Crime Fighter

Eine Leondinger IT-Firma hält mit einem ungewöhnlichen Ansatz Cyberangriffe von betrieblichen Infrastrukturen fern.

Von Daniel Pohselt

Gemeinsame Weggefährten: Alois Kobler, Gründer der Blue Shield Security (re.), mit den Eigentümern Günther Wiesauer und Johannes Siller (Mitte)

Es waren Profis am Werk. Solche, die nicht hitzefrei hatten. Als im vorigen Sommer im Heizungs-, Lüftungs- und Warmwasserbereitungskonzern Groupe Atlantic – zum 7.500-Mitarbeiter-Unternehmen zählt auch die Austria Email – eine Firmenübernahme im Gang war, witterten sie ihre Chance. Zeichnungsberechtigte des französischen Familienkonzerns waren aufgrund der Urlaubszeit

FOTOS: KLACZAK_BARBARA, FOTOLIA

teilweise nicht vor Ort. Also wandten sich die Angreifer an Führungskräfte der zweiten Reihe. Raffiniert formuliert – und auch orthografisch sattelfest – erging an ausgewählte Manager in E-Mails die Aufforderung, angesichts des anstehenden Zwischenclosings größere Summen auf ein Treuhandkonto zu überweisen. „Der Betrugsversuch wurde entlarvt, es entstand keinerlei Schaden“, erinnert sich Martin Hagleitner, CEO der Austria Email und in Konzernverantwortung unter anderem für die D-A-CH-Region. Dennoch war die Situation brisant. Und sie zeigte, dass sich Angreifer mit Unternehmensgruppen „und ihren Entscheidungsstrukturen, aber auch Kunden-Lieferantenbeziehungen mittlerweile intensiv beschäftigen“, sagt er.

„Angreifer beschäftigen sich heute sehr intensiv mit den Entscheidungsstrukturen von Unternehmen.“

Martin Hagleitner, CEO Austria Email

FOTOS: BEIGESTELLT

Liste des Grauens: geblockte Malware, Phishing-Versuche, alles im Blick

Skepsis wich Überzeugung. Und dennoch war Hagleitner Ende letzten Jahres trotz persönlicher Empfehlung skeptisch, als bei Austria Email ein Meeting mit dem Gründer einer auf IT-Security spezialisierten Firma angesetzt war. Ob Digitalisierung, Internet of Things oder eben IT-Sicherheit – „es ist schier beeindruckend, wie viel Hilfsbereitschaft Unternehmen in diesen Feldern von Consultants angedient bekommen“, sagt er. Doch die Sicherheitslösung, die der junge Mann bei einem schnellen Espresso skizzierte, weckte sowohl Hagleitners Interesse, als auch das von Gerhard Lampersber-

ger aus der IT & Organisation der Knittelfelder. Nicht nur, weil das Unternehmen in den Heartlands der Industrie, im oberösterreichischen Leonding, domiziliert ist. Dessen Gründer Alois Kobler (O-Ton Hagleitner: „Kein Schönredner und Faserschmeichler“) hat in der Blue Shield Security GmbH einer Lösung (Blue Shield Umbrella) ein Start-up-Umfeld geboten, die von den klassischen Firewalls absticht. Statt einer Namensauflösung auf externen DNS-Servern erfolgt diese auf Servern der Oberösterreicher. Der Eintrag, statt den DNS-Server des Internetproviders der Leondinger anzufragen, geht schnell vonstatten. So werden Gefahren nicht nur erkannt, sondern auch präventiv geblockt. Man habe damit „einen Schutzwall errichtet, statt Burgmauern weiter zu verstärken oder aufwendige Abwehrkämpfe innerhalb des Systems zu führen“, sagt Hagleitner. Lampersberger, seit 30 Jahren in der IT tätig, hat Zahlen. „Wir konnten bereits im Vorfeld 1.700 Phishing-Attacken abfangen, bevor überhaupt unsere Sicherheitsfilter greifen“, sagt er. Mit der Brechstange Zugänge zu sperren, war nie sein Ansatz. Weil es die Mitarbeiter

