Cyber-Kriminalität und Hacker-Attacken werden immer gefährlicher

Sicherheit schafft Vertrauen

Das Wort «Sicherheit» kommt vom lateinischen «securitas» und bedeutet ohne Sorgen oder gefahrenfrei. Gerne erinnert man sich an die 80/90er Jahre, während denen die Berufsbezeichnungen IT-Security Officer, Chief Information (Security-)Officer oder Fremdwörter wie «Ransomware», Phishing, Drive-by Infektionen gänzlich unbekannt waren und man relativ «sorgenfrei», was Viren- und Schadsoftware betraf, in der IT arbeiten konnte. Die damals bezeichnete «EDV» kam mit wenig Schutz (wenige oder keine Passwörter, ohne Antivirus-Programm, ohne Sperrbildschirm usw.) aus.

Heutzutage, 30 Jahre später, befinden wir uns inmitten der «digitalen Transformation», wo die enorme Geschwindigkeit und Optimierung von Arbeitsprozessen eine grosse Herausforderung für Mensch, Technik und Sicherheit darstellen.

Wer schnell fahren will, braucht Sicherheit

Technische Innovationen müssen schnell entwickelt und vermarket werden, trotzdem soll die Sicherheit und Benutzerfreundlichkeit der Produkte nicht eingeschränkt werden. Die Elemente Sicherheit, Benutzerfreundlichkeit und Wirtschaftlichkeit stehen in Konkurrenz. Mehr Sicherheit verlangt mehr Investitionen und schränkt die Benutzerfreundlichkeit ein und umgekehrt.

Das «gesunde» Mittelmass zu finden, hängt einerseits vom «Risikoappetit» des Managements ab, aber auch von den personellen und finanziellen Ressourcen eines Spitals, Heims oder einer Arztpraxis. Trotzdem sollte man für eine Entscheidungsfindung, wieviel Sicherheit notwendig ist, sehr sorgfältig gewichten und an die (Risiko-)Verhältnisse des Unternehmens anpassen. Soviel Freiheit wie möglich – soviel Sicherheit wie nötig. Bei der digitalen Transformation scheint sich die Tendenz zu entwickeln, dass der Vorwärtsdrang von Innovationen stärker ist als die Adaption der Sicherheit an die neuen Verhältnisse. Nebst Sicherheit und Bedienbarkeit der neuen Technologien kommen grosse Herausforderungen im Bereich Change Management auf uns zu. Schliesslich müssen Menschen die modernen Systeme entwickeln, vermarkten, bedienen und unterhalten können.

Immer wichtiger im rasanten Transformationsprozess ist es, einen Plan B bereit zu halten, damit man sich bei Schiffbruch über Wasser halten kann. Aber soweit muss es gar nicht erst kommen. Mit einem gesunden Mass an Menschenverstand und Aufrechterhalten eines minimalen IT-Grundschutzes kann eine IT-Infrastruktur relativ «sorgenfrei» betrieben werden.

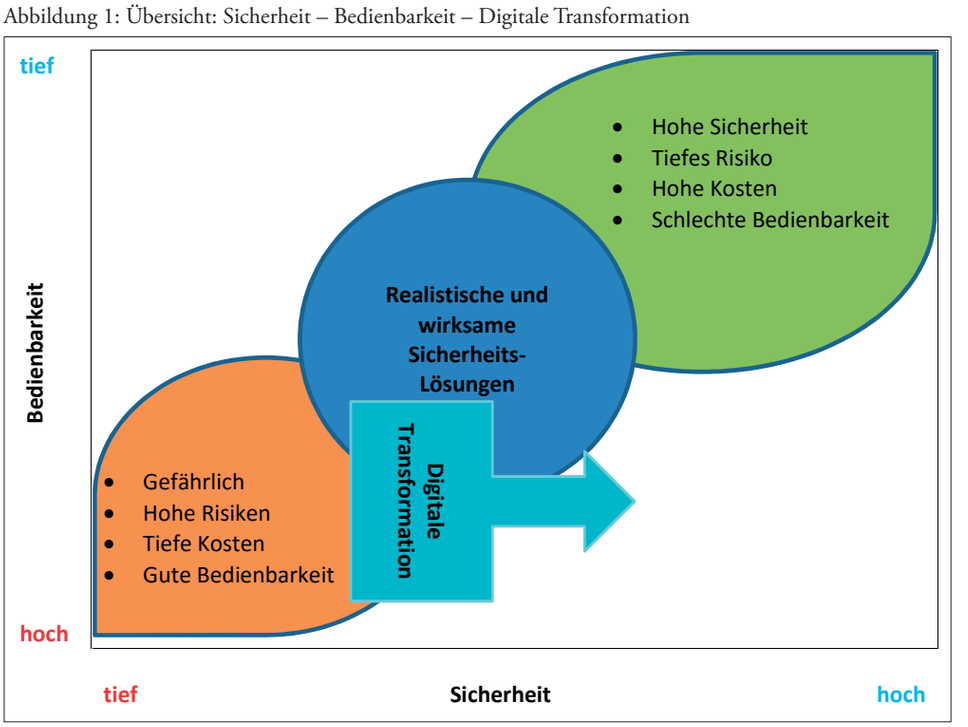
Patientendaten sind besonders schützenswert

