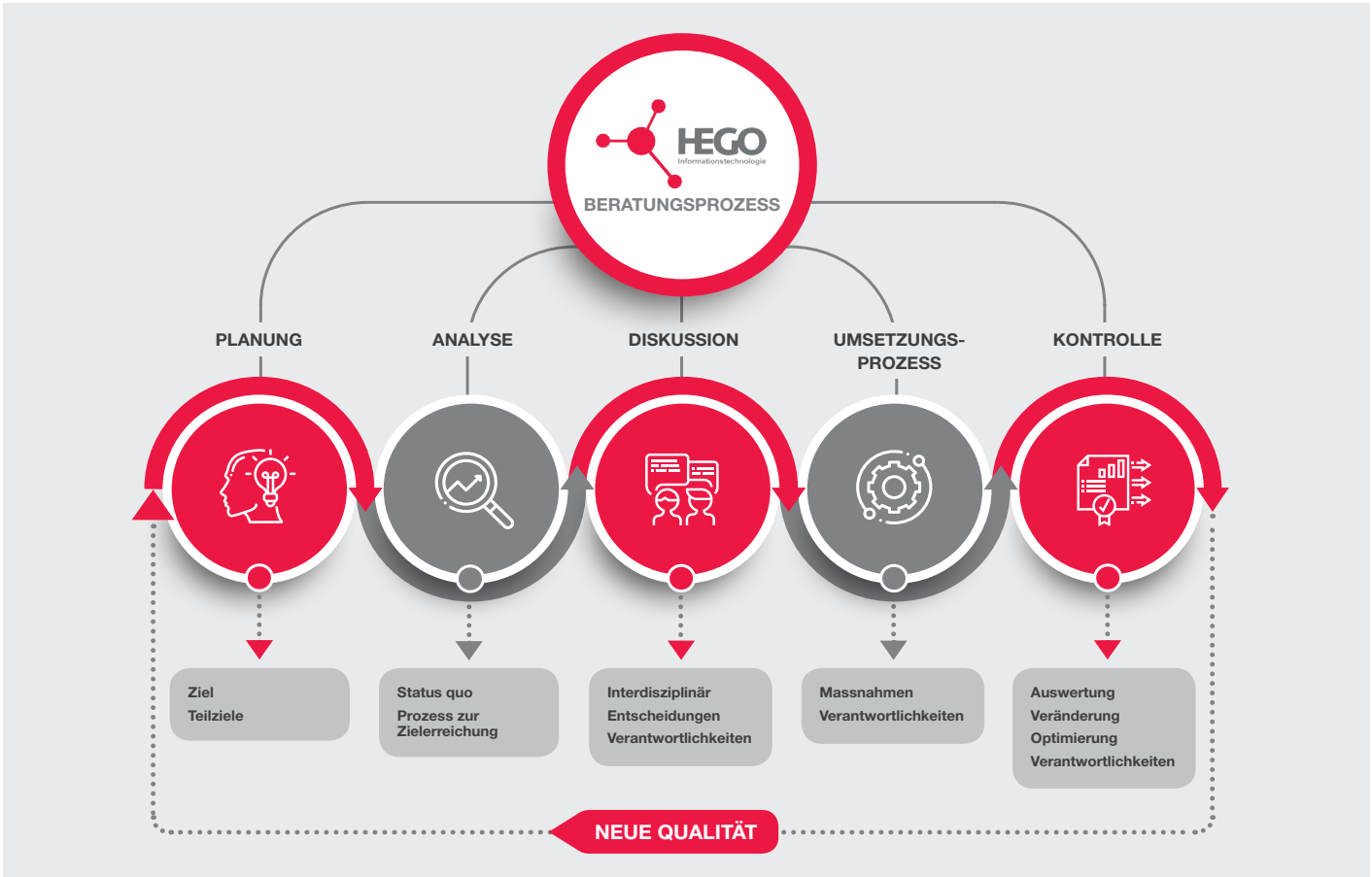
Cyber-Sicherheit
Wir tun alles für Ihren Schutz

Zu Beginn der Corona-Krise mussten viele Unternehmen sehr schnell agieren und mehr Budget als geplant in digitale Lösungen umschichten – nicht zuletzt, um arbeitsfähig zu bleiben. Mit Blick auf die notwendige IT-Transformation ist dies auch gut gelungen. Dem Aspekt der Cyber-Sicherheit wurde dabei jedoch in vielen Fällen zu wenig Aufmerksamkeit gewidmet, obwohl nahezu täglich über Cyberangriffe und Datendiebstahl sowohl in der Fach- als auch der Tagespresse berichtet wurde beziehungsweise wird und Malware wie etwa Ransomware längst zum IT-Alltag gehört. Obwohl die Menge der Daten, die aufgrund der Digitalisierung entsteht, stetig wächst und diese zu einem großen Teil über – teilweise ungesicherte – Router vom Heimarbeitsplatz ins Unternehmen übersendet werden.

