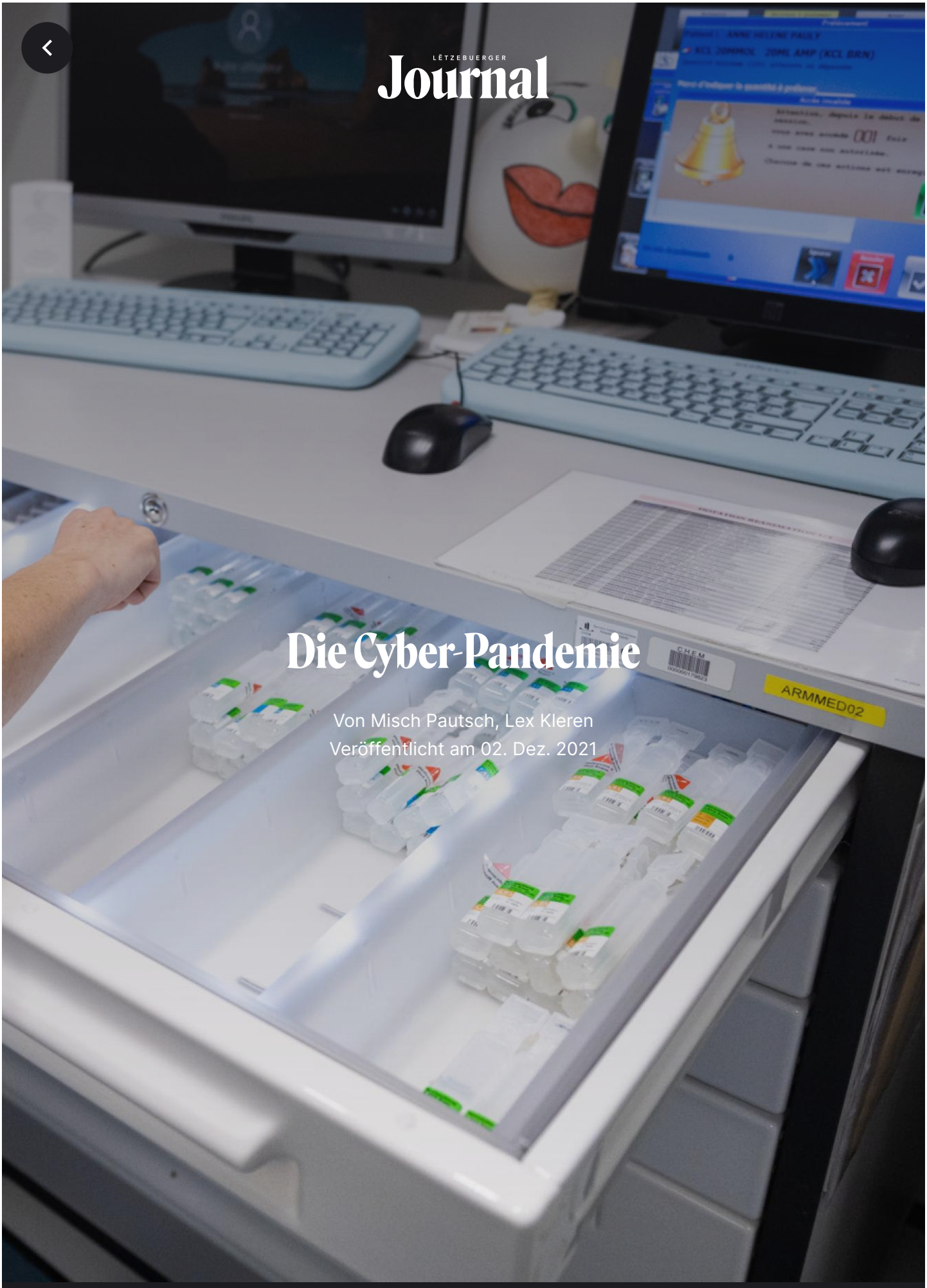
LËTZEBUERGER Journal



Die Cyber-Pandemie

Von Misch Pautsch, Lex Kleren
Veröffentlicht am 02. Dez. 2021

Diesen Artikel hören

11:34

Die Zahl der IT-Angriffe gegen Krankenhäuser ist weltweit während der vergangenen zwei Jahre drastisch gestiegen – teilweise mit tödlichen Konsequenzen. Luxemburgs Krankenhäuser konnten Angriffe erfolgreich abwehren. Aber der Kampf gegen die organisierten, oft staatlich unterstützten Banden geht weiter. Der Druck steigt.

Hinter den Kulissen der bereits dramatischen Szenen in den Krankenhäusern wird täglich ein zweiter, unsichtbarer Kampf ausgefochten: Organisierte Cracker-Gruppen profitieren von der Pandemie, um ihre Angriffe gegen das Gesundheitswesen zu verschärfen. Ransomware-Angriffe, bei denen Benutzer*innen aus ihrem infizierten Computer ausgesperrt werden, bis sie den Crackern ein Lösegeld überweisen – infizierte Computer zeigen einen „praktischen“ Hilfe-Bildschirm, auf dem Schritte zum Entsperren aufgelistet werden –, waren vor der Pandemie noch so programmiert, dass sie ziellos möglichst viele Leute treffen: Je mehr Opfer, desto mehr Lösegeld. Mittlerweile scheint sich der Fokus verlagert zu haben, sagt Paul Rhein, der Direktor des staatlichen Computer Emergency Response Teams (GOVCERT), das dem Hochkommissariat für nationale Sicherheit untersteht: „Der große Wandel über die letzten Jahre ist, dass der Fokus von Privatleuten auf Unternehmen gewechselt ist.“

Groß angelegte Ransomware-Attacken beschränken sich nicht auf den Gesundheitssektor, wie die Angriffe auf die größte Benzin-Pipeline in den USA, die Colonial-Pipeline, oder Fleischverarbeitungsfabriken von JBS, dem größten Fleischverarbeitungskonzern der Welt, zeigen. Bei diesen „Kampagnen“ wurden koordiniert Computer in den USA, Kanada und Australien blockiert, beide Male mit verheerenden Konsequenzen für weitreichende Lieferketten. „Krankenhäuser sind besonders jetzt, in der aktuellen Situation, ein dankbares Ziel für Cyberangriffe“,

