05/2018

DIE GEMEINDE

Zeitschrift für die kommunale Selbstverwaltung in Schleswig-Holstein

Schwerpunktthemen: IT, Datenschutz und Informationssicherheit

- *Lukas Gundermann,* Die neue EU-Datenschutz-Grundverordnung – was ändert sich bei der Datenverarbeitung durch Kommunen? Teil 1: Einordnung der DSGVO, Rechtsgrundlagen der Datenverarbeitung
- *Dr. Werner Degenhardt, Andreas Amann, Jan Koppelmann, Frank Weidemann,* SiKoSH besiegt den großen Weißen Hai
- *Nikolaus Stapels,* Angriff auf eine Kommune – Vorgehensweise von Cyber-Kriminellen
- *Oliver Maas,* Integriertes Antrags- und Fallmanagement – kostenlose Online-Lösungen für die Kommunen in Schleswig-Holstein

70. JAHRGANG ISSN 0340-3653 C 3168 E

SHGT Schleswig-Holsteinischer GEMEINDETAG

Deutscher Gemeindeverlag GmbH Kiel

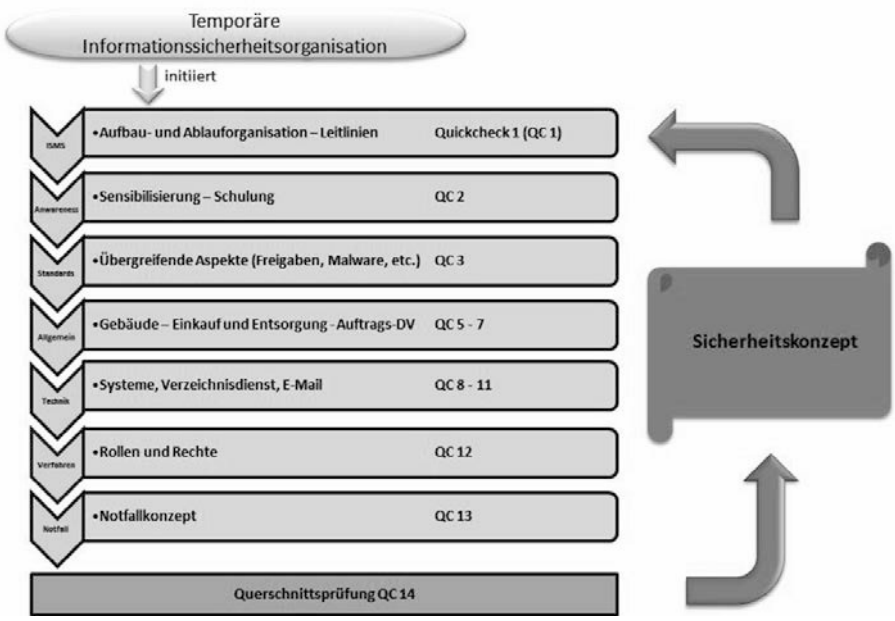

Abbildung 9: Das SiKoSH-Prozessmodell

Jede SiKoSH-Phase wird mit einem sogenannten Quickcheck gestartet. Dieser ermöglicht anhand zahlreicher kontextbezogener Kontrollfragen einen schnellen Überblick über die Sicherheitslage.
Zu jeder Phase werden unterschiedliche Dokumente z. B. in Form von Leitlinien, Konzepten oder Beispielen bereitgestellt, die kommunal angepasst werden können. Für die ‚Phase 1' (Aufbau- und Ablauforganisation ISMS) sind dieses vor allem eine Informationssicherheitsleitlinie und Material zur Bestellung und Regelung des Aufgabenfeldes eines Informationssicherheitsbeauftragten.
Nach Ablauf der ‚Phase 1' und somit Umsetzung der obligatorischen organisatorischen Aufgaben kann der Fokus dann auf eine frei gewählte Phase gelegt werden. SiKoSH empfiehlt, mit der Mitarbeitersensibilisierung zu beginnen.
Neben IT-spezifischen Phasen, die sich z. B. mit Hardware oder mit Verfahren beschäftigen, werden auch allgemeine Aspekte wie z. B. die Gebäudesicherheit betrachtet.
Nach Durchlauf der einzelnen Prozesse stehen mit dem ‚Quickcheck 14' Prüffragen bereit, die den Erfolg der zwischenzeitig umgesetzten SiKoSH-Maßnahmen transparent machen.
Nach Dokumentation der Maßnahmen im Sicherheitskonzept, auch hierfür gibt es eine Unterstützung, beginnt der Iterationsprozess im Sicherheitszyklus wieder von vorne und ermöglicht somit Nachbesserungen und die gezielte Reaktion auf neue Bedrohungen.

