Angriff mit globalen Folgen

USA Ein Hackerangriff auf eine IT-Firma in den USA hat Auswirkungen bis nach Europa. Nun hat US-Präsident Joe Biden die Geheimdienste mit der Untersuchung des Vorfalls beauftragt.

Bei der jüngsten Attacke mit Erpressungssoftware haben Hacker in den USA auf einen Schlag hunderte Unternehmen ins Visier genommen. Sie nutzten eine Schwachstelle beim amerikanischen IT-Dienstleister Kaseya, um dessen Kunden mit einem Programm zu attackieren, das Daten verschlüsselt und Lösegeld verlangt.

Folgen waren bis nach Schweden zu spüren, wo die Supermarkt-Kette Coop fast alle Läden schliessen musste. Das volle Ausmass der Schäden blieb zunächst unklar. Die IT-Sicherheitsfirma Huntress sprach von mehr als 1000 Unternehmen, bei denen Systeme verschlüsselt worden seien.

US-Präsident Joe Biden ordnete eine Untersuchung des Angriffs durch die Geheimdienste an. «Der erste Eindruck war, dass die russische Regierung nicht dahintersteckt – aber wir sind uns noch nicht sicher», sagte Biden nach Fragen von Reportern am Samstag. IT-Sicherheitsexperten hatten die Attacke anhand des Software-Codes der Hackergruppe REvil zugeordnet, die in Russland verortet wird.

REvil steckte vor wenigen Wochen bereits hinter dem Angriff auf den weltgrössten Fleischkonzern JBS, der als Folge für mehrere Tage Werke unter anderem in den USA schliessen musste. Biden hatte den russischen Präsidenten Wladimir Putin bei deren Treffen in Genf im Juni aufgefordert, auch keine Aktivitäten von Hackergruppen zu tolerieren und mit Konsequenzen bei weiteren Attacken gedroht.

Joe Biden rätselt: Steckt die russische Regierung hinter dem Angriff? Den Verdacht sollen nun die Geheimdienste klären. KEY

Eine Kettenreaktion

Kaseya teilte am Wochenende mit, nach bisherigen Erkenntnissen seien weniger als 40 Kunden betroffen. Allerdings waren darunter auch wiederum Dienstleister, die ihrerseits mehrere Kunden haben. Auf diesem Wege traf es auch die schwedische Coop-Kette, bei der die Kassensysteme nicht mehr funktionierten. Nur 5 der gut 800 Märkte – und der Online-Shop – blieben geöffnet.

Der Schaden hätte auf jeden Fall weit grösser sein können: Kaseya hat insgesamt mehr als 36 000 Kunden. Mit Hilfe des Kaseya-Programms VSA verwalten Unternehmen Software-Updates in Computer-Systemen. Ein Eindringen in die VSA-Software kann den Angreifern also viele Türen auf einmal öffnen.

Kaseya stoppte am Freitag seinen Cloud-Service und warnte die Kunden, sie sollten sofort auch ihre lokal laufenden VSA-Systeme ausschalten. Nach Angaben des Unternehmens waren Kunden des Cloud-Dienstes zu keinem Zeitpunkt in Gefahr – und alle betroffenen Firmen griffen auf lokale VSA-Installationen zurück. Kaseya sei zuversichtlich, die Schwachstelle gefunden zu haben, wolle sie demnächst schliessen und die Systeme nach einem Sicherheitstest wieder hochfahren, hiess es. Am Samstag kam noch ein Kunde zur Liste der Opfer dazu, der sein lokal laufendes VSA-System nicht abgeschaltet hatte.

Hohes Lösegeld

Attacken mit Erpressungs-Software hatten zuletzt wiederholt für Schlagzeilen gesorgt. Nur kurz vor dem JBS-Fall stoppte ein Angriff dieser Art den Betrieb einer der grössten Benzin-Pipelines in den USA und schränkte die Kraftstoffversorgung in dem Land vorübergehend ein. Den Hackern bringt es Geld: JBS zahlte den Angreifern umgerechnet elf Millionen Dollar in Kryptowährungen, der Pipeline-Betreiber Colonial 4,4 Millionen Dollar. Allerdings konnten Ermittler wenig später gut die Hälfte des Colonial-Lösegeldes beschlagnahmen. Es ist auch bereits die zweite binnen weniger Monate bekanntgewordene Attacke, bei der Hacker über einen IT-Dienstleister in Systeme seiner Kunden eindringen konnten. Über Wartungssoftware der Firma Solarwinds waren Angreifer vermutlich zu Spionage-Zwecken in Computernetzwerke von US-Regierungsbehörden gekommen, unter anderem beim Finanz- und Energieministerium.