erklärt Rhein. In schwer belasteten Krankenhäusern können selbst kleine Ausfälle zu schwerem menschlichem Schaden führen: Umso größer ist das Inzentiv für die Verantwortlichen, das Lösegeld, das eingefordert wird, auch zu zahlen – schließlich stehen Menschenleben auf dem Spiel.

Wenn Computerviren tödlich sind

Mindestens ein Todesfall in Düsseldorf zeigt, dass diese Ängste nicht unbegründet sind. Hier musste eine Frau in ein anderes Krankenhaus verlegt werden, nachdem ein Ransomware-Programm 30 Server des Krankenhauses lahmgelegt hatte. Während eine Untersuchung zeigte, dass die Frau vermutlich auch ohne den Angriff gestorben wäre, zeigt der Fall die potentielle Gefahr solcher Angriffe. Hatten einige Gruppen zu Beginn der Pandemie noch eine „Corona-Pause“ angekündigt, scheint diese also nun ins Gegenteil umgeschlagen zu sein. „Diese Angriffe haben hohe Kosten an allen Fronten“, schreibt das Genfer CyberPeace Institut: „Ressourcen, die für die Bekämpfung von COVID-19 bestimmt sind, werden lahmgelegt, die Sicherheit von Patienten wird gefährdet, sensitive Daten werden gestohlen und das Vertrauen der Gesellschaft in das Gesundheitssystem wird unterwandert.“

Paul Rhein, GOVCERT.lu

„Leider“, bedauert Rhein, „werden die Täter hinter solchen Angriffen nur selten zur Rechenschaft gezogen.“ Für die Cracker sind solche Angriffe mit niedrigem Risiko und sehr hohem potenziellen Gewinn verbunden: Lösegeld-Forderungen reichen gerne in die Millionen und grenzüberschreitende Ermittlungen außerhalb der EU sind äußerst schwierig.