Wo finde ich die SiKoSH-Dokumente?
Alle Arbeitsergebnisse sind unter www.sikosh.de abrufbar. Für Rückfragen stehen wir sehr gerne unter sikosh@komfit.de zur Verfügung.

Wie geht es weiter?
Zur Sicherung der Nachhaltigkeit und zur Gewährleistung, dass die Projektergebnisse situationsbezogen überarbeitet und fortgeschrieben werden, ist die Gründung eines schleswig-holsteinischen Forums für kommunale Informationssicherheitsbeauftragte geplant. Die Einladung zu einer konstituierenden Sitzung soll im ersten Halbjahr 2018 erfolgen.

Über die Autoren:

Werner Degenhardt ist Akad. Dir. und CIO i.R. an der LMU München und Spezialist für Human Factors in der Informationssicherheit bei Code and Concept (werner.degenhardt@codeandconcept.de).

Andreas Amann ist Behördlicher Datenschutzbeauftragter der Landeshauptstadt Kiel (andreas.amann@kiel.de).

Jan Koppelmann ist IT-Leiter der Landeshauptstadt Kiel (jan.koppelmann@kiel.de).

Frank Weidemann ist Projektleiter im Kommunalen Forum für Informationstechnik e.V. – KomFIT (frank.weidemann@komfit.de).

Technische Umsetzung der Phishing-Simulation durch Code and Concept (www.codeandconcept.de).

Angriff auf eine Kommune – Vorgehensweise von Cyber-Kriminellen

Aus den dunklen Ecken des Internets greifen sie an: Cyber-Kriminelle

Nikolaus Stapels

Sie wollen spionieren und gehen hochprofessionell und umsichtig dabei vor. Ihr Motiv ist das schnelle Geldverdienen. Der Tatort ist das Internet und die IT der betroffenen Firmen.

1. Das Verschmelzen der alten und der neuen Welt
In der alten Welt sind Kriminelle physisch in Unternehmen und öffentliche Einrichtungen eingedrungen; sie haben Alarmanlagen und Bewegungsmelder ausgeschaltet, um so eindringen zu können.
In der neuen digitalen Welt wandelt sich das Ganze: was früher der Einbruch war, ist heute der Datendiebstahl.
Und auch die Einbrecher werden immer moderner. Wo früher noch sogenannte Gaunerzinken verwendet wurden, gibt es heute Apps und Datenbanken, in denen „interessante" Häuser mit Informationen hinterlegt sind. Ein Blick vom Einbrecher vor Ort in die App und er erhält die gewünschten Informationen, bspw. ob die Eigentümer arbeiten oder ob es Hunde oder Bewegungsmelder gibt. Der klassische Einbrecher digitalisiert sich!
Und auch die Motive des Hackers wandelten sich in den letzten Jahren. Früher waren es vorwiegend allein agierende Hacker, die mit ihren Attacken Berühmtheit und Ansehen erlangen wollten und ihre Spuren nicht gut verwischten. Heutzutage schließen sich immer mehr Hacker kriminellen Organisationen an. Dort herrschen Hierarchien mit strengen Verhaltenskodexen, und nicht jeder kann dort Mitglied werden - häufig sind persönliche Kontakte wichtig. Wird man in diese Kreisen jedoch aufgenommen, verändert sich die Arbeitsweise eines Hackers drastisch.
Hat ein Hacker (oder Cracker) vorher noch zufällig seine Opfer ausgesucht und

