GSV
Die Plattform für Mobilität

Bericht zum GSV-Forum „Cyberangriffe – Erfahrungen und Gegenstrategien“

Cyberangriffe, also böswillige und vorsätzliche Versuche einer Person oder Organisation, die Sicherheit des Informationssystems einer anderen Person oder Organisation zu beeinträchtigen, treten immer häufiger auf – auch in Österreich. Dies ist einerseits dem Trend der zunehmenden digitalen Vernetzung geschuldet und andererseits der Tatsache, dass Angriffe von immer mehr Personen ohne großes Vorwissen durchgeführt werden können. Bei einem digitalen GSV-Forum zum Thema „Cyberangriffe – Erfahrungen und Gegenstrategien“ Ende Februar 2021 waren sich alle Experten einig, dass eigentlich kein Unternehmen vor derartigen Angriffen sicher ist. Es sind hauptsächlich kleine und mittlere Unternehmen betroffen, die bisher Cyberangriffe kaum bis wenig beachtet haben und gleichzeitig nur über begrenzte IT-Ressourcen verfügen. Doch auch große Unternehmen sind gefährdet: ein gutes Sicherheitsgefühl ist immer nur eine Momentaufnahme. Schutzfunktionen müssen ständig angepasst werden. Gleichzeitig gilt es weiter zu denken: Wie sicher sind beispielsweise Unternehmen der vor- und nachgelagerten Lieferkette? Ein gezielter Angriff an diesen Stellen kann ebenfalls beträchtlichen Schaden anrichten.

Erfahrungsbericht: Ein Cyberangriff legt ein weltweit operierendes Unternehmen lahm

Auch unser Mitglied PILZ GmbH, Anbieter sicherer Automatisierungstechnik für Maschinen und Anlagen, war im Jahr 2019 Opfer eines Cyberangriffes, wie David Machanek, Geschäftsführer der Tochtergesellschaft Pilz Österreich, berichtet: „Die ganze Unternehmensgruppe mit 42 Niederlassungen weltweit war betroffen.“

Hervorzuheben ist, dass es sich bei PILZ um ein Unternehmen handelt, dem das Thema zuvor durchaus bewusst war und welches sich sicherheitsmäßig gut aufgestellt gesehen hat. Es gab sogar Initiativen, die eigenen Kunden für das Thema zu sensibilisieren – wenn auch mit mäßigem Erfolg.

Am 13. Oktober 2019 wurde es offensichtlich, das Unternehmen wurde gehackt. „Was tatsächlich vorgefallen ist, ist erst nach einigen Stunden klar geworden: Cyber-Kriminelle waren ins Unternehmensnetz eingedrungen. Die Daten auf Rechnern und Servern weltweit wurden verschlüsselt und es wurde Lösegeld für die Entschlüsselung gefordert. Es handelte sich um einen sorgfältig geplanten und gezielten sogenannten Bitpaymer-Angriff auf PILZ. Mittel zur Verteidigung – wie Antivirenserver – wurden ebenfalls verschlüsselt“, berichtet Klaus Stark, Innovation Manager, PILZ GmbH in Deutschland.

Unbemerktes Eindringen im Vorfeld

Zu diesem Zeitpunkt war das Unternehmen bereits Monate lang unbemerkt infiltriert worden, geöffnete bösartige E-Mails haben das ermöglicht. In dieser Zeit wurden Schwachstellen in der IT-Infrastruktur gesucht und maßgeschneiderte Programme für einen Angriff entwickelt.

Mit weitreichenden Folgen: Computer, Festnetztelefonie, E-Mails, Customer-Relationship-Management (CRM)-Systeme, Dateiablagen, Telefonverzeichnisse und die Unternehmens-Website standen von heute auf morgen nicht mehr zur Verfügung. Das brachte enorme Herausforderungen in der Kommunikation mit Kunden, Lieferanten, den eigenen Mitarbeitern etc. mit sich.

Trotz der dramatischen Lage wollte PILZ auf die Forderungen der Verursacher nicht eingehen, betont Stark: „Da die Vertrauenswürdigkeit derartiger Erpresser nicht gegeben ist, haben wir ein Eingehen auf die Lösegeldforderungen von Anfang an ausgeschlossen.“

Ein Notbetrieb wurde eingerichtet

Nachdem der Angriff klarer wurde, habe man umfangreiche Erst-Maßnahmen getroffen, wie Stark weiter berichtet: „Wir haben unverzüglich alle IT-Systeme weltweit abgeschaltet und alle Mitarbeiter informiert, es geht nur mehr mit Papier und Handy. Als nächstes haben wir einen Krisenstab und Arbeitsgruppen gebildet und die Ermittlungsbehörden sowie die Aufsichtsbehörden informiert. Darüber hinaus haben wir auch externe Forensik-Spezialisten einbezogen, alleine das hat einen höheren sechsstelligen Euro Betrag gekostet. Für den internen Austausch richteten wir einen sicheren Messenger-Dienst ein und hielten tägliche Telefonkonferenzen ab. Für die Außenwelt wurde eine zentrale Telefonhotline und Mailadresse eingerichtet, um unsere Erreichbarkeit zu gewährleisten."