Die Zahl der Cyberangriffe auf Krankenhäuser ist seit Beginn der Corona-Pandemie deutlich gestiegen. Allein zwischen November 2020 und Februar 2021 ist die Zahl der Attacken gegen den Gesundheitssektor durch unterschiedliche Cyberangriffe wie „Ransomware, Botnets, remote code execution und DDoS Angriffe“, die Netzwerke, Systeme oder Computer auf unterschiedliche Weisen beschädigen laut Check Point in Zentraleuropa um 145 Prozent gestiegen. Deutsche Krankenhäuser wurden sogar von 220 Prozent mehr Angriffen getroffen. Koordinierte Angriffe in den Vereinigten Staaten haben manche Ärzt*innen gezwungen, tagelang auf handgeschriebene Notizen zurückzugreifen, Operationen wurden unmöglich, die gesamte Organisation und Koordination brach stunden- bis tagelang zusammen. Auch in Luxemburg sind solche Attacken häufiger geworden, bestätigt Rhein. „Ganz aktuell läuft eine Angriffs-Kampagne namens ‚Squirrelwaffle‘, die unter anderem ‚droper‘ oder ‚trojaner‘ auf betroffenen Maschinen installiert.“

Diese Situation könne sich zu einer großen Ransomwarekampagne entwickeln, denn Ransomware-Angriffe sind nur die letzte Stufe koordinierter Attacken: Cyberangriffe bestehen meist aus mehreren wiederholenden Etappen, die mehr oder weniger ausgetüftelt sein können: Ausspähen, Infektion, Stehlen von Dateien, und/oder Verschlüsselung, Erpressung und Defacement (ein Angriff auf eine Internetseite, die ihre Erscheinung verändert, vergleichbar mit „elektronischem Grafitti“). „Diese passieren prinzipiell in Wellen, die besonders ausgeprägt sind, wenn neue oder besonders performante Software entwickelt oder angepasst wurde, wie beispielsweise die Software namens ‚Emotet‘. Solche Angriffe sind prinzipiell nicht nur auf einen Sektor beschränkt“, sagt Rhein.

„Ein Arbeitsnetzwerk könnte zum Beispiel infiziert werden, indem ein Arbeitslaptop einmal am gleichen Netzwerk hing wie ein privater, infizierter Laptop.“