Im Gesundheitswesen sind die besonders schützenswerten Patientendaten dem Datenschutzgesetz mit hohen technischen und organisatorischen Anforderungen unterstellt. Leider sind in Arztpraxen immer noch viele veraltete oder schlecht gewartete Betriebssysteme (z.B. Windows XP), welche von den Software-Herstellern nicht mehr gewartet werden, im Einsatz. Oftmals will man aus Bequemlichkeit die IT-Systeme aufgrund jahrelanger zuverlässiger Dienste nicht mehr erneuern oder es fehlen die finanziellen Mittel. Dieser Zustand kann in der heutigen Bedrohungslage zu schwerwiegenden Störungen oder zu erheblichen Krisensituationen führen, bei denen letztlich das Management die Verantwortung übernehmen muss. Nebst finanziellen und rechtlichen Folgen muss man das schwer abschätzbare, aber folgenschwere Reputationsrisiko mit einkalkulieren.

Mehr IT-Komplexität erfordert mehr Fach-Spezialisten

Die Komplexität der IT-Systeme bezüglich Hardware und Software ist in den vergangenen Jahren stark gestiegen. Eine Folge davon ist, dass

Abbildung 1: Übersicht: Sicherheit – Bedienbarkeit – Digitale Transformation



für die Betreuung und den Unterhalt immer mehr Fachpersonal notwendig wird. Bei so vielen Spezialisten wird es schwierig, einen Gesamtüberblick der vielen Schnittstellen und Abhängigkeiten der Systeme untereinander zu behalten. Je mehr IT-Systeme unterhalten werden, umso mehr Schwachstellen können folglich auftreten. Gemäss «Threat Report» von McAfee Labs vom Juni 2016 wurden folgende Angriffsintensitäten festgestellt:

- McAfee[1] GTI (Global Threat Intelligence) erhielt täglich durchschnittlich 49.9 Milliarden Anfragen.
- Pro Stunde wurden (per E-Mail, Browser-Suchen usw.) mehr als 4.3 Millionen Versuche gestartet, die McAfee-Kundschaft zur Herstellung einer Verbindung zu riskanten URLs zu verleiten.
- Pro Stunde wurden in den Netzwerken der McAfee-Kunden mehr als 5.8 Millionen infizierte Dateien entdeckt.
- Pro Stunde versuchten weitere 1.8 Millionen potenziell unerwünschte Programme, sich zu installieren oder zu starten.
- Pro Stunde versuchten McAfee-Kunden 500 000 Mal, sich mit riskanten IP-Adressen zu verbinden, oder solche Adressen versuchten, eine Verbindung mit den Kundennetzwerken herzustellen.

Aufgrund dieser massiven Bedrohungslage müssen technisch und organisatorisch wirksame Gegenmassnahmen getroffen werden. Der Mensch als schwächstes Glied in dieser Kette kann über Erfolg oder Misserfolg grundsätzlich (fast) immer selber entscheiden.

Akute Bedrohungslage

Wie bereits erwähnt befinden wir uns – und dies unabhängig davon in welcher Branche wir tätig sind (privat und geschäftlich) – in einer ständigen Bedrohung aus dem Internet. Symbolisch kann man die Situation mit Eisbergen darstellen, die als schwimmende Eismassen durch Gletscherabspaltung in den Nord- oder Südatlantik gelangen. Die verschiedenen Formen und Farbausprägungen dieser «Kolosse» sind faszinierend, unheimlich und gefährlich zugleich. Vergleicht man die versteckte Eismasse unter dem Wasser, welche 90% des Volumens entspricht, mit dem sichtbaren Teil über Wasser, so ist der Respekt der Schiffskapitäne gegenüber diesen Kolossen nachvollziehbar. Die Bedrohung durch Eisberge symbolisieren auch die Gefahren in der IT- und Informationssicherheit. Meist sind nur die sichtbaren Spitzen der Schwachstellen bekannt und wir bemerken infolgedessen die versteckten Gefahren zu spät oder gar nicht.

NIS-Richtlinie

Am Mittwoch, 6.7.2016, haben die EU-Abgeordneten die Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) verabschiedet, welche die Zusammenarbeit der Mitgliedstaaten im Bereich Cyber-Sicherheit fördern soll. Unternehmen, die kritische Bereiche wie Energie und Gesundheitsversorgung unterhalten, müssen ihre IT-Infrastrukturen absichern und Übergriffe vollständig melden. Die Richtlinien müssen aller Voraussicht nach auch von der Schweiz adaptiert werden, vor allem, wenn Schweizer Firmen «grundlegende Dienste» in der EU anbieten oder solche von EU-Staaten genutzt werden (Quelle: http://www.europarl.europa.eu/news/de/news-room/20160701STO34371/EU-weite-Vorschriften-zur-St%C3%A4rkung-der-Cyber-Sicherheit).

Freche Erpresser am Werk

Gegenwärtig liest und hört man oft in den Medien über Schadprogramme im Bereich Ransomware, die den Zugriff auf Systeme und Daten blockiert und nur mit Bezahlung einer Lösegeldforderung evtl. wieder freigegeben wird (digitale Erpressung). Dieses Cyber-Angriff-Szenario ist in den ersten Windows-Betriebssystem-Varianten bereits 2006 entdeckt worden und hat sich in den letzten Monaten stark weiterentwickelt und massiv verbreitet.