Es dauerte rund ein halbes Jahr, bis alle wesentlichen Bestandteile wieder funktioniert haben

Anschließend widmete sich das Unternehmen dem Wiederaufbau: Über 5.000 PCs bzw. Server an unterschiedlichen Standorten mit unterschiedlichen Sprachen und Betriebssystemen wurden neu aufgesetzt. Ab Ende Oktober 2019 lief auch die Produktion sukzessive wieder an. Stark: „Wir haben bis zu sechs Monate gebraucht, bis alles Wesentliche wieder funktioniert hat. Ich musste als Mitarbeiter beispielsweise drei Monate ohne Daten arbeiten."

Was hat PILZ aus dem Angriff gelernt?

Stark dazu: „Wir haben gelernt, dass die Investition in Security-Software alleine nicht ausreicht und dass Cyber Abwehr, welche heute aktuell ist, in spätestens drei Jahren veraltet und verwundbar ist. Es ist unabdingbar, konstant in die Veränderung bzw. Verbesserung von Security-Konzepten zu investieren."

Insgesamt konnte PILZ wertvolle Erfahrungen sammeln, die das Unternehmen gerne auch externen Unternehmen anbieten möchte, wie Machanek betont.

BMI: Cyberangriffe sind ernst zu nehmen und es gilt sich vorzubereiten

Erfahrungen wie die der Firma PILZ sind dem Leiter der Cyber Security Centers im BMI, Philipp Blauensteiner, bestens bekannt und er appelliert daher: „Cybersicherheit bzw. IT-Sicherheit ist nicht nur ein Thema der IT und Technik, es braucht auch entsprechende Mitarbeiterprozesse und mehr Berücksichtigung im Top-Management. Außerdem ist es wichtig, vorbereitet zu sein, wenn doch ein Cyberangriff passiert. Denn die Angreifer wollen größtmöglichen Schaden anrichten, damit zuverlässig bezahlt wird. "

Die Republik Österreich bereitet sich auf Cyberangriffe im größeren Maßstab vor, setzt Blauensteiner fort. Mehrere Ministerien arbeiten diesbezüglich zusammen: Das Bundeskanzleramt, das Innenministerium (BMI), das Bundesministerium für Landesverteidigung (BMLV) und das Außenministerium. Auch mit privaten Unternehmen gibt es Kooperationen: „Wir haben auf staatlicher Ebene beschlossen, sowohl untereinander als auch mit der Privatwirtschaft zusammenzuarbeiten. Es ist nicht einfach, im öffentlichen Dienst Cyber-Security-Experten zu rekrutieren. Wenn wir uns gegenseitig die Experten abwerben, hat niemand etwas davon." U.a. tausche man sich in wöchentlichen Telefonkonferenzen über aktuelle Cyberfälle aus. Im BMI hat das BVT auch die Aufgabe, die kritische Infrastruktur zu schützen. Dazu stehe man mit den einschlägigen Unternehmen in ständigem Kontakt, übermittelt Lageinformationen und führt nationale und europäische Übungen durch.

COVID-19 wurde und wird von Angreifern ausgenutzt

Auch die COVID-19 Krise hatte Auswirkung auf die Cyberkriminalität und Cybersicherheit. Im Zuge einer überhasteten Home-Office-Implementierung stand die Sicherheit nicht unbedingt im Vordergrund, was Angreifern zusätzliche Möglichkeiten eröffnet hat – auch durch den Einsatz von Privatgeräten im Home Office. Angreifer zielten auch auf Gesundheitseinrichtungen ab, wohl auch, da sie davon ausgingen, dass der Druck zu bezahlen hier besonders groß war. Auch spiegelte sich das Thema COVID-19 bei Phishing-Kampagnen wider, wenn sich Phishing-Mails zum Beispiel als Information des Sozialministeriums zum Thema COVID-Unterstützung tarnen.

Generell tritt die Schadsoftware in Wellen auf: Manche Gruppierungen können in Abstimmung mit internationalen Organisationen zwar einige Zeit lang aufgehalten werden, jedoch folgt wenig später bereits die nächste Variante. Blauensteiner spricht hier von einem „Katz und Maus Spiel."

BMLV: Hochprofessionelle Angreifer und mittlerweile eigener Wirtschaftszweig

Auch das BMLV arbeitet intensiv mit dem BMI zusammen, berichtet Lambert Scharwitzl, Leiter des Militärischen Cyber-Zentrums im BMLV. Scharwitzl appelliert, das Thema ernster zu nehmen: „Es ist hochprofessionell, was uns da gegenübersteht und mittlerweile ein eigener Wirtschaftszweig. Den einfachen Hacker gibt es nicht mehr. Auch das österreichische Bundesheer funktioniert schon lange nicht mehr ohne IT. Daher sind wir permanent im Einsatz, was Cyberverteidigung betrifft." Wichtig sei es, Security-Aspekte von Anfang an mitzudenken. Ein System sollte erst dann in Betrieb gehen, wenn es auch sicher ist. Das gelte auch für Branchen, in denen die IT nicht immer so präsent war, wie z.B. Automechaniker.