Doch dies hat Folgen, wie verschiedene Studien belegen: Zum Beispiel erlitten in den vergangenen Jahren die von Cyber-Angriffen betroffenen Unternehmen dadurch teilweise sehr schwere oder sogar existenzbedrohende Schäden – und hier vorwiegend kleine und mittelständische Unternehmen aber auch kommunale Einrichtungen. Dies sind durchweg leichte Opfer, da es ihnen oftmals an Ressourcen mangelt und sie nicht die finanziellen Mittel aufbringen können, um – wie vom BSI empfohlen – 20 Prozent ihres IT-Budgets in Cyber-Sicherheit zu investieren. Von daher rücken diese Unternehmen und Einrichtungen zunehmend in das Visier von Cyberkriminellen – denn mittlerweile geht es diesen weniger um Industriespionage, sondern vielmehr Erpressung.



Unser Beratungsansatz – 5 Schritte für Ihre Cyber-Sicherheit

Insbesondere mittelständische Unternehmen stehen vor dem Problem, dass ihre IT-Infrastruktur organisch gewachsen ist, weil diese zumeist parallel mit Wachstum des Unternehmens stetig erweitert wurde. Folglich existiert häufig keine strategisch geplante Struktur. Dies ist ein wesentlicher Aspekt, den es bei der Planung eines Sicherheitskonzepts zu beachten gilt.

Generell müssen Unternehmen sich von der Vorstellung verabschieden, Informationssicherheit als fertige technische Komplett-Lösung einkaufen zu können. Stattdessen heißt es, den grundlegenden Bedarf an Absicherung aller unternehmenskritischen Geschäftsprozesse, Anwendungen und IT-Systeme zu ermitteln, um basierend darauf die notwendigen Schutzmaßnahmen angemessen abzuleiten.

Denn ein ganzheitliches Konzept zur Informationssicherheit beinhaltet zahlreiche Aspekte. Hierbei müssen sämtliche relevanten Maßnahmen zur Erreichung eines adäquaten Schutzlevel bedacht und umgesetzt werden: also alle wirksamen Präventions- und Reaktionssicherheitsmaßnahmen zur Abwehr von Ausspähungen, gegen den Abfluss von Know-how, Datenmanipulationen und Sabotage. Des Weiteren ist es auch unerlässlich, organisatorische und personelle Maßnahmen einzuplanen: dazu gehört die Definition zum Umgang mit sensiblen Daten ebenso wie die spezifische Richtlinie zur sicheren Nutzung der mobilen Endgeräte.

1. Planung: Zu Beginn des Prozesses ist für Unternehmen relevant zu wissen, wo sie beginnen sollen, um ihr Sicherheitsniveau – gemäß den bestehenden Risiken – zu erhöhen. Aus diesem Grund ist der wichtigste Schritt im Rahmen unserer Beratung, Ziele mit den entsprechenden Teilzielen – auch unter Berücksichtigung der Wirtschaftlichkeit – zu definieren. Im Mittelpunkt steht dabei, die spezifischen Sicherheitsanforderungen des Unternehmens sowohl zu identifizieren als auch zu klassifizieren.

2. Analyse & Aufnahme des Status Quo: Dieser Schritt dient dazu, die Vorgehensweise für die Teilziele zu definieren. Das bedeutet, hier findet unter Einsatz aktueller Analysemethoden eine Überprüfung der IT-Infrastruktur statt, um Schwachstellen aufzudecken und den Bedarf im Hinblick auf das Schutzniveau zu eruieren. So lässt sich ein jeweils adäquates Schutzlevel erreichen.