Die Erpressungstrojaner lösen offenbar die konventionellen Virenprogramme als neue lukrative Geldmasche ab. Die Verschlüsselungstrojaner nisten sich relativ einfach und unbemerkt z.B. durch Öffnen eines E-Mail Anhangs mit Word-Datei in das IT-System des Opfers ein und beginnen anschliessend mit der Verschlüsselung der Festplatte(n). Die Melde- und Analysestelle Informationssicherung MELANI rät dringend davon ab, auf die Lösegeldforderungen der Täter einzugehen. Trotz dieser Empfehlung werden immer wieder die geforderten Lösegelder bezahlt, somit die Täterschaft belohnt und wiederum darin bestärkt, es weiter zu versuchen.

Heute erlebt die Verbreitung von Ransomware einen richtigen Boom. Innerhalb eines Jahres haben sich die Ransomware-Varianten mehr als verdoppelt. Gemäss einer Studie von Kaspersky Lab vom Juni 2016 ist Ransomware für 42.2 Prozent der mittelständischen Unternehmen eine geschäftskritische Bedrohung.

Die häufigsten Angriffsmethoden zur Verbreitung von Verschlüsselungstrojanern sind Spam-E-Mails mit schädlichen Anhängen (z.B. Office-Dokumente mit bösartigen Makros) sowie gehackte Webseiten (Drive-by-Angriffe), bei denen man sich lediglich durch Aufruf der Webseite infiziert.

Warum gehen die Opfer trotzdem auf die Lösegeld Forderungen ein?

Einerseits sind die IT-Systeme der Opfer (PCs, Server usw.) ungenügend oder überhaupt nicht durch ein aktuelles Backup sichergestellt, andererseits ist die Wichtigkeit und Notwendigkeit der verschlüsselten Daten für das Unternehmen grösser als die Lösegeldforderung der Kriminellen. Beide Faktoren bestärken die Täterschaft in ihrem Vorgehen und die Opfer zur Lösegeldzahlung. Dabei müsste man es nicht soweit kommen lassen. Man kann wichtige präventive Massnahmen ergreifen.

Ein zentrales Element, um gegen Verschlüsselungstrojaner zu bestehen, ist ein regelmässiges tägliches Backup von Daten und Systemen einzurichten. Diese Sicherung sollte auf ein externes Laufwerk erfolgen und anschliessend auch extern aufbewahrt werden. Im Falle einer aktiven Verschlüsselung durch Ransomware werden womöglich sämtliche Laufwerke (auch mit USB angeschlossene Speichermedien), die am PC-System angeschlossen sind, verschlüsselt und somit der rettende Backup-Effekt praktisch eliminiert. Zudem sollten nur E-Mails geöffnet werden, von deren Absendern auch welche erwartet werden. In einem simplen Drei-Sekunden-Sicherheits-Check vom Bundesamt für Sicherheit in der Informationstechnik (BSI) sind E-Mails in einer ersten groben Beurteilung wie folgt zu klassifizieren:

- Ist der Absender bekannt?
- Ist der Betreff sinnvoll?
- Erwarte ich gegebenenfalls überhaupt einen Anhang von diesem Absender?

Im Zweifelsfall empfehlen wir, die E-Mail unwiderruflich zu löschen (Shift-Delete). Auch wenn mal eine E-Mail zu viel gelöscht wurde, bricht noch keine Welt zusammen: Bei wichtigen E-Mails melden sich die Absender bestimmt später wieder.

DDoS-Attacken

Eine weitere Möglichkeit, Opfer zu erpressen, sind sogenannte DDoS-Attacken (Distributed Denial of Service). Diese Angriffe zielen auf die Verfügbarkeit von Netzwerkdiensten, insbesondere Internet-Diensten (Web-Server, E-Banking-Server usw.) ab. Dabei werden die externen Datenleitungen des Opfers derart mit Daten-