nur kurzzeitig versucht, in fremde Systeme einzudringen, um Daten zu entwenden - gemäß dem Motto „so wenig Aufwand wie möglich" – so arbeitet er fortan bei Advanced Persistent Threat (APT)-Angriffen mit. APT bedeutet zu Deutsch „fortschrittliche andauernde Bedrohung", da die Kriminellen häufig eigene Software speziell für den Angriff nutzen. APT´s starten zielgerichtet auf ein Unternehmen. Dabei sind die Täter beharrlich und lassen sich Zeit (andauernd). Bei einem APT spielt es keine Rolle, ob das Ziel in einer Woche oder einem Jahr erreicht wird, wichtig ist nur, dass es erreicht wird. Keine Behörde, Branche oder Unternehmen ist gegen solch eine Attacke zu 100% geschützt. In der Regel sehen es die Cyber-Kriminellen dabei auf Ziele ab, die ihnen einen hohen Profit bringen.

2. Wie gehen Cyber-Kriminelle vor?

2.1 Auswahl eines geeigneten Opfers (Phase I)

Anhand eines Angriffs auf eine öffentliche Einrichtung wird aufgezeigt, wie Cyber-Kriminelle vorgehen:

Eine Kommune in Süddeutschland soll angegriffen werden, es geht darum, Informationen von Bürgern zu erhalten.

Ein Grund, warum öffentliche Einrichtungen gerne angegriffen werden, sind Kundendatensätze. Diese können im Darknet ca. 30€ je Datensatz bringen, wenn folgende Daten gestohlen werden: Name, Adresse, Geburtsdatum, Kommunikations- und Bankdaten.

Der Ablauf des Angriffs lässt sich auch auf ein kleines Unternehmen und eine kleine Kommune anwenden.

Zu unserer Beispielkommune.

Es ist gerade 10:17 Uhr – die meisten Mitarbeiter sind bereits am Arbeitsplatz, checken Emails, führen Telefonate, nehmen Anfragen entgegen… ein ganz normaler Arbeitsalltag. Sie wissen nicht, dass sie soeben nach ausgiebiger Recherche als DAS lukrative Ziel für einen Angriff ausgewählt wurden… der Hacker „L3g!0n" (ausgesprochen Legion) lächelt zufrieden und nickt… er hat sein nächstes Opfer gefunden…

2.2 Auswahl seines Spezialistenteams „Alpha-H4ck3r" (Phase II)

Nachdem das Ziel identifiziert und analysiert wurde, beginnt umgehend Phase II.

„L3g!0n" stellt sich seine Crew aus Spezialisten zusammen, diese lassen sich auf speziellen Webseiten im Darknet finden. Für dieses Ziel werden mehrere Spezialisten benötigt, unter anderem mehrere auf Social Engineering spezialisierte Hacker. Diese sollen durch eine zwischenmenschliche Beeinflussung die Opfer u.a. dazu bewegen, vertrauliche Informationen preiszugeben. Daneben werden spezialisierte Hacker für die IT-Landschaft der anzugreifenden Kommune benötigt.

Da „L3g!0n" sich bereits in einschlägigen Foren im Darknet bewegt, findet er zügig seine ausgewählten Hacker, um dieses Projekt anzugehen. Normalerweise braucht man persönliche Bürgen, um in solche Foren zu gelangen – die braucht er schon lange nicht mehr… er ist bereits bekannt, und die ausgewählten Spezialisten, die bereits mehrere Jobs für ihn erledigt haben, folgen sofort seinem Aufruf. Da er allerdings noch ein paar neue Spezialisten benötigt, checkt er bei den registrierten Hackern die Skill-Levels, welche ihm aussagekräftig zeigen, welche Fähigkeiten der jeweilige Hacker vorweisen kann. Die Skill-Levels steigen nach erfolgreichen Aufträgen und werden in der Agenda aufgelistet. Je mehr und kompliziertere Fälle auf der Agenda auftauchen, desto besser und herausfordernder werden die nächsten Aufträge für einen Hacker… und besser bezahlt, in der Regel mit Bitcoins. Bitcoins, ein dezentrales Zahlungssystem für eine digitale Währung. Der Vorteil für die Hacker ist die Anonymität bei der Zahlung. Es ist mit den richtigen Voraussetzungen nicht mehr möglich, den Sender und Empfänger der Transaktion zu ermitteln. Dies bietet einen besseren Schutz der Anonymität als eine konventionelle Überweisung.