3. Diskussion & Entscheidung: Zur Entscheidungsvorbereitung werden die Analyseergebnisse aufbereitet, dokumentiert und vorgestellt. Auf dieser Basis wird dann im nächsten Schritt – unter Berücksichtigung der wirtschaftlichen Kosten-/Nutzenaspekte – ein individuelles Sicherheitskonzept erstellt.

4. Umsetzungsprozess: Entsprechend dem verabschiedeten Cyber-Sicherheitskonzept erfolgt die Realisierung der erforderlichen Einzelmaßnahmen. Die Zuordnung der Verantwortlichkeiten umfasst auch die organisatorischen Maßnahmen, wie etwa die Definition zum Umgang mit sensiblen unternehmenskritischen Daten.

5. Kontrolle: Im Rahmen der Auswertung aller umgesetzten Maßnahmen findet eine Revision dahingehend statt, ob – und falls ja, wo – noch Optimierungsbedarf besteht.

Cyber-Sicherheit ist nicht statisch. Nur mittels eines fortlaufenden Prozesses lässt sich gewährleisten, dass der Schutzlevel der aktuellen Gefährdungslage entspricht.

Was Sie über Cyber-Sicherheit wissen sollten

Ein elementarer Baustein für die erfolgreiche Digitalisierung in Unternehmen ist der Schutz von Geschäftsprozessen, Anwendungen und IT-Systemen.

Voraussetzung für die Auswahl geeigneter Cyber-Sicherheitsmaßnahmen zum Absichern von Unternehmensressourcen ist das Wissen über gängige Herausforderungen und Angriffsvektoren im Cyber-Raum.

Herausforderungen, die für Ihr Unternehmen relevant sein können

Softwarequalität
Aufgabenstellung: Software ist niemals fehlerfrei – selbst bei sorgfältigster Programmierung treten im Mittel zwei Fehler pro 1.000 Zeilen Code auf. Einige Fehler werden im Laufe der Zeit behoben, aber zum Ende der Nutzungsdauer steigt die Fehlerkurve wieder an. Das führt letztendlich dazu, dass die Software veraltet. Dies birgt ein hohes Gefährdungspotential für die Unternehmen, denn vorwiegend über nicht einwandfreie Programme und Betriebssysteme mit Schwachstellen – dies

gilt insbesondere für die gängigen Produkte – wird oftmals Schadsoftware in die IT Systeme und Netzwerke der Unternehmen eingeschleust.

Lösung: Hier hilft nur, in Ihrem Unternehmen ein stringentes Update-Management einzurichten.

Patch-Management
Aufgabenstellung: Es gibt keine Garantie dafür, dass Hersteller ihre Geräte und Komponenten tatsächlich in einer fehlerfreien Software-Version ausliefern. Von daher ist es notwendig, alle Systeme mittels Updates immer auf dem neuesten Stand zu halten, um Schwachstellen für Angriffe zu schließen.

Lösung: Auch wenn dies einerseits Aufwand erfordert und andererseits daraus weder erkennbar eine Leistungssteigerung noch ein Effizienzgewinn resultiert, sollte unter sicherheitstechnischen Aspekten Ihr Patch-Management zentral kontrolliert erfolgen.

Schadprogramme
Aufgabenstellung: Angreifer setzen Schadsoftware wie Spyware, Keylogger oder Ransomware ein, um Daten auszuspähen, Zugangsdaten abzugreifen oder Erpressungen durchzuführen. Hierfür werden vorhandene Schwachstellen in den IT Systemen ausgenutzt. Social Engineering, also die Beeinflussung von Mitarbeitern, wird dabei eingesetzt, um die Effizienz der Angriffe zu erhöhen.

Das Einschleusen der Malware beziehungsweise der speziellen Schadfunktionen einer Malware – ein Hauptziel sind hierbei IT-Endgeräte – geschieht über E-Mail-Anhänge oder infiltrierte Webseiten mithilfe von so genannten Drive-by-Downloads.
Lösung: Ihre IT-Systeme müssen vor Angreifern geschützt werden. Hierzu gilt es einen gewissen Grundschutz vor Schadsoftware herzustellen, der individuell auf den Bedarf Ihres Unternehmens abgestimmt ist.