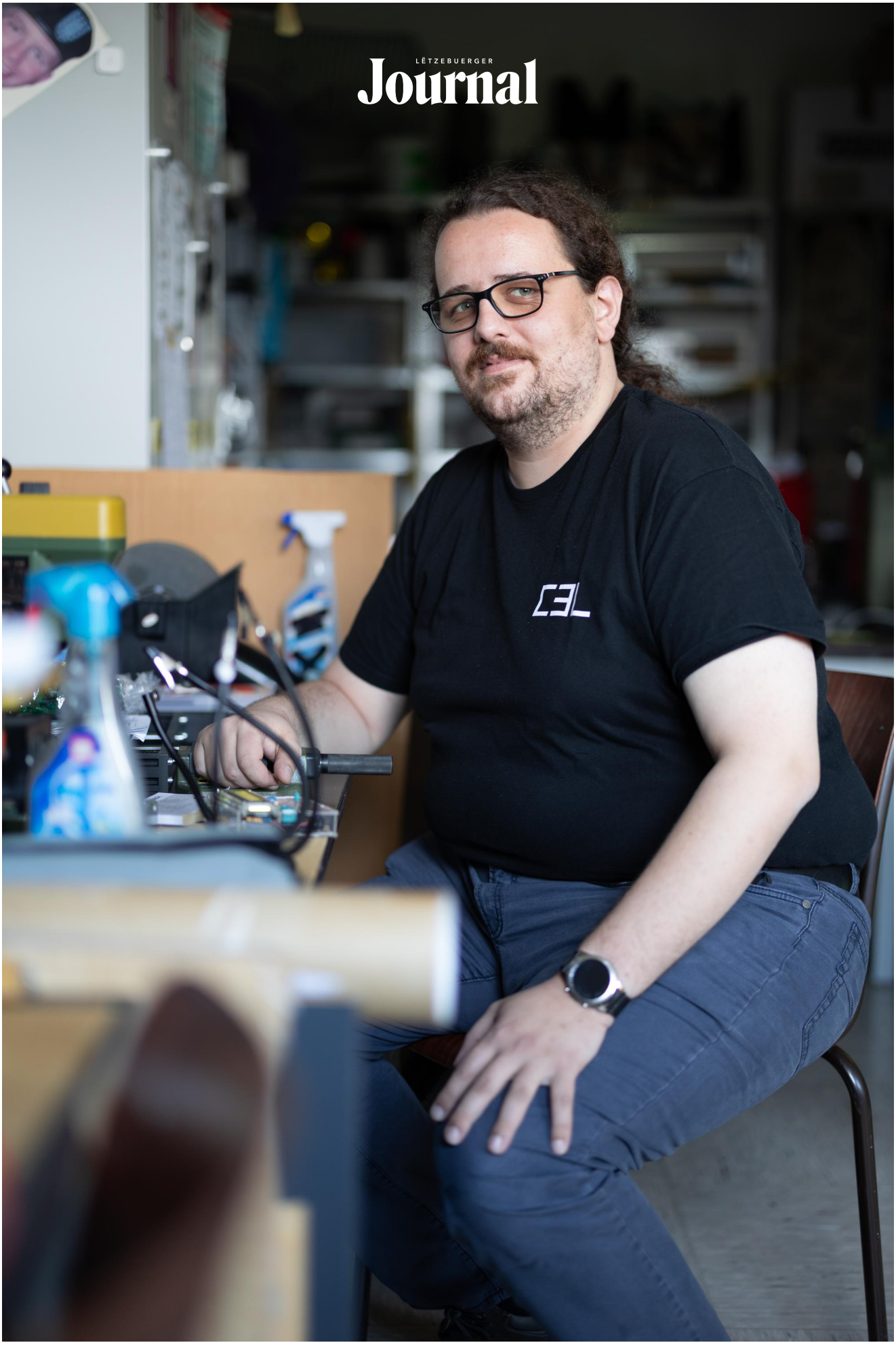
Dennis Fink vom Chaos Computer Club Luxembourg (C3L) beschreibt, wie perfide bösartige Programme dabei funktionieren kann: „Bei performanter Malware sehen wir, dass sie weit mehr tut, als sich nur auf einem Computer einzunisten. Ein Fall in einem Krankenhaus in Großbritannien 2017 hat gezeigt, wie Software automatisch von einem infizierten Gerät aus dem Netzwerk nach weiteren Sicherheitslücken durchsucht hat. Ein Arbeitsnetzwerk könnte zum Beispiel infiziert werden, indem ein Arbeitslaptop einmal am gleichen Netzwerk hing wie ein privater, infizierter Laptop.“ Hat sich das nahezu unsichtbare Programm einmal im Netzwerk ausgebreitet, ebnet es den Weg für weitere Software, unter anderem auch Ransomware, die dadurch in allen infizierten Maschinen gleichzeitig aktiviert werden kann – ohne dass der*die Besitzer*in der ersten betroffenen Maschine je wusste, dass sein Computer Patient Null war.