2.3. Das Sammeln von Informationen (Phase III)

Nur kurze Zeit später steht seine Spezialisten-Crew „Alpha-H4ck4r" für dieses Projekt fest. Es beginnt die Phase 3, die Social Engineere machen sich ans Werk. Sie recherchieren über die Kommune alles, was sie über das Opfer im Internet finden können. Hierbei erhalten sie, u. a. über die Webseite, Informationen über die Mitarbeiter. Es werden gezielt die Social Media Plattformen nach Mitarbeitern durchsucht, dabei werden z. B. bei „Xing" mehrere falsche Profile generiert und genutzt, damit der Besuch des Hackers nicht zu sehr auffällt. Durch diese Art der Informationsgewinnung erhalten die Angreifer wertvolle Informationen über die Firma und deren Mitarbeiter.

Es konnten u. a. folgende interessante Informationen über die Firma gesammelt werden:

- mehrere Mitarbeiter sind unzufrieden, haben sich negativ über den Arbeitgeber geäußert und Lebensläufe für Recruiter veröffentlicht;
- eine Mitarbeiterin hat Selfies von sich am Arbeitsplatz gemacht und auf einer Social Media Plattform veröffentlicht - im Hintergrund sind Login Daten auf Zetteln zu lesen;
- es gibt mehrere Firmen, die die Kommune als Referenzkunden hinterlegt haben;
- für mehrere Standorte werden Mitarbeiter gesucht - hier besteht die Möglichkeit eines Praktikums;
- Hobbys und Freizeitgestaltung mehrerer Führungskräfte konnten ermittelt werden;
- Auf Bildern ist erkennbar, dass Mitarbeiter Funkmäuse für Ihre Dienstlaptops nutzen;
- Es gibt mehrere Bilder aus den Firmengebäuden, auf denen sind Kopierer zu sehen mit dem Namen des für die Wartung zuständigen Unternehmens.

Akribisch sammelt „Alpha-H4ck3r" alle Informationen und setzt so in einer Übersicht das Informations-Puzzle zusammen – Informationen über verschiedene Führungskräfte, über den Aufbau von Abteilungen und welche Mitarbeiter diese umfassen. Nachdem die ersten Vorbereitungen abgeschlossen sind, macht sich das Hacker-Team nun Gedanken, welche Angriffsmethode und Vorgehensweise am effektivsten sind.

2.4 Die Auswahl der Angriffsstrategie (Phase IV)

Üblicherweise wird bei solch einem Angriff eine nicht öffentlich bekannte Sicherheitslücke im Betriebssystem oder der genutzten Software ausgenutzt; dies nennt sich Zero-Day-Angriff. Solche Zero-Day-Exploits können im Darknet gekauft werden. Ein Exploit ist ein Programm bzw. ein Programmcode, mit dessen Hilfe sich die Hacker einen Zugang zu Systemen verschaffen; solch ein Exploit kann mit der Brechstange eines Einbrechers verglichen werden. Mit beiden kann der Einbrecher sich Zugang zu fremdem Eigentum verschaffen. Der große Vorteil bei der Nutzung eines Zero-Day-Exploits ist es, dass ein Unternehmen sich nicht gegen etwas schützen kann, das allgemein nicht bekannt ist.

Während „Alpha H4ck3r" noch Informationen über das Unternehmen sammelt, wird der Angriffscode bereits von unserem Hacker „L3g!0n"geschrieben und für verschiedene Formate, wie PDF, Word, Excel etc. vorbereitet.

Phase IV: Es werden nun verschiedene Angriffswege bzw. verschiedene Szenarien durchgespielt, dazu werden u.a. auch die Erkenntnisse der Social Engineere herangezogen.

Folgende Angriff-Szenarien sind u. a. möglich:

- Es wurde herausgefunden, dass einige Führungskräfte E-Zigaretten rauchen; dies war u. a. auf Bildern und den beigetretenen Gruppen auf Social-Media-Plattformen ersichtlich; der Angriff könnte hier über infizierte E-Zigaretten erfolgen, welche über den USB-Port des Dienst-Laptops geladen werden können. Die Zigaretten werden als Geschenk an die Führungskräfte verschickt.