AIT: Wir sind verwundbarer, als wir glauben

Helmut Leopold, Head of Center for Digital Safety & Security am AIT Austrian Institute of Technology, kann die bisherigen Ausführungen nur bestätigen und zeigt die Verwundbarkeit unserer Systeme auf: „COVID hat die Vernetzung der Menschen zur Spitze getrieben. Ohne Kommunikationsinfrastruktur funktioniert heute nichts mehr – auch kein Energienetz. Gleichzeitig kann jeder ohne besonderes Fachwissen mit Tools aus dem Internet dasselbe anrichten, was früher nur einzelne Spezialisten konnten. Unsere immer komplexeren Systeme, die die Ingenieure gesamthaft auch immer weniger verstehen und der Innovationsdruck nach schnellen Lösungen tragen auch nicht unbedingt zum Sicherheitsgewinn bei. Gleichzeitig sind Themen wie Safety und Security nach wie vor eher Neuland. So wird das nicht weiterfunktionieren."

Wie leicht jeder von uns betroffen sein kann, illustriert Leopold anhand eines einfachen und leider nach wie vor alltäglichen Beispiels: „Wenn Sie Ihr WLAN-Router Passwort nach Auslieferung nicht ändern, ist das leicht zu finden und über die Webcam schaut dann ein Fremder in Ihr Wohnzimmer."

Schwächen in Systemen sind laut Leopold kaum zu vermeiden, womit kaum jemand nicht angreifbar ist. Und selbst wenn die Lücken entdeckt worden sind, dauere es erfahrungsgemäß ein halbes Jahr, diese zu schließen – manchmal passiert das auch nicht.

Viele mögen sich nun denken, dann stelle ich eben geeignetes Personal ein. Auch dieses ist aber Mangelware, u.a. aufgrund vielfach fehlender Ausbildungsangebote für diesen Beruf, betont Leopold.

Security by Design muss Standard werden

Alles in allem empfiehlt Leopold, gemeinsam laufend Informationen zu Angriffen in Katalogen zu sammeln, Security-by-Design umzusetzen und neue Methoden zur Netzwerk-Überwachung

einzusetzen, um auch nicht bekannte Angriffe zu erkennen. Ein Best Practice Beispiel für Security-by-Design ist laut Leopold die Autoindustrie: „Neue Autos werden in Europa laut Regulierung nur mehr zugelassen, wenn eine entsprechende Validierung der digitalen Sicherheit erfolgt. Von Anfang an wird Sicherheit mitgedacht und werden Standards entwickelt, um Fehler im Design zu vermeiden – so müsste es auch in anderen Branchen sein."

Was können kleinere oder mittlere Unternehmen jetzt tun?

Blauensteiner empfiehlt sich anzusehen, was das Herzstück des Unternehmens bzw. was besonders schützenswert ist. Mit diesem Wissen können entsprechende Berater bzw. Spezialisten dann unterstützen. Sich zu überlegen, welche Maßnahmen ergriffen werden sollten, wenn der Cyberangriff einmal erfolgt ist, wäre auch für kleine Unternehmen sehr empfehlenswert. Für eine Erstunterstützung bietet sich auch die kostenlose Cyber-Security Hotline der Wirtschaftskammer an.

Was macht die EU?

Leopold informiert, dass es mit dem „digital cyber security act" Bestrebungen gibt, Regularien und Gesetze, die derzeit nur für kritische Infrastruktur gelten, künftig auf alle Produkte auszuweiten, mit dem Ziel, dass künftig alle Produkte aus der EU und damit auch aus Österreich gewisse Minimum-Sicherheitsstandards erfüllen – das wäre auch ein Wettbewerbsvorteil.

Wie sicher sind Entwicklungen wie smart metering?

Leopold dazu: „Die erste Reihe der Entwicklungen von smart meter haben das Thema Security nicht wirklich berücksichtigt. Studierende haben entsprechende Lücken innerhalb weniger Tage ohne großen Aufwand herausgefunden. Deshalb gibt es jetzt Standards und Vorgaben, um die nächste Generation sicherer zu bauen. Der ganze Prozess ist etwas überstürzt und unbedacht passiert."

Was sind eigentlich die Motive der Angreifer?

Geld ist eines der wichtigsten Motive, betont Blauensteiner: „Cybercrime ist heute der größte Geschäftszweig der organisierten Kriminalität, sogar vor dem Drogenhandel. Daneben gibt es weitere Motivationen - von Aktivisten, die auch Unternehmen angreifen, die etwas produzieren, was nicht gewünscht wird, bis hin zur Wirtschaftsspionage."

Abschließend noch ein wichtiger Punkt von Machanek: „Man kann die beste Cyber Security aufbauen - wenn man die Mitarbeiter nicht mit ins Boot holt und entsprechend schult, bringt das alles nichts."

16.3.2021, Bernhard Weiner, GSV