Foto: Envato

HACKER

Katharina Kröll, BA

Das mit dem Internet nicht nur Vorteile einhergehen, musste die Freiwillige Feuerwehr St. Ruprecht an der Raab Ende April erfahren, als sie durch einen Fehler im System gehackt wurde. Hilfe kam aus den eigenen Reihen und zwar vom 17-jährigen Alexander Sandrießer, der den Informatikzweig der HTLBA Kaindorf besucht. Gemeinsam mit seinem Professor OStR. Dipl.-Ing. Gerold Haynaly konnten sie nicht nur der eigenen Feuerwehr helfen, sondern Menschen auf der ganzen Welt, die von dem gleichen Cyberangriff betroffen waren.

Der 17-jährige Alexander Sandrießer, Schüler der dritten Klasse an der HTLBA Kaindorf, war gerade beim Mathematiklernen, als ihn der Anruf seines Onkels am Nachmittag erreichte: die Freiwillige Feuerwehr St. Ruprecht a. d. Raab war zum Opfer einer Cyberattacke geworden. Ohne zu zögern machte sich Alexander, der seit einem Jahr Mitglied der Feuerwehr ist, mit seinem Fahrrad in Richtung Rüsthaus auf. Zu Beginn dachte er noch, es wäre ein Witz oder gar ein Missverständnis, denn wer kommt auf die Idee, eine Freiwillige Feuerwehr zu hacken? Vor Ort angekommen und nach einem kurzen Blick auf den PC stand fest, dass es sich nicht um einen kindischen Scherz handelte, sondern tatsächlich um einen Hackerangriff, der nicht nur bei der FF St. Ruprecht a. d. Raab Schaden anrichtete. Weltweit waren Unzählige von dieser Attacke betroffen.

Zwei Stunden zuvor

Für OLM Leon Christandl, der Schriftführer der FF St. Ruprecht a. d. Raab, sollte es ein ganz gewöhnlicher Nachmittag im Rüsthaus werden. Als er gerade im Begriff war, ein Dokument auszudrucken, bemerkte er, dass etwas mit dem Computer nicht in Ordnung war. Plötzlich waren alle Dateien verschlüsselt und mit einer Dateiendung versehen, die ihm völlig unbekannt war. Die einzigen Dateien, die sich zu diesem Zeitpunkt noch auf dem Rechner befanden, waren entweder unbrauchbar oder Textdateien, die mit dem Namen „read me“ versehen waren. In gebrochenem Englisch war dort zu lesen, dass sie den Schlüssel, der für die Entschlüsselung der Dateien essenziell ist, erst dann erhalten, wenn sie den Hackern über das Darknet 0.01 Bitcoins überweisen. Zu diesem Zeitpunkt wären das umgerechnet ungefähr 570 Euro gewesen. Nach dem Lesen dieser Nachricht war Christandl bewusst, dass es sich um ein ernstes Problem handelte und er ohne fremde Hilfe nicht weiterkommen würde, dennoch behielt er einen kühlen Kopf: „Kurz

Die FF St. Ruprecht an der Raab wurde kürzlich gehackt.

wurde mir heiß, aber dann habe ich so agiert, wie ich es als Einsatzleiter bei einem Verkehrsunfall mit eingeklemmten Personen tun würde: Die Schadenslage erfassen und Sonderkräfte anfordern und zwar sofort!“, schildert Christandl.

Nach dieser Erkenntnis war klar, die Polizei muss eingeschaltet werden, denn auf dem PC befanden sich sensible Daten wie die Brandschutzpläne großer Firmen, Sozialversicherungsnummern und sämtliche Informationen über alle Mitglieder.

ANGRIFF

Nach über
100 STUNDEN ARBEIT
konnten die verschlüsselten
DATEIEN GERETTET werden

Eine Anzeige bei der Polizei wurde zwar erstattet und die Daten konnten an das Landeskriminalamt übermittelt werden, aber leider hilft eine solche Anzeige nicht viel. Das ist auch für die Polizei eine komplexe Lage, denn um diese Delikte aufklären zu können, bedarf es einer jahrelangen und äußerst fundierten Ausbildung.

Der Gegner

Kurz nach dem Angriff war niemandem klar, ob sich der Hackangriff nur auf den einen Rechner beschränkte, denn vorübergehend ließen sich die Türen des Rüsthauses nicht öffnen. Jedoch konnte schnell Entwarnung gegeben werden, ein Fehler im System war für den temporären Schockmoment verantwortlich. Die Hacker hatten die vorhandenen originalen Dateien auf den Computern durch Verschlüsselte ersetzt. Es ging also darum, die gelöschten Dateien wieder herzustellen, denn diese zu entschlüsseln ist ohne den Schlüssel der Hacker fast nicht machbar. Bis heute ist nicht bekannt, wer hinter diesem Angriff steckte, was man allerdings weiß ist, dass die Hacker innerhalb von zwei Wochen mindestens 370.000 US-Dollar erbeutet haben.