- Die Führungskräfte haben feste Parkplätze, verschiedene „normale“ Mitarbeiter haben sich darüber in sozialen Medien aufgeregt, dass diese nicht von den Mitarbeitern genutzt werden dürfen, auch nicht, wenn die Führungskraft auf Dienstreise/im Urlaub ist. Da bekannt ist, auf welchen Parkplätzen die Führungskräfte parken, kann leicht ein Angriff über ausgelegte USB-Sticks initiiert werden.
  Neben der Fahrertür könnte ein USB-Stick mit der Aufschrift „Mitarbeiter Abbaupläne“, „Gehaltsliste“, „Bonifikationen“ platziert werden.
  Durchschnittlich sieben von zehn neugierigen Mitarbeitern schauen nach, was sich darauf befindet, bevor der Stick in der IT-Abteilung landet.
- Es könnten Werbegeschenke an Abteilungsleiter verschickt werden, diese könnten u. a. Computer-Mäuse oder USB-Sticks mit Wanzen sein, welche sich aktivieren, sobald jemand spricht; das gesprochene Wort wird dann automatisch in Text umgewandelt und gezielt nach bestimmten Wörtern durchsucht.
- Es werden neue Mitarbeiter gesucht, es bestünde die Möglichkeit, vorab ein Praktikum zu absolvieren. Getarnt als Praktikant könnte jemand dann Schadsoftware einschleusen.
- Neben der Möglichkeit, jemanden persönlich einzuschleusen, gibt es auch die Option, eine Bewerbungsmail mit schadhafter Software zu verschicken; das Unternehmen wird dies i.d.R. kennen, dennoch wird diese gleiche Angriffsmethode angewandt, weil immer wieder Mitarbeiter durch fehlende Konzentration, Stress oder Zeitdruck darauf hereinfallen.
- Über das sogenannte „Spear Phishing“ könnten ausgewählte Mitarbeiter durch den Erhalt von auf sie zugeschnittenen Nachrichten angegriffen werden. Das Spezialistenteam hat bspw. herausgefunden, dass einige Mitarbeiter begeisterte Thailand-Urlauber sind, diese würden dann in der nächsten Zeit gezielt Informationen zu Thailand mit Geheimtipps erhalten. Nachdem die Opfer nach einiger Zeit und einigen Mails später Vertrauen gefasst hätten, würde der zweite Schritt folgen – diese könnten, nachdem sie sich mit einem Passwort registriert haben, durch die Eingabe von Informationen eine Thailandreise gewinnen. Das Hacker-Team weiß, dass viele Anwender für mehrere Anmeldungen dasselbe Passwort nutzen und missbraucht diesen Umstand nur zu gerne. Im dritten Schritt sollten die Opfer dann auf einen Link klicken, um Angebote für eine Thailandreise zu erhalten - mit 50% Nachlass. Durch den Besuch der Webseite wird dann der Schadcode im Hintergrund runtergeladen.
- Durch die Nutzung von Funkmäusen, sogenannten „MouseJacks“, könnten PC, Linux oder Mac angegriffen werden; und dieses auch, wenn der Rechner nicht mit dem Internet verbunden ist. Bei dem Angriff würden die Funksignale der Maus manipuliert. Wenn ein Nutzer einen linken Mausklick tätigte, dann übertrüge die Maus ein Funksignal zum Computer „linker Mausklick“. Und genau hier würde der Angriff ansetzen, das Signal würde überlagert und ein Schadcode statt dessen übertragen. Der Computer führt anschließend den Befehl aus. Die dafür notwendigen Werkzeuge kosten ca. 30 €.
- Auf Bildern vom Arbeitsplatz konnte der Dienstleister für die Wartung der Kopierer identifiziert werden, „Bürosysteme S+N“ (Name geändert). Durch die Fälschung von Ausweisen könnten „Techniker“ in die Firma gelangen, um die Festplatten aus den Geräten auszutauschen, welche i.d.R. alles speichern, was jemals kopiert, gedruckt oder gefaxt wurde. Dadurch könnten neue Einblicke in die Firma gewonnen werden.