1 McAfee=Einer der grössten Software-Hersteller für Antiviren

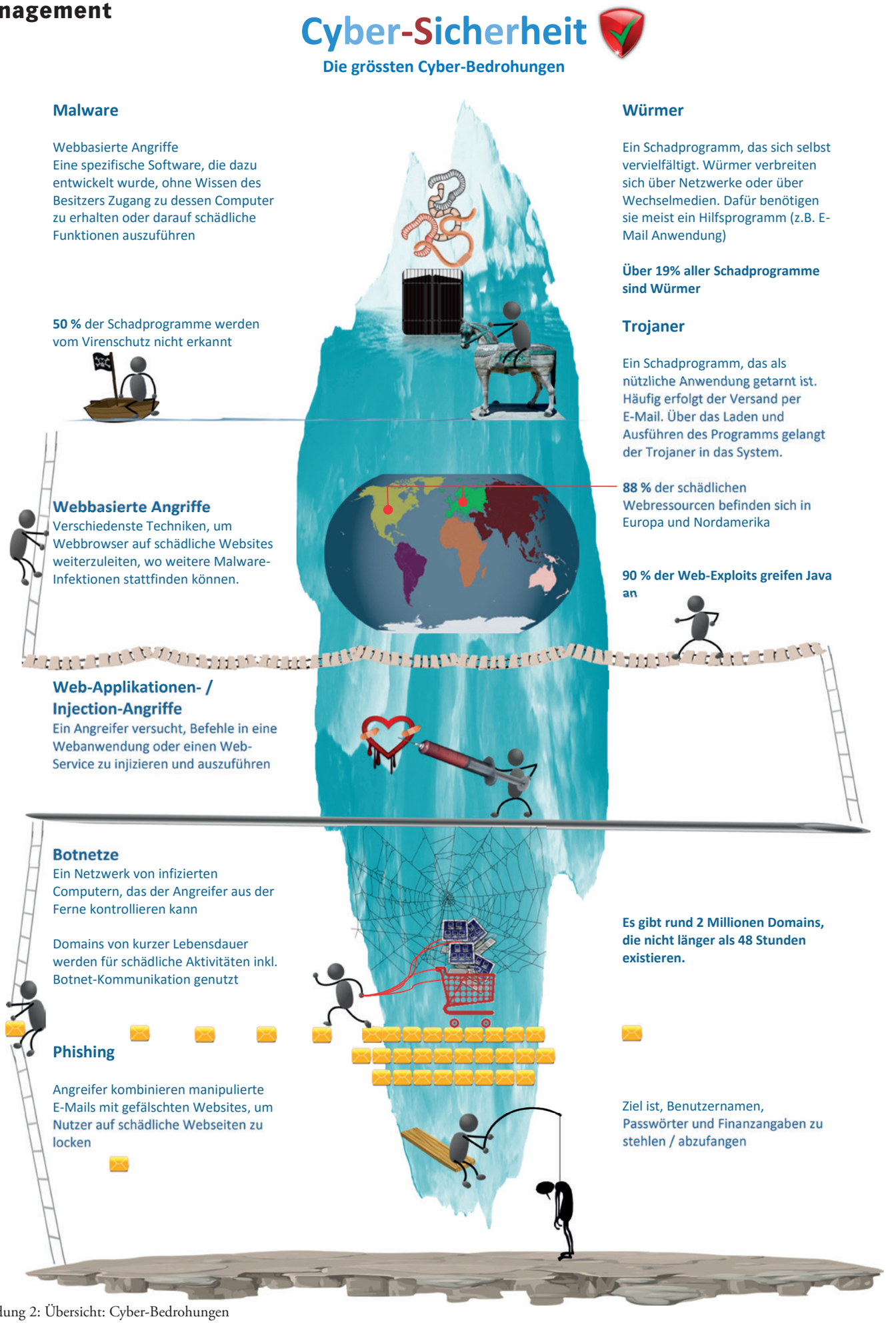


Abbildung 2: Übersicht: Cyber-Bedrohungen

paketen oder E-Mails geflutet, dass die Netzwerkkommunikation in die Knie gezwungen oder zum Absturz gebracht wird. Die DDoS-Attacke wird meist mit einer Ankündigung per E-Mail inkl. Lösegeldforderung kurz vor der Auslösung kommuniziert. Leider gibt es für diesen Angriffstyp noch keine wirksame Gegenmassnahme. In solchen Fällen empfehlen wir, mit dem ISP (Internet Service Provider) Kontakt aufzunehmen, um weitere Schritte zur Behebung oder Entlastung der Situation einzuleiten und den Fall bei der Polizei zu melden.

Wirksame Massnahmen zu Schutz und Prävention

Wie bei jeder Bedrohung folgen wir unserem Ur-Instinkt aus der Steinzeit. Dabei gibt es grundsätzlich drei verschiedene Verhaltensweisen, die sich bis heute nicht geändert haben:
- Angriff/Verteidigung
- Weglaufen
- Tot stellen

Überträgt man die drei Grund-Reaktionen bei Bedrohungssituationen auf die IT-Sicherheit, so können wir folgende interessante Parallelen feststellen:

Angriff/Verteidigung?

E-Mail und Internet-Verkehr müssen durch eine aktuelle Antiviren-Software umfassend geschützt werden. Empfehlenswert sind Produkte, die in unabhängigen Tests in den ersten Rängen abschneiden. Die Funktionalität eines sogenannten URL-Filters kann verdächtige und suspekte Webseiten sperren oder davon warnen. Bei eingehenden E-Mails empfehlen wir, infektionsgefährdende Anhänge wie z.B. .exe Dateien zu blockieren und in eine Quarantäne zu verschieben. Um den Faktor Mensch als unberechenbarstes und schwächstes Element bezüglich Sicherheit nachhaltig zu schulen, ist es von zentraler Bedeutung, die Sensibilisierung (Awareness) als dauernde Aufgabe in die Unternehmenskultur einzubinden. Wenn Mitarbeitende die Internet-Gefahren und die Verhaltensmassnahmen nicht kennen, werden sie auch nicht angemessen und richtig handeln. Das Ziel der Awareness gemäss InfoGuard AG ist, den Menschen vom unbewusst falschen Handeln zum unbewusst richtigen Handeln zu bewegen (siehe Abbildung 4).