Attacken mit Erpressungs-Trojanern hatten in den vergangenen Jahren mehrfach für Schlagzeilen gesorgt. 2017 legte im Mai der Erpressungs-Trojaner «WannaCry» neben den Computern vieler Privatleute unter anderem Computer in britischen Spitälern sowie Fahrplan-Anzeigen der Deutschen Bahn lahm. Wenige Wochen später traf die Lösegeld-Software «NotPetya» unter anderem die Reederei Maersk und den Nivea-Hersteller Beiersdorf.

«Wir bringen alles online»

Diese Attacken breiteten sich seinerzeit unter anderem deshalb so schnell aus, weil Computer mit älteren Windows-Systemen und nicht geschlossenen Sicherheitslücken für sie ein leichtes Opfer waren. Sie galten deshalb als ein Weckruf für mehr IT-Sicherheit. Dennoch gab es nun erneut mehrere erfolgreiche Angriffe mit Lösegeld-Software.

Die Pandemie und die Arbeit von zu Hause aus verschärfte die Situation laut Experten. Mikko Hyppönen von der IT-Sicherheitsfirma F-Secure führt dies unter anderem darauf zurück, dass die Angriffsfläche mit dem digitalen Wandel grösser werde: «Wir bringen alles online.» Es werde noch dauern, bis diese allgemeine Bewegung ins Netz angemessen abgesichert werde: «Ich denke nicht, dass wir das Schlimmste schon erlebt haben.» Raj Samani von der IT-Sicherheitsfirma McAfee sieht das Problem auch darin, dass sich inzwischen eine ganze Industrie gebildet habe, in der Attacken mit Erpressungssoftware Interessenten als Bezahl-Service angeboten werden. *sda*

Bisher kein Schweizer Opfer

Nach der Cyber-Attacke stehen die Schweizer Behörden mit dem betroffenen IT-Dienstleister Kaseya in Kontakt. Zunächst war nichts von Schweizer Firmen unter den Opfern bekannt. Beim Nationalen Zentrum für Cybersicherheit (NCSC) seien bislang keine entsprechenden Meldungen eingegangen, teilte eine Sprecherin des Eidgenössischen Finanzdepartements (EFD) gestern Abend auf Anfrage der Nachrichtenagentur Keystone-SDA mit. Es sei aber gut möglich, dass ein Angriff erst mit dem Beginn der Arbeitswoche heute bemerkt und gemeldet werde. *sda*

Neue Leitung für den Innovationspark

Biel Raoul Stöckle ist der neue Chef der Switzerland Innovation Park Biel/Bienne AG. Bereits ziehen die ersten Mieter in den Neubau ein.

Raoul Stöckle hat die operative Leitung der Switzerland Innovation Park Biel/Bienne AG (SIPBB) übernommen. Der CEO-Wechsel von Felix Kunz zu ihm erfolgte per 1. Juli, wie die SIPBB mitteilt. Kunz hatte während acht Jahren den Aufbau des Innovationsparks geleitet. Er werde künftig die Funktion als Delegierter des Verwaltungsrats haben und sich in strategischen Projekten einbringen, heisst es in der Mitteilung weiter. Stöckle werde den SIPBB «nach einer intensiven Aufbauphase in ein stabiles Wachstum überführen», wird Kunz zitiert. Kunz selber wird für das Museum Enter in Solothurn einen Neubau realisieren.

Erfahren im Forschen und Gründen

Raoul Stöckle verfügt über breite Forschungserfahrung. Er hat an der University of Kent Materialwissenschaften studiert und an der ETH Zürich in Physik und Chemie promoviert. Zudem verfügt er über ein MBA. Er kenne als Seriengründer die Möglichkeiten und Hürden von Startup-Gründern aus eigener Erfahrung, teilt die SIPBB mit. «Der Switzerland Innovation Park Biel/Bienne bietet mir die Möglichkeit, die verschiedenen Erfahrungen aus meinen beruflichen Stationen symbiotisch einzubringen», wird er in der Mitteilung zitiert.

Weit fortgeschritten ist der Neubau des Innovationsparks am Bieler Walserplatz. Derzeit beziehen sowohl das Personal als auch die Mieter und Kooperationspartner der SIPBB AG schrittweise ihre Räumlichkeiten, während noch letzte Arbeiten am Innenausbau im Gang sind. Der Vermietungsstand ist laut Mitteilung «über Erwarten positiv». Die offizielle Eröffnung erfolgt Ende August.