Dies ist nur eine kleine Auswahl von Angriffsstrategien, welche das Hacker-Team „Alpha-H4ck3r“ in Erwägung zieht und zeigt nur oberflächlich auf, welche Möglichkeiten es gibt, um in eine Firma einzudringen.
Um die Sicherheitsabwehr von Firmen zu überwinden, werden in der Regel mehre Angriffswege parallel durchgeführt. Bei solch einem Angriff ist es nicht wichtig, wie lange der Angriff dauert, einzig die Erreichung des Ziels steht im Vordergrund. Deshalb sind diese zielgerichteten Angriffe so schwer abzuwehren.

2.5 Das Einschleusen des Schadcodes (Phase V)

Um den Erfolg versprechendsten Weg zu finden, zieht unser Hacker „L3g!0n“ nun zwei externe Berater hinzu und diskutiert mit diesen und seinem bereits vorhandenen Team „Alpha-H4ck3r“ die Vielzahl von Möglichkeiten, die sich ihnen eröffnet haben. Nach einigen Stunden wurden alle Vor- und Nachteile der einzelnen Strategien gegeneinander abgewogen und bezüglich der Effektivitätswahrscheinlichkeit analysiert. Ihre Strategie steht nun fest und der Angriff kann beginnen.

Phase V: Es wird versucht, den Schadcode in die Zielumgebung zu liefern.

Die einfachste und effektivste Möglichkeit, um in die Systeme einzudringen, ist das Einbeziehen der Mitarbeiter des Unternehmens. Dabei werden die menschlichen Schwächen - u. a. Neugierde und Stress - ausgenutzt.

Da neues Personal gesucht wird, verschickt „Alpha-H4ack3r“ zunächst die „Bewerbungsmail“ mit einem Link zur Dropbox. Da diese Angriffsmethode vielen Unternehmen heutzutage jedoch bekannt ist, hat dieser Angriff auf den ersten Blick keinen großen Erfolg. Dennoch werden mehrere hochwertige Bewerbungen verschickt, zum einen in der Hoffnung, dass doch ein unachtsamer Mitarbeiter den Anhang öffnet und somit den Schadcode runterlädt, zum anderen sollen diese die Mitarbeiter und die IT-Abteilung konditionieren. So wird kontinuierlich jeden Tag ein schadhaftes Word Dokument verschickt; im Unternehmen wissen nun alle, dass dies sofort gelöscht werden muss.
Die Anzahl der Mails erhöht sich im Laufe der Zeit auf 50 schadhafte Word-Bewerbungen pro Woche. Während sich alle auf die Word-Bewerbungen konzentrieren, kommt eine Bewerbung per PDF. Diese ist erst einmal nicht schädlich, aber wenn der Nutzer auf den Link in der PDF klickt, dann lädt sich auch hier die Schadsoftware herunter und der Rechner ist infiziert.
Die Schadsoftware „versteckt“ sich dann erst einmal im System und wird zu einer bestimmten Uhrzeit, z.B. erst am Samstag um 20 Uhr gestartet, wenn kaum noch ein Mitarbeiter im Unternehmen ist.
Durch einen falschen Klick in solch einer PDF-Bewerbung konnte von „Alpha-H4ck3r“ mehrere verschiedene Remote-Access-Trojaner (RAT) eingeschleust werden, welche Hintertüren öffneten, um Rechner fernsteuern zu können. Damit die vorhandene Antiviren-Software ausgetrickst werden kann, wird der Trojaner mit einer Tarnkappe versehen, dem „Rootkit“, mit deren Hilfe der Trojaner tief im Betriebssystem versteckt wird.
In den ersten sechs Wochen konnten darüber hinaus mehrere Mitarbeiter auf eine Webseite gelockt werden, die Bali-Reisen mit 50% Nachlass verspricht. Diese haben sich dort registrieren müssen, so dass „Alpha-H4ck3r“ mit den gewonnenen Daten unter anderem in die privaten Mailpostfächer eindringen konnte. Und das mit den berechtigten Login-Daten, da einige Mitarbeiter tatsächlich für verschiedene Webseiten dasselbe Passwort genutzt haben.
Da einzelne Mitarbeiter sich berufliche Mails an ihr privates Mailpostfach weitergeleitet hatten, konnten auch so noch weitere interne Informationen über das Unternehmen gesammelt werden. Besonders bemerkenswert – und von unserem Hacker-Team mit belustigtem Kopfschütteln festgestellt – war ein Mitarbeiter, der im „Media Center“ ein Word Dokument mit dem Namen „Passwortliste – Geheim.docx“ hochgeladen hatte.
Somit offenbarten sich Alpha-H4ck3r“ alle seine privaten und beruflichen Passwörter, die jeweiligen Zahlencodes für die