„Mitarbeiter können Mails gefahrlos öffnen, da die Schadsoftware nicht zum Nachladen kommt.“

Alois Kobler, Gründer
Blue Shield Security

unnötig einengt. Aber auch weil man potenzielle Kunden, die vielleicht nur den Geschäftsabschluss suchen, nicht einfach generalstabsmäßig wegblocken will, nur weil eine Adresse verdächtig erscheint. Mit dem Tool der Oberösterreicher ließen sich nun effizient die Blockaden prüfen: Blockierte Anfragen werden protokolliert und im Dashboard der Software aufbereitet dargestellt. Und das alles zu – wie er erzählt – nicht horrenden Kosten. Zusätzliche Lizenzen fallen auch keine an. Darüber hinaus lassen sich mobile Geräte wie Handys oder Laptops ebenfalls per App einbinden.

FOTOS: KLACZAK_BARBARA

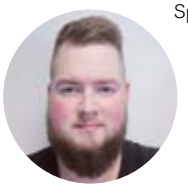
Anfänge im Jahr 2013. Die Anfänge der Blue Shield Security gehen auf das Jahr 2013 zurück. Damals, erzählt Alois Kobler, habe alles nach USA oder Asien geblickt, die Bedrohungen erhielten aber stärker regionalen Fokus. Mit zwei langjährigen Weggefährten realisierte Kobler – erfahren im Aufbau von Start-ups und Vertriebsstrukturen – die Story der Blue Shield Security. Günther Wiesauer, mit seiner Paladin Technologies GmbH zu 74 Prozent Mehrheitseigentümer des Unternehmens, „hatte die Idee zum Produkt", sagt Kobler. Johannes Siller, der mit seiner MapCon consulting GmbH die restlichen Anteile der Blue Shield Security hält, sei „eher der harte Stratege".

Der Großteil des Umsatzes (2018: vier Millionen Euro, heuer soll verdoppelt werden) des 36-Mitarbeiter-Unternehmens, das Referenzen im Versicherungssektor (Wiener Städtische), der Bau- und Fertigungsindustrie (Strabag, Kremsmüller, Austria Email, Banner) oder der Verlagsbranche (Oberösterreichische Nachrichten) hat, werde laut Kobler in F&E reinvestiert.

Training eines evolutionären Algorithmus. Die entscheidende Weichenstellung gelang schon 2013. Damals begannen die Oberösterreicher mit dem Training eines evolutionären, vorausschauenden Algorithmus, der Web Codes auf Schadsoftware scannt. Dieser – stetig um Erfahrungswissen angereichert – setzt bei der Prüfung Maßstäbe „und hat heute noch lange nicht ausgelernt", heißt es in Leonding. Die Anwender am Einzelrechner – egal ob in der Buchhaltung, am Notebook im Home Office oder dem Produktionstablet – können dabei nichts falsch machen. Mails können gefahrlos geöffnet werden, da die Schadsoftware – die Fachleute sprechen von Payloads – „nicht zum Nachladen kommt", erklärt Alois Kobler. Überzeugt hat die Lösung auch Martin Fischer, Netzwerkbetreuer und Spezialist für Informationssicherheit beim Batteriehersteller Banner. Speziell bei Bedrohungen in europäischen Sprachen zeige das Tool „sehr hohe Erkennungsraten gegenüber anderen Lösungen", sagt er. Und als das Schadprogramm WannaCry 2017 in der Ukraine wütete, warnten Fischer befreundete IT-Kontakte aus der Region schon über Nacht vor, was hier im Anrollen sei. Ein Blick ins Reporting des Tools ließ ihn dann aber wieder ruhig schlafen: Die Lösung der Leondinger hatte die Angriffe bereits geblockt.

„Speziell bei Bedrohungen in europäischen Sprachen zeigt das Tool sehr hohe Erkennungsraten."

Martin Fischer, Netzwerkbetreuer und Spezialist für Informationssicherheit, Banner



FOTOS: BEIGESTELLT