Weglaufen? Das Internet vergisst nie

Sobald man sich mit dem Internet verbunden hat, ist man mit der ganzen Welt vernetzt. Leider kann man vor dem Internet nicht einfach davonlaufen wie beispielsweise, wenn es regnet oder kalt ist. Zudem hinterlassen wir im Internet

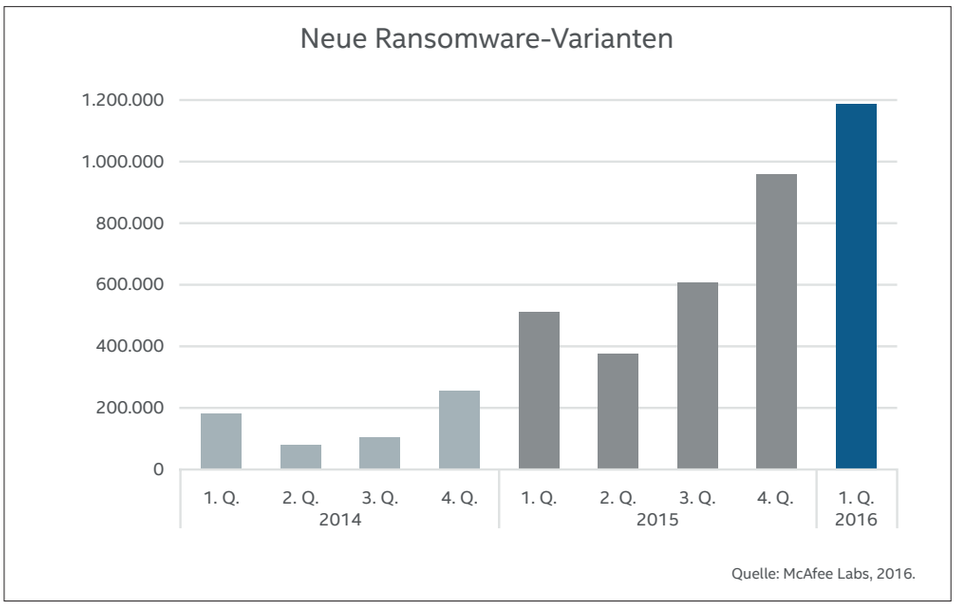


Abbildung 3: Entwicklung Ransomware-Varianten

Spuren, welche immer wieder über unsere Aktivitäten Auskunft geben, für Werbezwecke genutzt und jahrelang aufbewahrt werden.

Sich tot stellen?

Ein sehr wichtiges Sicherheits-Prinzip bei der Internet-Benutzung ist die Tarnung und Verschleierung von persönlichen und vertraulichen (Patienten-)Daten. Ein einfaches Beispiel ist die Aktivierung des Abwesenheits-Assistenten für eingehende E-Mails bevor man in die Ferien verreist und auf Facebook die Absenz «postet» und das Ereignis mit schönen Urlaubs-Fotos untermalt. Diese Gratis-Informationen werden von aufmerksamen Einbrechern gerne entgegengenommen und für ihr Handwerk genutzt (gut informiert macht Diebe). Unser Tipp: Abwesenheitsmeldung (privat und geschäftlich) wenn immer möglich nicht einschalten. Eventuell muss das aufgrund interner Geschäftsrichtlinien aber doch sein. In diesem Fall empfehlen wir, nur allgemeine Formulierungen anzuwenden wie: «vorübergehend abwesend», «momentan nicht anwesend» usw. Die elegantere Möglichkeit wäre, personelle Abwesenheiten im Betrieb organisatorisch zu regeln, in dem man seine E-Mails an seine Stellvertretung weiterleitet und nur interne Abwesenheitsmeldungen versendet.

Das Zauberwort, um sich tot zu stellen, heisst Verschlüsselung und Zugriffsschutz, wo immer es möglich ist (verschlüsselte E-Mails und Datenleitungen, starke Passwörter, Rechtevergabe nach dem «need-to-know»-Prinzip usw.). Ebenso sollte man nur in einem geschützten Umfeld über vertrauliche (Patienten-)Informationen sprechen (Vorsicht bei Telefongesprächen, Diskussionen usw.). Mobile Geräte wie Tablets, Notebooks, Smartphones mit Zugriff auf sensible Daten (Remote oder direkt) sollten immer unter Aufsicht mitgenommen werden oder sicher verschlossen (z.B. abschliessbare Tischschublade) ohne Aufsicht aufbewahrt werden. Generell müssen sensible Daten immer verschlüsselt und mit starkem Zugriffsschutz (Zweifaktor-Authentifizierung) konfiguriert werden. Ein aufgeräumter Bürotisch (Clear-Desk) und die Aktivierung des Sperrbildschirmes (Windows-Taste +L) auch bei kurzen Absenzen helfen gegen neugierige Blicke in (Patienten-)Daten und sonstige vertrauliche Dokumente.

Der Grundsatz KISS

Die Tendenz, dass IT-Systeme immer komplexer werden und die Übersichtlichkeit resp. die Sicherheitselemente sich immer dynamischer anpassen müssen, können wir mit der fortschreitenden Digitalisierung nicht aufhalten. Dennoch empfehlen wir, nach dem Grundsatz KISS (keep it simple and stupid) bei der Umsetzung und Anpassung von IT-Systemen und deren Sicherheitsanforderungen vorzugehen. Wir stellen bei unserer Kundschaft häufig fest, dass die gekauften Soft- und Hardware-Produkte bedenkenlos und rasch installiert werden, ohne die Gewissheit zu besitzen, ob diese den aktuellen Bedrohungen (Viren, Trojaner, Phishing, Ransomware usw.) standhalten können. Für das Überprüfen der Sicherheit im Bereich IT- und Informationssicherheit sollte eine unabhängige Beurteilung (externe Beratung und Spezialisten) in Form einer Zweitmeinung oder eines Sicherheits-Reviews eingeholt werden.