Tiefgarage und verschiedene Bereiche im Unternehmen.
Zu „L3g!0n“s voller Zufriedenheit werden nun bereits seit Tagen über den eingeschleusten Trojaner wertvolle Informationen gesammelt. Diese Daten werden jedoch nicht sofort ausgeschleust, sondern erst einmal zentral im gehackten Unternehmen gesammelt.
Des Weiteren wurde von „L3g!0n“ ein deutscher Hacker beauftragt, sich bei dem Unternehmen zu bewerben und dort ein Praktikum zu beginnen. Das Einschleusen des Hackers mit gefälschten Unterlagen und Social-Media-Profilen war kein Problem. Diesem Mitarbeiter wurden schon während des Praktikums als Entwicklungsinformatiker weitere Zugriffsrechte gewährt, so dass er mit seiner eigenen Anmeldung bereits tiefergehende Informationen zu verschiedenen Projekten sammeln konnte.
Ausgestattet mit mehreren Hardware-Keyloggern - einer Art USB-Stick, der zwischen Tastatur und Computer gesteckt wird und alles speichert, was geschrieben wird - konnten von Mitarbeitern und Hauptabteilungsleitern sämtliche Login-Daten mitgelesen werden. Das Abrufen der Passwörter funktioniert per Funk über ein Tablet, das der deutsche Hacker mit in die Firma gebracht hat.
In der Mittagspause konnte sich dieser Hacker mit den gewonnenen Daten ohne Probleme als Hauptabteilungsleiter einloggen und Daten kopieren. Bei den Hauptabteilungsleitern waren die USB-Ports gegenüber den normalen Arbeitnehmern nicht gesperrt, so konnten Daten auf eine externe Festplatte kopiert werden.
Nach ein paar Tagen brach der Hacker das Praktikum dann plötzlich ab, mit der Begründung, dass er etwas Besseres in seiner Nähe gefunden habe.
Über die Hintertür im System konnte währenddessen das Hacker-Team Daten im System sammeln und für das Ausschleusen vorbereiten. Dazu wurden die Daten in eine Rar-Datei gepackt und verschlüsselt. Am darauffolgenden Wochenende wurden dann die Dateien in kleineren Paketen auf einen Server im Ausland hochgeladen.
Nachdem die Daten erfolgreich über mehrere Server anonymisiert werden konnten, sind diese nun im Hauptquartier angekommen und können von unserem Hacker gesichtet werden. Zufrieden stellt er fest, dass es sich bei den Projekten u. a. um die Integrierung neuer Hardware für verschiedene Bundeswehrstützpunkte im In- und Ausland handelt.

2.6 Das Verwischen von Spuren (Phase VI)

Phase VI: In der vorletzten Phase werden von dem Spezialisten bei „Alpha-H4ck3r Z“ vorhandene Beweise auf dem infizierten System vernichtet. Das Hauptziel ist es, dass alle eventuellen Spuren des Angriffs auf dem System entfernt werden. Dazu wird u. a. Software genutzt, die automatisch Protokolle und Software vom System löscht. Auch manuell wird noch vieles gelöscht und verwischt. Im Anschluss werden dann noch mehrere Hintertüren eingebaut, für den Fall, dass das Team in der Zukunft nochmals in das System eindringen möchte.