Ihre Mitarbeiter im Fokus
Aufgabenstellung: Mitarbeiter stellen ein beliebtes Angriffsziel dar, da sie mittels spezieller Praktiken, etwa Social Engineering und/oder Phishing dazu gebracht werden können, infiltrierte E-Mail-Anhänge zu öffnen oder Passwörter am Telefon preiszugeben. Eine weitere Möglichkeit, Identitätsdaten zu erlangen, besteht im Einsatz spezieller Schadprogramme, die unter anderem über manipulierte Webseiten heruntergeladen werden.

Lösung: Dieses Gefährdungspotential lässt sich durch Awareness-Schulungen minimieren, indem den Mitarbeitern das notwendige Wissen über bestehende Gefahren bezüglich der Nutzung von IT-Systemen und dem Umgang mit Daten vermittelt wird. Darüber hinaus kann mit darauf spezialisierten Programmen das Nachladen von Schadcode kontrolliert werden.

Angriffsvektoren, die Ihr Unternehmen betreffen können

Es gibt nichts zu beschönigen, die Zahl krimineller Angriffe auf Unternehmen steigt kontinuierlich und ebenso die Schadenssummen, die durch die Cyber-Attacken verursacht werden. Letztere sogar sprunghaft: im vergangenen Jahr konnte hierbei ein Rekordwert von 223 Milliarden Euro verzeichnet werden. Problematisch mittlerweile auch, dass es nicht nur alle Branchen trifft, sondern dass vor allem in zunehmendem Maße der Mittelstand im Fokus der Angreifer steht.

Genutzt werden hierfür Angriffsvektoren, um Unternehmen auf unterschiedliche Art und Weise zu schaden – von Erpressungen über Sabotage bis hin zur Wirtschaftsspionage. Nachfolgend die wichtigsten Angriffsvektoren im Überblick.

APT (Advanced Persistent Threat)
Unter APT wird grundsätzlich ein gezielter Angriff mit komplexen Angriffstechnologien verstanden. Um ihr Ziel zu erreichen, setzen die Cyberkriminellen dabei unter anderem Malware ein. Stuxnet ist wahrscheinlich vielen noch im Gedächtnis haften geblieben – eine Schadprogramm, das vor ungefähr zehn Jahren zum ersten Mal in Erscheinung trat und primär darauf ausgerichtet war, ganze Produktionsanlagen zu manipulieren. Stuxnet hat heute natürlich keine besondere Relevanz mehr – doch für die Sicherheitsexperten damals war, neben der erstmalig langen Zeitspanne, in der diese Malware unentdeckt im System verbleiben konnte, auch die extrem hohe Durchschlagskraft beunruhigend. Dies ist tatsächlich ein prägnantes Attribut von einem APT-Angriff: der enorme Schaden, der sich damit verursachen lässt. Ein APT-Angriff erfordert einen – auch qualitativ – sehr hohen Programmieraufwand (Advanced) und ebenso viel Manpower, vor allem damit es möglich ist, über einen längeren Zeitraum (Persistent) unentdeckt den geplanten Angriff (Threat) durchführen zu können. Daraus lässt sich schließen, dass Cyberkriminelle sehr versiert im Umgang mit fortschritt-

lichen Technologien sind und die entsprechenden Organisationen im Prinzip hochprofessionell wie ein Unternehmen agieren müssen, da verschiedene Aufgabenbereiche abzudecken sind. Diese sind zum einen das Programmieren und Implementieren der Malware-Elemente – zum anderen der Aufbau der notwendigen IT-Infrastruktur sowie eine sorgfältige Organisation und Überwachung des Angriffs.

Konkret verschaffen sich die Cyberkriminellen dann zum Beispiel mittels infiltrierter E-Mail Anhänge einen Zugang in das Unternehmen. Im nächsten Schritt werden individualisierte Malware-Elemente implementiert, um den Zugang zu etablieren. Aufgrund dessen können sich die Angreifer in dem kompromittierten IT-System frei bewegen und gleichzeitig auch ihre Spuren verwischen. Das nächste Ziel ist, mit aktualisierten Angriffsmethoden die Administrationsrechte zu erweitern, um so Kontrolle über zusätzliche IT-Systeme zu erhalten und lateral in die Netzwerke vordringen zu können. Dies ermöglicht den Angreifern sowohl in den Besitz von sensiblen Informationen und Daten zu gelangen als auch Wissen über vorhandene Schwachstellen oder Funktionen zu sammeln.
Die Dauer des Angriffs spielt aufgrund mehrerer Gründe eine entscheidende Rolle.