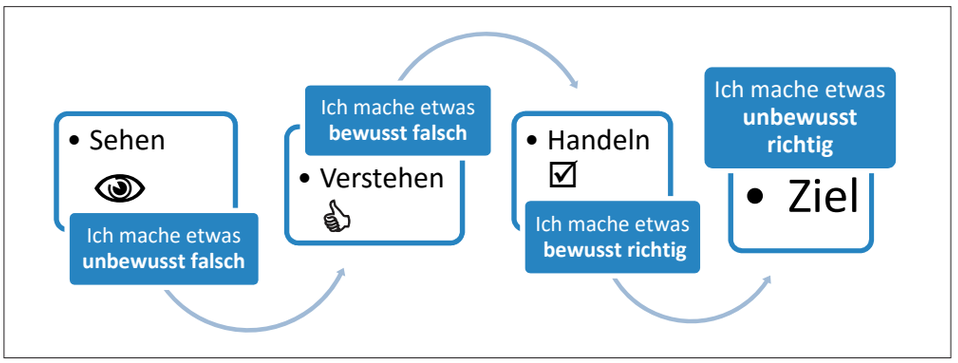


Abbildung 4: Awareness-Stufen

Die Basis für das Erstellen eines Sicherheitskonzepts ist die Aufnahme oder Erhebung des Ist-Zustandes der genutzten IT-Systeme. Diese «First Cut-Analyse» ist für die Definition des Soll-Systems und die daraus folgenden Sicherheits-Massnahmen von zentraler Bedeutung.

Eine wichtige und umfangreiche Massnahme in diesem Zusammenhang ist die Klassifizierung der Daten. Diese Aufbereitung bedarf einer sorgfältigen Erhebung und Inventarisierung der Daten. Aufgrund der Klassifizierung (z.B. vertraulich, intern und öffentlich) werden die entsprechenden Data-Owner als verantwortliche «Eigner» zugeteilt und die entsprechenden Sicherheitsbarrieren mit Zugriffsrechten implementiert.

Einfache (Verhaltens-)Regeln

Im privaten Umfeld sollten folgende Hinweise und Tipps für die IT-Sicherheit eingehalten werden:

- Betriebssysteme und alle auf dem Gerät installierten Applikationen (Adobe Reader, Adobe Flashplayer usw.) sind immer und unverzüglich auf dem neuesten Stand, Aktivierung von automatischen Updates.
- Regelmässig und zeitnah eine Sicherungskopie (Backup) auf einen externen Datenträger erstellen. Nach erfolgreichem Sichern das externe Medium von der USB-Schnittstelle entfernen → Gefahr der Verschlüsselung des Mediums durch Verschlüsselungstrojaner.
- Bei eingehenden unbekannten oder verdächtigen E-Mails den drei Sekunden Sicherheitscheck befolgen:
  1. Kenne ich den Absender?
  2. Ist der Betreff aussagekräftig/verständlich?
  3. Erwarte ich einen Anhang?
- Einen aktuellen Virenschutz installieren und unterhalten sowie alle Warnmeldungen ernst nehmen (Virenschutz abgelaufen, Probleme beim Update usw.).
- Immer eine Firewall verwenden (bei Microsoft standardmässig aktivieren oder über das Virenschutzprogramm einschalten – sofern vorhanden).
- In Sicherheitsfragen sich nach dem **M A M I-Prinzip** verhalten:
  - **M** grundsätzlich **m**isstrauisch
  - **A** grundsätzlich **a**ufmerksam
  - **M** **M**ithelfen: Kolleginnen und Kollegen bei Fehlverhalten oder Missgeschicken freundlich darauf hinweisen (z.B. Bildschirmschoner ist beim Verlassen des Arbeitsplatzes nicht eingeschaltet)
  - **I** sich in den Medien **i**nformieren (Internet: z.B. https://www.melani.admin.ch/melani/de/home.html) über die aktuelle Bedrohungslage, Sicherheitslücken und mögliche Gegenmassnahmen
- Verdächtige Phishing-Mails oder Phishing-Webseiten unter folgendem Link melden: https://www.antiphishing.ch/de/ Sie helfen damit im Kampf gegen Phishing.

