlocken. Wettbewerb oder ein schwaches Ego können ebenfalls Motivation für Cyberkriminalität sein. In den meisten Fällen stecken aber organisierte Banden bis hin zu Geheimdiensten hinter Attacken auf Einrichtungen und Netzwerke von Unternehmen und staatlichen Einrichten, primär um zu spionieren aber auch um Schaden anzurichten oder Geld zu erpressen.

Was ist ein Hackerangriff?
In den meisten Fällen wird ein Schadprogramm auf dem Computer über das Internet installiert, meist in Form eines Links in einem E-Mail oder beim Surfen auf unseriösen Webseiten. Diese Schadsoftware verschlüsselt alle Daten auf dem Computer und meldet eine Adresse, über die nach Zahlung eines Betrages in Form einer digitalen Währung (z.B. Bitcoin) die Daten wieder entschlüsselt werden können. Die Verschlüsselung erfolgt in den meisten Fällen so gut, dass das Opfer keine andere Wahl hat, als die geforderte Summe zu zahlen. Wenn Hacker gezielt Unternehmen mit dem Motiv der Erpressung attackieren, sind die geforderten Summen durchaus im sechsstelligen Bereich und höher. Die Frage, ob die Daten nach der Zahlung des Lösegeldes auch wirklich wieder entschlüsselt werden können, kann in über 90% der Fälle mit Ja beantwortet werden, andernfalls würde dieses System der Erpressung nicht funktionieren und niemand würde mehr Lösegeld bezahlen.

Was muss ich tun, wenn ich betroffen bin?
Wenn man von einem Hackerangriff betroffen ist, sollte man zunächst durch einen EDV-Spezialisten prüfen lassen, um welche Art von Angriff es sich handelt. Für einige der benutzten Verschlüsselungen gibt es im Internet bereits Entschlüsselungsprogramme, die die Daten zum Großteil wiederherstellen, ohne dass Lösegeld bezahlt werden muss. Sollte eine Entschlüsselung nicht möglich sein, hilft nur eine Datensicherung, die Daten wieder zu rekonstruieren. Sollte diese nicht vorhanden sein und die Daten sind von entsprechender Wichtigkeit, wird man um die Lösegeldzahlung nicht herumkommen. In jedem Fall ist bei der Behörde eine Anzeige gegen unbekannt zu erstatten.

Cybersecurity – Wie kann ich mich schützen?
Zu behaupten, dass es einen 100%igen Schutz gegen Hackerangriffe gibt, wäre falsch. Hacker sind darauf spezialisiert, Sicherheitslücken in Computersystemen zu finden und diese können sehr vielfältig sein. Neben dem Betriebssystem auf dem eigenen PC über häufig genutzte Anwendungen bis hin zum Mobiltelefon gibt es unzählige Möglichkeiten für Cyberkriminelle, Schadsoftware zu etablieren oder die Kontrolle über ein System zu gewinnen.
Sehr häufig geschieht es einfach durch ein E-Mail, das unter einem banalen Vorwand auf eine Internetseite verweist (Link) die dann im Hintergrund Schadsoftware auf dem eigenen PC installiert. In diesen Fällen spricht man von sogenannten Trojanern, die etwas Belangloses oder Alltägliches vortäuschen und dann im Hintergrund aktiv werden, um das System auszuspionieren oder Schadsoftware aus dem Internet zu laden und so den Computer für den Hack vorzubereiten.

Einen teilweisen Schutz vor solchen Angriffen bietet ein aktuelles Computersystem – „aktuell" heißt, dass das Betriebssystem laufend aktualisiert wird und ein Antivirensystem installiert ist, das ebenfalls laufend über die neuesten Updates verfügt. Am wichtigsten ist aber, Vorsicht beim Öffnen von E-Mails walten zu lassen. Links ins Internet in E-Mails sollten immer im Vorfeld geprüft werden bevor man sie anklickt. Dies erfolgt, indem man die Absender-E-Mail Adresse prüft und einfach den Mousecursor auf den Hyperlink im Mail legt, ohne diesen noch anzuklicken. Dann wird die Adresse angezeigt, auf die der Link verweist. Meist erkennt man daran schon, dass es sich um eine bedenkliche Adresse handelt. In diesem Fall ist das E-Mail sofort als SPAM-Mail zu entfernen. Neben dem Schutz ist aber auch eine Absicherung unerlässlich und das ist ein aktuelles Backup, also eine Sicherung aller relevanten Daten auf dem System. Dieses Backup sollte technisch so gewählt werden, dass die gespeicherten Daten auf einem Medium abseits des Computers gelagert werden (z.B. externe Festplatte oder Datensicherungsbänder) und nur an den Computer angeschlossen werden, wenn der Sicherungsvorgang durchlaufen wird. Eine Sicherung auf eine eingebaute Festplatte kann bei einem Hackangriff nutzlos werden, da auch die gesicherten Daten verschlüsselt werden. Daher muss man sich bei jedem Computer genau überlegen, wie und wie oft welche Daten gesichert werden müssen, um bei einem Totalausfall des Computers wieder auf die Sicherung der relevanten Daten zurückgreifen zu können.
Zusammengefasst kann gesagt werden, dass man sich mit dem Thema Cybersecurity genauer auseinandersetzen sollte. Die Sicherheit des Systems basiert auf einem aktuellen Betriebssystem inkl. Antivirenschutz, einem guten Backup-System und der Vorsicht des Nutzers vor möglichen Fallen im Internet.