Auf der einen Seite beansprucht die Strategieentwicklung für bestimmte Angriffe eine längere Planungszeit. Teilweise kann deren Durchführung erst erfolgen, wenn genügend Informationen – zum Beispiel über Schwachstellen – zusammengetragen worden sind. Oder ganz pragmatisch betrachtet – mit detaillierten Kenntnissen über die unternehmenskritischen Daten ist es eher möglich, eine effiziente Ransomware-Attacke in einer Supply-Chain umzusetzen, die den größtmöglichen Schaden verursacht und so das Unternehmen sowie deren Kunden zur schnellen Zahlung eines hohen Lösegeldes motiviert. Auf der anderen Seite könnte auch Wirtschaftsspionage ein Beweggrund sein – also über einen längeren Zeitraum relevante Informationen abzugreifen, zum Beispiel aus dem Bereich ‚Forschung und Entwicklung'.

Empfehlung: Das A und O ist ein ganzheitliches Konzept zur Informationssicherheit, in dem alle relevanten Sicherheitsmaßnahmen zur Erreichung eines adäquaten Schutzniveaus verbindlich festgelegt sind. In Bezug auf APT sollten zum Beispiel Maßnahmen wie eine regelmäßige Schwachstellen-Analyse oder ein definiertes Patch-Management verpflichtend geregelt sein.

DDoS (Distributed Denial of Service)
Für einen DDoS-Angriff wird ein IT-System ganz gezielt überflutet, wodurch es zu einer Überlastung kommt. Im Prinzip können mit einem DDoS-Angriff zwei Ziele verfolgt werden: Erpressung oder Sabotage. Die Strategie ist jeweils absolut identisch. Für diesen Angriff wird ein IT-System – etwa ein Webserver – ganz gezielt mit einer großen Anzahl von dedizierten Anfragen überflutet, wodurch die verfügbaren Ressourcen – wie Bandbreite oder CPU – komplett ausgereizt werden, was zur Lahmlegung des attackierten IT-Systems führt. Erfolgreich realisieren lässt sich dies in der Regel unter Einsatz von Botnetzen, deren Bots die Schadfunktion „DDoS" aktiviert haben, sowie weiteren Verstärkungsmechanismen. Dadurch ist es letztendlich möglich, zum Beispiel ganz gezielt bestimmte IT-Dienste außer Betrieb zu setzen.

Doch auch wenn die Vorgehensweise immer gleich ist, können die Motive der Cyberkriminellen sehr unterschiedlich sein: Denkbar ist, dass auf diesem Wege ein IT-Dienst – etwa das Buchungssystem für ein Konzert oder Fußballspiel – für eine definierte Zeit zum Stillstand gebracht werden soll, um so den Kartenverkauf zu verhindern, oder eben ganz allgemein einen Konkurrenten zu schädigen. Aber ebenso ist es möglich, dass der Angriff beziehungsweise eine entsprechende Androhung mit der Absicht erfolgt, ein Unternehmen zu erpressen – also um eine bestimmte Summe verlangen zu können, damit der DDoS-Angriff gestoppt oder gar nicht erst durchgeführt wird.

Empfehlung: Es besteht die Gefahr, dass die Art der Angriffe zunehmen werden – allein aufgrund der stetig steigenden Anzahl von IoT-Geräten. Denn diese können sehr gut für DDoS-Attacken ausgenutzt werden, da sie meistens nur unzureichend geschützt sind. Von daher ist es für die Cyberkriminellen das reinste Kinderspiel diverse Endgeräte wie Überwachungskameras oder Smartwatches mit Malware zu infizieren und diese dann für ihre DDoS-Angriffe einzusetzen. Das mögliche Ausmaß des Bedrohungspotentials zeigte sich bereits 2020 durch einen DDoS-Angriff von 2,3 Terabit pro Sekunde (TBit/s) auf Amazon, unter anderem mittels IoT-Botnetzen.

Aus diesem Grund müssen sich Unternehmen darauf mit On-Site-Robustheitsmaßnahmen oder Off-Site-Dienstleistungsmodellen vorbereiten, um nicht auf diese Weise erpressbar zu sein.