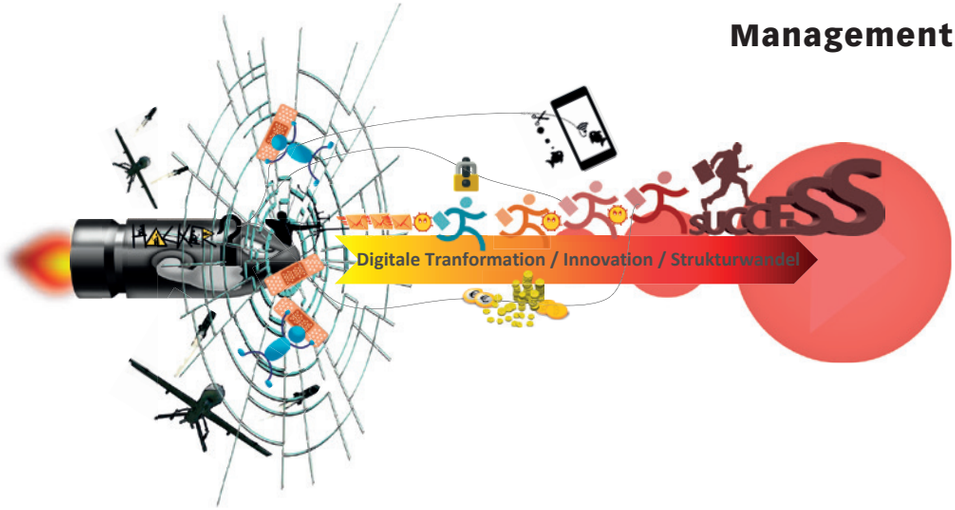
Zusätzliche Massnahmen für Unternehmen

- Eine zentrale Anlaufstelle für Sicherheitsfragen oder Abklärungen einrichten (z.B. bei Erhalt eines verdächtigen E-Mails). Diese Anlaufstelle kann intern aber auch extern (externe Sicherheitsberater) organisiert werden.
- Die Mitarbeitenden regelmässig bezüglich Awareness im Bereich IT- und Informations-Sicherheit schulen. Es ist vorteilhaft, dafür auch externe und kompetente Unterstützung in Anspruch zu nehmen.
- Regelmässig die Risiken im Bereich Informationssicherheit überprüfen und die Geschäftsleitung über die aktuelle Situation informieren (Reporting).
- Eine starke Passwort-Richtlinie definieren (z.B. Wechsel alle 3 Monate mit 12 Zeichen mit Buchstaben, Zahlen und Sonderzeichen).
- Vorsicht bei Cloud-Diensten. Die Verantwortung können Unternehmen durch Outsourcing der Daten nicht abgeben – im Gegenteil: Sie müssen die Aufsicht und Kontrolle (Zugriffe) für ferngespeicherte Daten vertraglich regeln und überprüfen. Sensible Daten sollten sie nur im eigenen Netzwerk oder lokal speichern.
- Wer über eine eigene Website verfügt, sollte das Content Management-System (CMS) immer auf aktuellem Sicherheitsstand halten – dazu eine Web Application Firewall (WAF) verwenden, um die Webapplikationen gegen Internet-Angriffe zu schützen.
- Log-Dateien protokollieren und auf suspekte Einträge bei kritischen Systemen überprüfen (Mailserver, Webserver, Datenbankserver usw.). Die Dateien sollen für mindestens 6 Monate aufbewahrt werden; dafür ist der Backup-Prozess entsprechend einzurichten.
- Zugriffsrechte ausschliesslich nach dem need-to-know-Prinzip vergeben (nur so viele Rechte vergeben, wie nötig sind) und die Rechte regelmässig (z.B. jährlich) von der vorgesetzten oder verantwortlichen Stelle überprüfen lassen. Bei Personalaustritten muss der User-Account unverzüglich deaktiviert werden.
- Netzwerke segmentieren: Sensible Daten sollten in einem eigenen Netzwerk vor unberechtigten Zugriffen geschützt sein (need-to-know-Prinzip).
- Potenziell gefährliche E-Mail Anhänge wie .exe, .bat, .com, .vbs, .vba, .js, .jar usw. blockieren und einen effizienten Spamfilter einsetzen.
- URL-Filter einsetzen (wenn nicht bereits im Antiviren-Programm enthalten), um bereits bekannte verdächtige und suspekte Webseiten zu sperren oder davor zu warnen.
- Remote Zugänge sollten immer mit Zweifaktor-Authentifizierung geschützt werden (One-Time Password, SMS-Token usw.).
- Sensible Daten auf mobilen Geräten immer verschlüsseln oder diese erst gar nicht auf den Endgeräten speichern. Wenn möglich einen verschlüsselten Zugriff vom mobilen Gerät auf die benötigten Daten einrichten (nur View-Ansicht). Bei einem allfälligen Diebstahl oder Verlust des Gerätes sind die sensiblen Daten nicht physisch gespeichert und können so auch nicht gehackt werden.

Aus all diesen Überlegungen und Vorschlägen lässt sich folgendes Fazit ziehen: Sicherheit ist nicht bequem, muss aber mit gesundem Menschenverstand gelebt werden.

Spitäler und Praxen haben grossen Handlungsbedarf

Die Gefahren sind enorm, die drohenden Schäden nicht minder. Handlungsbedarf ist gegeben. Wie sieht das konkret aus? Wie sollen Institu-



Die digitale Transformation und laufende IT-Innovationen schaffen viele Vorteile, aber auch neue Risiken.

tionen im Gesundheitswesen vorgehen, damit sie zu einem systematischen Schutz ihrer vielen sensiblen Daten gelangen? – Markus Säuberli, als unabhängiger externer Sicherheitsberater der Säuberli IT-Security Services (sITss), stellte sich unseren Fragen:

Wo sehen Sie die grössten Gefahren?