Die Task Force

Anfänglich sah auch Alexander schwarz, nachdem er sich mit der Lage vor Ort vertraut gemacht hatte, wusste er, dass er helfen möchte. Da Cybersicherheit erst für vierte Jahrgänge als Wahlpflichtfach angeboten wird, bat er seinen Professor Gerold Haynaly um Hilfe. Der Professor, der unter anderem Netzwerktechnik und Security unterrichtet, war sofort mit an Bord und gemeinsam begannen die Beiden mit der Arbeit. Relativ schnell fanden sie im Internet ein Forum, in dem sich Leidensgenossen, die ebenfalls unter dem Cyberangriff zu leiden hatten, austauschten. „Durch dieses Forum hatte ich Kontakt mit Menschen aus der ganzen Welt. Egal ob in Kanada oder Singapur alle hatten mit den gleichen Problemen zu kämpfen“, erinnert sich Alexander. Durch diese Community fanden sie ebenfalls heraus, dass einige den geforderten Preis der Hacker bereits bezahlt hatten, jedoch damit nicht genug, denn sobald das Lösegeld eingezahlt wurde, erhöhten die Hacker den Preis für den Schlüssel auf 0.03 Bitcoin.

Deshalb warnen sowohl der Professor als auch der Schüler davor, diesen Forderungen nachzugehen, denn es ist nie sicher, ob der Schlüssel nach Zahlungseingang überhaupt freigegeben wird. Nach und nach entwickelten die Zwei neue Strategien, Ideen und Ansätze, wie man die verschlüsselten Dateien wieder zurückbekommen könnte. Nach über 100 Stunden harter Arbeit war es endlich geschafft: Bis heute konnten 94 Prozent der originalen Dateien mit den richten Namen, Endung und Struktur wiederhergestellt werden, die jetzt auf einer externen Festplatte sichergestellt sind. Vorsorglich wurde die Rüsthaussteuerung komplett vom Stromnetz genommen und neu aufgesetzt. Glücklicherweise beschränkte sich der Angriff „nur“ auf einen PC. Würden Hacker eine Feuerwehr gezielt angreifen, könnte theoretisch Schlimmeres als der Verlust von Daten passieren: Mittlerweile wird bei Feuerwehren vieles mithilfe technischer Geräte geregelt, würde die Rüsthaussteuerung angegriffen werden, könnte es sein, dass Alarmmeldungen nicht mehr bei Kameraden eingehen oder Tore sich bei Einsätzen nicht öffnen lassen.

OStR. Dipl.-Ing. Gerold Hanaly mit OLM Leon Christandl und Alexander Sandrießer

Kostenlose Hilfe

Das Problem, welches für diesen weltweiten Angriff verantwortlich war, war eine Sicherheitslücke in einem Programm, zu dem der Hersteller kein Update bereitstelle. So war es den Hackern ohne viel Aufwand möglich, in die Computer tausender Menschen einzudringen und erheblichen Schaden zu verursachen. Jeder Schritt, der zur Lösung des Problems beitrug, wurde von Alexander akribisch genau festgehalten. Schlussendlich entstand ein über 90 seitenlanger Blogeintrag, in dem die gesamten Erkenntnisse festgehalten und veröffentlicht wurden. Dieser Eintrag ist für jeden abrufbar und soll dafür sorgen, dass jeder die verschlüsselten Daten kostenfrei zurückbekommt. Bis heute haben 40.000 Menschen diesen Eintrag gelesen und viele neue Lösungsansätze sind hinzugekommen.

Alexander Sandrießer und sein Professor dachten nicht eine Sekunde daran, Geld für ihrer Leistung zu verlangen, nicht von der Feuerwehr und auch nicht von jenen, die ihre Anleitung verwendeten. Angebote gab es aber genügend „Wir wollten nie irgendetwas für unsere Arbeit verlangen, für die Leute ist es schon schlimm genug, dass sie gehackt wurden", führt Professor Haynaly weiter aus. Stellungnahme von dem Unternehmen gab es keine. Erst ungefähr sechs Wochen später brachte das Unternehmen dann ein Programm heraus, mit dem Betroffenen ihre Originaldateien wieder zurückerlangen konnten. Diese Anleitung verwies auf den von Alexander und seinem Professor anonym verfassten Blogeintrag.

Große Dankbarkeit

„Ohne das selbstlose Handeln von Professor Haynaly und unserem Feuerwehrkameraden Alexander wäre die Situation niemals so glimpflich ausgegangen. Wären sie nicht gewesen, weiß ich nicht, was wir als Feuerwehr getan hätten. Wenn wir eine Firma beauftragt hätten, das zu leisten, was die beiden kostenlos für uns getan haben, hätten wir mit mindestens 20.000 Euro rechnen müssen", erzählt Christandl sichtlich erleichtert. Der Schriftführer sieht aber nicht nur Negatives in dem Angriff, vielmehr sei es ein Denkanstoß für die Zukunft: „Es müssen neue Strategien überlegt und erarbeitet werden, wie wir sensible Daten besser schützen können. Der Anfang wird sein, dass die Feuerwehr auf Anraten von Professor Haynaly zumindest drei Back-ups erstellen wird, die auf unterschiedlichen Speichermedien abgesichert werden.

Hoffentlich kann diese Geschichte anderen Feuerwehren zeigen, dass ein Bewusstsein für Internetkriminalität gebildet werden muss, denn wie wir gesehen haben, kann es jeden treffen!", so Christandl. Noch heute kommt von den Feuerwehrkameraden und dem Lehrpersonal sehr viel Lob für ihre erbrachte Leistung an.

Der **17-JÄHRIGE ALEXANDER** hat sensible **DATEN** der Feuerwehr **RETTEN KÖNNEN**