Hinzu kommt, wie Fink erklärt, dass Krankenhäuser generell dazu tendieren, ihre Software nicht sofort zu updaten – einer der wichtigsten präventiven Schritte gegen eine Infektion: „Ich weiß nicht genau, wie die Situation in Luxemburg ist, aber tendenziell arbeiten Krankenhäuser häufig mit älteren Software-Versionen, weil sie Systeme vorziehen, von denen sie sicher sind, dass sie zuverlässig laufen.“ Updates könnten mit Kompatibilitätsproblemen einherkommen, es könnten sich unbekannte Bugs (Systemfehler) in kritische Maschinen einschleichen „und es ist nicht so praktisch, wenn der Techniker alle paar Tage alle Maschinen von Hand updaten muss. Also arbeiten sie lieber mit alten, zuverlässigen Versionen, die sicher funktionieren. Das ist an sich nicht verwerflich, solange das System gut vom Internet isoliert ist … wovon ich vor allem bei Krankenhäusern stark ausgehe.“

Vollbremsung

In einem Worst-Case-Szenario, in dem der gesamte Betrieb von einem Moment auf den nächsten gestoppt wird, meint Fink, sei generell „je nach Art der Software nicht mehr viel zu machen, außer auf Backups zurückgreifen – wenn diese nicht zum Zeitpunkt des Angriffes auch gesperrt wurden – … oder zahlen. Überraschenderweise bekommen die Leute scheinbar in den meisten Fällen tatsächlich das Passwort zugeschickt, wenn sie das Geld überweisen.“ Die Cracker posieren als verzerrte „Dienstleister“, die den Leuten ihre Daten „zurückgeben“ und wollen dementsprechend auch, dass ihre „Kund*innen“ zufrieden sind. Häufig erklärt das nicht wegklickbare Fenster, auf dem die Schritte zum Freischalten des Computers aufgelistet werden – nachdem das Virus aktiv wurde –, dass der Computer „zum Schutz der Dateien“

gesperrt wurde, weil er von einem anderen, bösartigen Programm infiziert worden sei. Zum Dank für diesen „Schutz“ solle man nun die angegebene Summe an die unbekannten Wohltäter*innen zahlen, damit sie den Computer „geschützt haben“. Obszöne Ironie.



Dennis Fink, Chaos Computer Club Luxembourg

Das tatsächliche Motiv hinter den Cyberattacken ist jedoch laut GOVCERT.lu-Direktor Paul Rhein fast immer Geld: „Bei den Erpressungsversuchen geht es meist um finanzielle Interessen. Es kann natürlich nicht ausgeschlossen werden, dass andere Aspekte eine Rolle spielen können, wie wir bei einigen Situationen im Ausland gesehen haben. Aktuell beobachten wir bei uns im Land jedoch immer, dass es schlussendlich darum geht, Geld zu erpressen. Wir sehen uns heute mit einem regelrechten Ökosystem konfrontiert, in dem verschiedene Akteure unterschiedliche illegale Dienstleistungen anbieten um anderen Kriminellen ihr Handwerk zu ermöglichen“.

Für diese kriminellen Organisationen scheint es laut Expert*innen einen sicheren Hafen zu geben: Russland. Weil viele „Ransomware Gangs laut Cybersecurity-Experten aus der Ukraine und Russland operieren“ – in den Augen vieler Analyst*innen mit der stillen Zustimmung des Kremls –, wurde Russland im Oktober 2021 von einer Versammlung von Vertreter*innen von 30 Ländern zum Thema Cybersecurity und Ransomware ausgeschlossen.