Neue Verwaltungsräte

Auch im Verwaltungsrat der SIPBB AG hat es Veränderungen gegeben. An der ordentlichen Generalversammlung Ende Juni wurden Hans Gattlen und Sebastian Wörwag neu in das Gremium gewählt. Gattlen ist unter anderem in der Swiss Factory Group AG in Neuenegg engagiert. Wörwag ist seit 2020 Rektor der Berner Fachhochschule BFH, die ihren Campus für Technik und Architektur gleich gegenüber dem Innovationspark realisieren wird. Seine Wahl reflektiere die «heute sehr engen strategischen Verbindungen zwischen SIPBB AG und der BFH als auch die gemeinsamen Zukunftsaussichten». *mt*

Nachrichten

RECHTSSTREIT

Lafarge Holcim einigt sich mit US-Klägern

Der Zementkonzern Lafarge Holcim hat beim Rechtsstreit mit US-Klägern um die Nutzung enteigneter Grundstücke eine endgültige Einigung erzielt. So hätten sich die beiden Seiten in einer gemeinsamen Vereinbarung vom 22. Juni über eine Abweisung der Klage geeinigt, schrieb die «Sonntagszeitung» mit Verweis auf Gerichtsdokumente. Finanzielle Details zur Einigung sind keine bekannt. Gemäss den Dokumenten trägt jede Partei ihre eigenen Anwaltsgebühren, Kosten und Auslagen. Die Bedingungen der Vereinbarung sind vertraulich. Beobachter hielten der Zeitung zufolge eine Strafzahlung aus dreifachem Schadenersatz plus Anwaltsgebühren in Höhe von zu 160 Millionen US-Dollar für möglich. Beim Rechtsstreit ging es um ein Grundstück, welches nach der kubanischen Revolution beschlagnahmt wurde und auf dem LafargeHolcim und die kubanischen Regierung heute ein Zementwerk betreiben. *sda*

Jobsuche im digitalen Dschungel

Ratgeber

Pia Wegmüller

Zuerst einmal ganz analog: Die Gefahr ist gross, dass Sie sich im Dschungel der digitalen Jobplattformen verlieren. Nichts ist frustrierender, als Stunden zu investieren und am Schluss kaum Treffer zu haben. Darum ist es am besten, zuerst mal ganz analog vorzugehen: Klären Sie, was Sie genau suchen und welches Ihre beruflichen Wunschkriterien sind.

Welche Art von Job, Funktion suchen Sie? Welche Tätigkeiten wollen Sie ausüben? Mit welchen Produkten, Dienstleistungen oder Themen wollen Sie sich befassen? In welcher Branche, welcher Art von Firma, Organisation sehen Sie sich? Welche Rahmenbedingungen sind Ihnen wichtig?

Suchbegriffe als Kompass: Sie brauchen einen Kompass, um sich in der Fülle von Jobplattformen und digitalen Jobsuch-Möglichkeiten zu orientieren und gezielt vorzugehen. Ihre beruflichen Wunschkriterien sind Ihr Kompass. Aus Ihnen leiten Sie die Begriffe ab, mit denen Sie die Suchmaschinen füttern.

Stellen Sie Ihre Begriffsfavoriten zusammen. Dies können verschiedene Funktionsbezeichnungen sein. Hierbei dürfen Sie gerne kreativ denken. Wie könnten die potenziellen Arbeitgeber Ihre Wunschfunktion benennen? Sie können eine der geläufigen, allgemeinen Jobplattformen nutzen, indem Sie eine Wunschtätigkeit – zum Beispiel Immobilien bewirtschaften – eingeben und dann schauen, welche Funktionsbeschreibungen erscheinen.

Unrelevantes aussondern: Filtern ist das A und O, um im digitalen Dschungel genau das Richtige zu finden. Auf allen Jobplattformen können Sie selbst mit unterschiedlichen Kombinationen von Filterkriterien nach Ihren Traumjobs Ausschau halten. Oder Job-Abos definieren. Praktisch sind dabei die jederzeit abrufbaren Handy-Apps der Jobplattformen. Sie können damit jederzeit die in Frage kommenden Stellen auf eine Merkliste setzen. Berufsspezifische Plattformen sondern viel Unrelevantes von vornherein aus. Recherchieren Sie über Berufsverbände nach Links oder konsultieren Sie die Fachplattformen auf jobchannel.ch.

Eine andere Art vorzugehen ist, dass Sie sich vor allem auf Ihre Wunsch-Arbeitgeber konzentrieren. Werfen Sie einen Blick auf die digitalen «gelben» Seiten und suchen Sie dort nach Branchen oder nach Regionen. Einige Unternehmen haben spezielle Karriererubriken auf ihrer Webseite und geben Tipps und Ratschläge für Bewerberinnen und Bewerber.

Info: Pia Wegmüller ist stv. Geschäftsführerin und Beraterin im Frac, dem zweisprachigen Bieler Informations- und Beratungszentrum rund um das Thema «Arbeits- und Berufsleben gestalten». Kontakt über info@frac.ch oder 032 325 38 20.