2.7 Der Verkauf der Daten (Phase VII)

Phase VII: Unser Hacker „L3g!0n“ verkauft nun die Daten, was sich leichter anhört als es in Wirklichkeit ist. Um in diese speziellen Foren zu gelangen, musste er sich seinerzeit mehreren Interviews mit verschiedenen Mitgliedern stellen. Der Zugang zum gewünschten Forum war kostenpflichtig und kostet für 12 Monate 12.000 $. Dadurch hat aber jedes Mitglied die Möglichkeit, die passenden Ansprechpartner für seine Produkte zu finden. Es werden dort neben Firmengeheimnissen auch Zugänge zu Bankkonten, PayPal, etc, angeboten.
Der Aufbau der Seite ähnelt einer Kleinanzeigen-Seite, es wird ein kostenloses Inserat eingestellt sowie ein sehr geringer Teil der Daten bzw. eine Übersicht der vorhandenen Daten. Aufgrund des Namens vom gehackten Unternehmen haben sich sehr schnell interessierte Käufer gemeldet; vorwiegend aus Russland und China. Zur besseren Qualitätssicherung wurde den interessierten Käufern ein Einblick in die Daten gewährt; dies geschieht durch eine Remote-Verbindung, so dass keine Daten übertragen werden, sondern der Käufer sich die Daten lediglich ansehen konnte wie bei einer TeamViewer-Sitzung. Nachdem die Daten gesichtet wurden, können nun Gebote abgegeben werden….
Die Verhandlungen dauerten insgesamt eine Woche und die Daten konnten letztendlich für 3,4 Mio. $ verkauft werden.
Das Team hat ungefähr 150 Tage in das Projekt investiert. Insgesamt 10 engagierte Hacker waren im Kern-Team von „Alpha-H4ck3r“ tätig und haben in der Zeit zusammen 750.000 $ zuzüglich einer Bonifikation von 10% des Erlöses verdient; jeder Hacker hat somit insgesamt 109.000 $ verdient.
Für externe Berater und den eingeschleusten Hacker wurden 20.000 $ bezahlt
Der Verdienst von „L3g!0n“ beläuft sich somit auf 2.290.000 $ in „nur“ 150 Tagen.
„L3g!0n“ arbeitet mit seinem Team bereits am nächsten Projekt – voraussichtlicher Erlös zwischen 6,5 und 8,25 Mio. $.

3. Fazit

Daten sind der Rohstoff des 21. Jahrhunderts. Im Untergrund blüht der Handel mit hochsensiblen Daten und Schadsoftware; dabei wird der Einstieg für Kriminelle immer einfacher. Durch verschiedene Foren im Darknet können Cyber-Kriminelle mit relativ wenig Aufwand viel Geld verdienen.
Wenn man von „Hackerangriffen“ und „Cybercrime“ hört, dann denken viele sofort an den typischen „Nerd“, der im Keller sitzt und das Tageslicht scheut.
Um als Täter aktiv mitmachen zu können, bedarf es weder tiefergehenden Wissens noch Programmierkenntnisse. Jeder kann theoretisch innerhalb von 72 Stunden eine kriminelle Laufbahn starten. Die nötigen Tools und Anleitungen finden sich schnell in Foren und auf „Youtube“.
Darüber hinaus ist die Größe einer Kommune kein Indiz dafür, ob diese für einen Hacker interessant ist. Vor allem kleine sind bei Hackern sehr beliebt, da es dort – so wird vermutet – weniger IT-Sicherheit gibt und viele ungeschützte „vermeintlich nicht wertvolle“ Daten.
Um sich dagegen zu schützen, müssen u.a. die Mitarbeiter sensibilisiert werden, denn sie müssen wissen, wie Cyberkriminelle vorgehen und was dies für den Arbeitgeber bedeuten kann.
Des Weiteren sollten Kommunen die Absicherung der Restrisiken durch Versicherungen berücksichtigen, diese können keinen Cyberangriff verhindern, jedoch die finanziellen Folgen abfedern. Hier lohnt es sich, mit einem Versicherer über mögliche Konzepte zu sprechen.

Über den Autor:

Nikolaus Stapels, geboren 1979, ist selbständiger VdS-Fachberater für Cyber-Security, zertifizierter IT-Risk-Manager sowie Information-Security-Officer gemäß ISO 21001 und BSI Grundschutz. Seit vielen Jahren konzentriert er sich auf das Thema IT-Sicherheit in Klein- und mittelständischen Unternehmen und Kommunen.
Er unterstützt und berät Unternehmen und Kommunen deutschlandweit bei der Entwicklung und Umsetzung einer Cyber-Security-Strategie; dazu zählt u. a. die Absicherung der Cyber-Risiken und die Sensibilisierung von Mitarbeitern. In zahlreichen Vorträgen zeigt er diesen auf, u. a. mithilfe von Live-Hacking, welche Gefahren im Internet lauern.