Kompromittierung von Webseiten
Die Kompromittierung einer Webseite wird mittels eines gezielten Hacking-Angriffs durch Platzierung von Schadsoftware unter Nutzung einer vorhandenen Schwachstelle auf dem Webserver umgesetzt. Dabei spielt es den Cyber-Kriminellen in die Hände, dass manche Unternehmen ihre Internetauftritte oft über mehrere Monate nicht aktualisieren, da dementsprechend auch die aktuellen Sicherheits-Updates nicht installiert sind. Über die bekannten Schwachstellen der überwiegend genutzten Weblog-Software ist es für Angreifer somit ein Leichtes in das Backend einer Webseite einzudringen, um dann beispielsweise Links einzufügen, die zu einer geclonten Phishing-Webseite führen, oder eine Schadsoftware zu implementieren, mit der Besucher der Webseite infiziert werden können. Hier finden Cyber-Kriminelle immer neue Möglichkeiten, um ihre Ziele zu erreichen – so werden aktuell CAPTCHAs mit Malware infiziert.

Die kompromittierten Webseiten werden von den Cyber-Kriminellen im Weiteren genutzt. Zum einen, um Informationen wie Zugangsdaten von Nutzern abzugreifen – zum anderen, um Schadsoftware auf deren Endgeräte zu schleusen, indem beim Zugriff auf die manipulierten Webseiten beim Drive-by-Download Sicherheitslücken von Browsern oder dem Betriebssystem des IT-Systems des Anwenders ausgenutzt werden.

Empfehlung: Der Angriffsvektor „Kompromittierung von Webseiten" ist für Unternehmen aus zwei Gründen relevant. Zum einen müssen alle Maßnahmen – wie beispielsweise das Einspielen von Updates – ergriffen werden, um die eigene Unternehmensseite entsprechend gegen Angriffe abzusichern.

Zum anderen zeigt es, dass Angreifer nicht ausschließlich auf Phishing-E-Mails setzen, um Mitarbeiter dazu zu verleiten, auf kompromittierte Webseiten zu gehen. Von daher ist es essenziell, im Rahmen von Awareness-Schulungen die Mitarbeiter kontinuierlich über aktuelle Angriffsvektoren aufzuklären, um ein angemessenes Schutzniveau aufrechterhalten zu können.

Phishing
Als Phishing wird die entsprechende Technologie bezeichnet, die zur Ausführung eines Social Engineering-Angriffs Anwendung findet. Um das Ziel Identitätsdiebstahl – also relevante Daten eines Nutzers abgreifen zu können – zu erreichen, wird beim klassischen Phishing wahllos eine große Anzahl an E-Mails versendet. Die Angreifer spekulieren dabei darauf, dass die Empfänger entweder aus Naivität oder im guten Glauben auf einen schädlichen Link klicken und vertrauliche Informationen preisgeben. Hierfür erstellen die Angreifer eine präparierte Webseite, die einer realen aufgrund des imitierten Corporate Design – beispielsweise das einer Bank – täuschend ähnlich sieht, und von daher den Nutzer dazu verleitet, Daten wie etwa Nutzername und Passwort preiszugeben.

• **Spear-Phishing**
Beim Spear-Phishing ist der Empfänger sorgfältig ausgewählt worden. Dem Angriff voran geht eine sorgfältige Recherche – das Internet eröffnet hier ein breites Spektrum nicht nur für die Suche nach Kontaktdaten, sondern auch bezüglich weiterer Hinweise zur Person. Da der Angreifer vorab genügend Informationen über den Empfänger gesammelt hat, ist es möglich, die E-Mail mit exakter Anrede und persönlich zugeschnitten zu formulieren. Aufgrund dessen wirkt diese nicht nur glaubwürdig, sondern auch vertrauenserweckend.

Dadurch erhöht sich die Wahrscheinlichkeit, dass der Empfänger den Anweisungen in der E-Mail folgt und zum Beispiel ein Attachment öffnet, in dem ein Schadcode enthalten ist, der dem Angreifer einen Zugriff auf den Computer, hier unter anderem auf vertrauliche Daten, ermöglicht.

• **Whaling**
Whaling basiert auf der Methode des Spear-Phishings. Jedoch handelt es sich hierbei um einen Angriff, der – in Analogie zu dem „großen Fisch" – gezielt auf Führungskräfte ausgerichtet ist.