Markus Säuberli: «Einerseits sehe ich im rasch wachsenden Prozess der «digitalen Transformation» und Innovation eine starke Zunahme der Automatisierung und Roboterisierung, die in vielen Sektoren wie beispielsweise im Finanzbereich, Gesundheitswesen und in der Auto-Industrie voll im Gange ist, eine wachsende Bedrohung. Die Kontrolle und Aufsicht von (geschäfts-)kritischen Prozessen werden vermehrt durch digitale Entscheide gesteuert, was wiederum den Kriminellen mehr Potential bietet, die Systeme zu beeinträchtigen, zu manipulieren oder ganz zu zerstören. Aufgrund der zunehmenden technischen Komplexität fehlt meist die Gesamtübersicht der IT-Systeme und folglich sind auch die entsprechenden Sicherheitselemente nicht vorhanden.

Andererseits passieren oft gravierende Sicherheitsvorfälle durch menschliche Fehlentscheide, sei es durch tägliche Routine, Bequemlichkeit oder Sorglosigkeit. Der Mensch handelt und entscheidet nicht immer rational und nachvollziehbar und trotzdem darf der Mensch in wichtigen Prozessen nicht fehlen (Beschriftung von Reagenzgläsern und Ampullen usw.). Beide Faktoren, Mensch und Technik, benötigen ein «gesundes» Mittelmass – dieses muss für jeden Betrieb individuell festgelegt werden.»

Markus Säuberli, unabhängiger externer Sicherheitsberater der Säuberli IT-Security Services (sITss)

Was raten Sie, als erste Schritte zu unternehmen?

«Ein wichtiges Element für jeden Betrieb, sei es in Arztpraxen, Spitälern oder im privaten Umfeld, ist die Übersicht der IT-Systeme zu behalten. Heutzutage ist man eher dazu geneigt, alte bestehende Systeme auszubauen als zu erneuern. Um eine Auslegeordnung vorzunehmen, ist es von Vorteil, eine unabhängige externe Begutachtung der IT- und Sicherheits-Infrastruktur vorzunehmen und in einem persönlichen Gespräch und einer Besichtigung der IT-Systeme den Ist-Zustand zu erfassen. Mit einer Checkliste in Form eines Fragebogens (First-Cut-Analyse) werden Fragen gestellt wie: ‹Auf welche Daten und Applikationen sind Sie in Ihrem Aufgabengebiet angewiesen?› oder ‹Was passiert, wenn diese nicht mehr verfügbar sind?›. Die Ergebnisse der umfangreichen Fragen und Antworten bezüglich Management, Organisation, Technik und Recht werden ausgewertet, die Handlungsbedürfnisse ermittelt und mit dem Kunden besprochen. Ziel ist es, einen angemessenen IT-Grundschutz für den Betrieb zu realisieren.»

Sie erwähnen häufig die Mitarbeitenden als Gefahrenpotenzial. Wie sind diese zu motivieren, IT-Sicherheit als tägliche Aufgabe zu sehen?

«Ein zentrales Element für die kulturelle Einbindung der IT-Sicherheit im Betrieb ist die Unterstützung und Vorbildfunktion der Vorgesetzten und des Managements. Ebenso sollte eine zentrale Anlaufstelle für Sicherheitsfragen eingerichtet werden, die rasch, unkompliziert und kompetent Auskunft z.B. über verdächtige E-Mails oder ungewöhnliche Ereignisse (Meldungen, suspektes Applikationsverhalten usw.) geben kann. Die meines Erachtens wichtigste Massnahme ist eine regelmässige Schulung im Bereich Awareness, Awareness und nochmals Awareness. Jeder Mitarbeitende soll nachvollziehen können, dass nur mit gegenseitiger Unterstützung und Zusammenarbeit ein konstant hohes Mass an IT-Sicherheit erreicht werden kann. Es genügt schon ein einziges Fehlverhalten eines Mitarbeitenden, um die Sicherheitsbarrieren der Unternehmung zu stürzen und die Kriminellen zum Erfolg zu führen.

Schliesslich trägt auch ein gesundes und intaktes Arbeitsklima dazu bei, loyale und zufriedene Mitarbeitende zu beschäftigen, die das Thema Sicherheit zum Wohle der Unternehmung gewissenhaft umsetzen. Wenn man nicht mehr erklären muss, warum man etwas richtig gemacht hat, sondern jeder Mitarbeitende intuitiv richtig handelt, hat man sein Ziel erreicht.»

Weitere Informationen

Wichtige Links oder Quellen-Nachweise
https://www.melani.admin.ch
https://www.medinside.ch
https://www.antiphishing.ch
https://securityblog.switch.ch
https://www.ebas.ch
https://www.cybercrime.admin.ch
https://www.bsi.bund.de
https://www.bsi-fuer-buerger.de
https://www.enisa.europa.eu
http://www.sihb.ch

Nützliche Merkblätter z.B. Facebook oder Twitter Einstellungen
https://www.ebankingabersicher.ch/de/ihr-sicherheitsbeitrag/merkblaetter

Beratung für IT-Sicherheit
Markus Säuberli
MAS Information Security HSLU
Dipl. Wirtschaftsinformatiker
Säuberli IT-Security Services
5722 Gränichen
markus.saeuberli@sitss.ch
www.sitss.ch