Ein ungewöhnlicher Weg, sich gegen entsprechende Attacken zu schützen, untermauert solche Anschuldigungen, spekuliert Dennis Fink vom C3L: „Wenn man sich den Code von vielen dieser Viren anschaut, stellt man fest, dass ein ganz präzises Kriterium existiert, das verhindert, dass sie aktiv werden: russische Tastaturen. Tatsächlich ist das eines der Hauptkriterien, nach denen viele Viren gesucht haben. Sie schienen also ganz spezifisch russischsprachige Computer aus ihren Kampagnen auszuschließen. Vermutlich, weil die Banden dann mehr Streit mit dem Staat bekommen würden als es ihnen wert ist. Ich muss mir noch so eine Tastatur besorgen.“

„Bei den Erpressungsversuchen geht es meist um finanzielle Interessen. Wir sehen uns heute mit einem regelrechten Ökosystem konfrontiert, in dem verschiedene Akteure unterschiedliche illegale Dienstleistungen anbieten.“

Paul Rhein, Direktor von GOVCERT.lu

Für kritische Infrastrukturen wie Krankenhäuser jedoch offensichtlich keine erfolgsversprechende Strategie, ausschließlich russische Tastaturen zu installieren. Die Aufgabe, solche wichtigen Systeme im Auge zu behalten, obliegt dem GOVCERT, wie ihr Direktor erklärt: „Unser Ziel ist, allen Organisationen, die in unseren Bezirk fallen den bestmöglichen Schutz gegen Cyberangriffe zu bieten, wobei wir uns im Klaren sind, dass 100-prozentige Sicherheit nicht existieren kann. Was vom Menschen geschaffen wurde, kann auch vom Menschen zerstört werden. Aber die letzte und einzige Infektion durch eine Ransomware von einem Laptop unserer Kunden geht auf 2017 zurück. In diesem Fall hat es gereicht, die Maschine zu isolieren und auf Backups zurückzugreifen.“ Generell seien Backups und Isolation von infizierten Maschinen die Hauptmechanismen, wenn Prävention und Detektion nicht gereicht haben.

Notfallplan

„Im Falle eines koordinierten Angriffes auf den gesamten Gesundheitssektor mit einem signifikanten Einfluss auf nationalem Niveau, hat das Hochkommissariat für nationale Sicherheit den ‚Plan d’intervention d’urgence Cyber (PIU Cyber)‘ ausgearbeitet, um auch diese Situation zu meistern“, erklärt Paul Rhein. Bisher war dies jedoch nicht nötig: „Bis heute hat noch keiner der zahlreichen Angreifer es geschafft, Daten bei uns zu verschlüsseln oder ein Lösegeld zu erhalten.“

In letzter Instanz jedoch, betont Rhein, liege die „rechtliche Verantwortung beim ‚Besitzer‘ des IT-Systems“. Und diese lassen sich beim Thema Cybersecurity nicht gerne in die Karten schauen. Auf *Journal*-Anfrage hin bestätigt das Centre Hospitalier Emile Mayrisch (CHEM) nur, dass sich ihre IT-Teams der Gefahren bewusst seien und sie die Situation gemeinsam mit GOVCERT (zentrale Kontaktstelle für alle Arten von IT-Vorfällen, die die Informationssysteme der Regierung und anderer als kritisch eingestufter öffentlicher oder privater Infrastrukturbetreiber gefährden könnten) im Blick hätten – viel mehr könne man aus sicherheitstechnischen Gründen nicht preisgeben. Die anderen Krankenhäuser wollten gar keinen Kommentar zu dem Thema abgeben.

„Cybersecurity ist nie eine abgeschlossene Aufgabe“, fasst der GOVCERT-Direktor zusammen, „sondern ein fortlaufender Prozess.“ Immer häufigere und raffiniertere Attacken werden diesen Prozess in Zukunft sicher nicht einfacher machen, vor allem wenn in Krankenhäusern mehr als ohnehin schon jede Sekunde und jedes freie Bett zählt.

Veröffentlicht am 02.12.2021
Aktualisiert am 15. Dez. 2021 um 20:28

Misch Pautsch

Journalist und Fotojournalist

Lex Kleren

Fotojournalist und Bildredakteur