Social Engineering
Social Engineering ist die professionelle Beeinflussung oder Täuschung der Mitarbeiter und basiert darauf, dass Menschen manipulierbar sind. Zur Anwendung der Methode muss ein Angreifer lediglich Schwächen, Vorlieben oder sonstige Knackpunkte des von ihm anvisierten Mitarbeiter in Erfahrung bringen – dies gelingt zum Beispiel über soziale Netzwerke. Um diese Methode für kriminelle Absichten zu instrumentalisieren, setzt der Angreifer die erworbenen Kenntnisse entsprechend ein – zum beispielsweise bei einer Person mit Autoritätshörigkeit kann er als Helpdesk-Mitarbeiter sehr bestimmend auftreten und dann mittels Aufbaus von Druck erreichen, dass ihm (innerhalb kürzester Zeit) Passwörter preisgegeben werden.
Aber auch durch das Verwenden bekannter E-Mail-Adressen von Kollegen oder aus dem Be-

kanntenkreis des anvisierten Opfers wird dieses geschickt dazu verleitet, eine Handlung auszuführen. Also entweder auf den Anhang einer E-Mail zu klicken oder auf einen Link in der E-Mail, der auf eine Webseite weiterleitet, die natürlich infiltriert ist. Die Absicht dahinter ist in beiden Fällen, dadurch einen Prozess zu starten, der das Installieren einer Schadsoftware ermöglicht.

Empfehlung: Dieses Gefährdungspotential lässt sich durch Awareness-Schulungen minimieren.

Supply Chain-Angriffe
Supply Chain-Angriffe zielen auf mittelständische Unternehmen ab – im Wesentlichen aus zwei Gründen: Zum einen sind große Unternehmen weitaus besser geschützt als diese, da letztere (immer noch zu oft) davon ausgehen, dass sie per se kein lohnendes Ziel für Angreifer darstellen. Zum anderen eröffnet sich dadurch, dass ein Dienstleister kompromittiert wird, der Zugang zu unzähligen mittelständischen Unternehmen. Supply-Chain-Angriffe basieren meist darauf, dass ein Dienst oder Programm, das im Unternehmen seit längerem im Einsatz ist, durch einen illegalen Zugriff schädlich wird. Um diesen Angriff durchführen zu können, dringt der Angreifer zuerst in das IT-System des Dienstleisters (Supplier) – etwa ein vertrauenswürdiges Unternehmen für Rechnungssoftware – ein und infiltriert zum Beispiel das aktuelle Software-Update mit Malware. Bleibt dieser Vorgang unentdeckt, wird der Angriff durchgeführt – von daher ist es aus Sicht des Angreifers notwendig, dass die Umsetzung an einer bestimmten Prozessstelle erfolgt. Nur so lässt sich sicherstellen, dass das manipulierte Software-Update offiziell als Hersteller-Update digital signiert und somit als autorisierter Code vom Kunden akzeptiert und eingespielt wird.

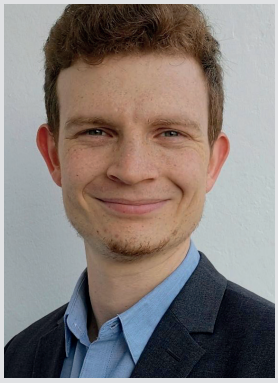
Empfehlung: Installation und Betrieb sollten nur mit den minimal notwendigen Berechtigungen erfolgen können. Zudem ist eine regelmäßige Kontrolle sowohl des Betriebs als auch des Verhaltens der Software ratsam, ebenso wie ein regelmäßiges und zeitnahes Einspielen der Updates. Administrative Berechtigungen sollten in Funktionsgruppen gesplittet werden, so dass der Wirkungskreis von Schadcode bei Verwendung eines administrativen Zugangs eingegrenzt ist.

Generell ist zu empfehlen, dass sich Unternehmen kontinuierlich mit Angriffsvektoren im Allgemeinen und bekannten Sicherheitslücken oder „Backdoors“ zu den eingesetzten Programmen im Speziellen auseinandersetzen.

Ihre Ansprechpartner

Ralf Gogolin
Geschäftsführer

Jörg Hermanns
Geschäftsführer



Patrizio Ziino
Prokurist

Kontakt
HEGO Informationstechnologie GmbH
Telegrafenstrasse 8
D-42929 Wermelskirchen

Telefon +49 (0) 21 96 8 82 97-0
Telefax +49 (0) 21 96 8 82 97-23
info@hego-it.com