Weiterbildungskurse 2018

SBV Schweizerischer Brunnenmeister-Verband

www.brunnenmeister.ch

IT-Sicherheit im technischen Umfeld der Wasserversorgungen

Von:

Christian Rentsch
Sollberger Ingenieure GmbH
Bielstrasse 14
3270 Aarberg

Sollberger Ingenieure GmbH
Netz- & Prozessleittechnik

www.sollbergering.ch

christian.rentsch@sollbergering.ch

Veranstaltungsort:
CAMPUS SURSEE
Lernen / Leben / Erleben

IT-Sicherheit im technischen Umfeld der Wasserversorgungen

Christian Rentsch

1 Einleitung

IT-Sicherheit ist in aller Munde und gewinnt laufend an Wichtigkeit. Es vergeht kein Tag, an dem nicht grössere IT-Pannen oder Hackerangriffe gemeldet werden.
Kein Wunder, es werden auch immer mehr Funktionen und Prozesse digitalisiert.

So auch in der Wasserversorgung. Es werden immer mehr IT-Systeme genutzt, um den neuen Anforderungen an Innovation und Effizienz gerecht zu werden. Dies birgt jedoch auch Gefahren im Bereich IT-Sicherheit und bedingt entsprechende Kenntnisse der Anlagenverantwortlichen.

Im Folgenden soll auf das Thema IT-Sicherheit aus Sicht des Brunnenmeisters eingegangen werden. Es wird eine Übersicht über Bedrohungen gegeben und es werden einige Vorschläge für einfache Sicherheitsmassnamen gemacht. Der Schwerpunkt liegt dabei auf technischen IT-Systemen, welche häufig in Wasserversorgungen eingesetzt werden. Als Beispiel wird das Leitsystem betrachtet. Die Aussagen sind aber grundsätzlich und gelten auch für andere IT-Systeme.

Das Dokument richtet sich an Brunnenmeister und Techniker und soll als Einstieg und Übersicht dienen. Einzelne Themen können über die angegebenen Links vertieft werden.

1.1 Der Begriff «IT-Sicherheit»

In den folgenden Kapiteln sprechen wir immer wieder von IT-Sicherheit. Es geht also um Sicherheitsfragen in der Informationstechnik oder kurz gesagt um sichere Informatiksysteme. Diese arbeiten wiederum mit Daten. Ob Wasserstandskurven oder Pumpenbefehle, es sind am Schluss immer Daten, um die es sich in der Informationstechnik dreht.

Dabei ähneln IT-Systeme einer Wasserversorgung: Im übertragenen Sinn entspricht das Wassernetz mit seinen Pumpen und Klappen, welche das Wasser fördern und speichern einem IT-System. Die Daten wiederum können mit dem Wasser verglichen werden: Sie sind das Produkt, um das sich das System kümmert.
Wie mit dem Wasser, muss auch mit den Daten und den IT Systemen sorgfältig umgegangen werden, sie müssen geschützt und gepflegt werden.

2 Das IT-Umfeld des Brunnenmeisters

2.1 Ausgangslage

Heute werden im technischen Umfeld bereits zahlreiche IT-Systeme wie Leitsystem, Qualitätsmessungen und Leckortungssysteme betrieben. Jedoch werden diese meistens als Komplettsystem angeschafft und quasi als Insel und ohne Schnittstellen zu anderen IT Systemen betrieben.

Im Bereich der Kommunikation sind bei Wasserversorgungen zum Teil noch alte Signalkabel mit Wechselstromtelegrafie-Verbindungen oder anderen seriellen Verbindungen mit proprietären Protokollen im Einsatz. Ethernet-Verbindungen existieren, stehen meist aber nur einzelnen Systemen zur Verfügung.

Die Vorteile sind abgeschottete Systeme und klare Liefergrenzen. Jedoch ist es schwierig neue Systeme ein- oder anzubinden und Synergien zu nutzen.

2.2 Was hat sich geändert

In den letzten Jahren haben sich die Anforderungen an die technischen Systeme geändert. Die Systeme müssen offen und von fern erreichbar sein. Daten werden immer öfter mit anderen Systemen ausgetauscht und die Kommunikation soll schnell und standardisiert über Datennetze vonstattengehen. Zudem werden immer mehr Funktionen digitalisiert, was immer mehr IT Systeme mit sich zieht.

Dies bringt entscheidende Vorteile mit sich:

- Daten stehen digital weiteren Systemen und Anwendungen zur Verfügung. Arbeiten wie Statistiken und Berichte können automatisiert erstellt werden.
- Durch die Vernetzung kann auch von ausserhalb der Firma auf die Systeme zugegriffen werden. Sei es von Zuhause aus mit dem privaten PC oder über mobile Geräte wie Tablet und Smartphone: Es ist möglich, sich jederzeit und überall einen Überblick zu verschaffen oder sogar in die Wasserbewirtschaftung einzugreifen.
- Durch die Digitalisierung der Funktionen sind diese nicht mehr an bestimmte Hardware gebunden. Es wird möglich, Ressourcen zusammenzulegen oder gar ausserhalb der Firma in eine Cloud auszulagern.

Doch jede Medaille hat zwei Seiten. So müssen auch Nachteile genannt werden:

- Die Systeme und deren Zusammenspiel werden immer komplexer. Dies macht sie anfälliger auf Pannen und Fehlfunktionen. Häufig müssen für Updates, Anpassungen und Erweiterungen Spezialisten beigezogen werden.
- Je mehr Funktionen durch IT-Systeme übernommen werden, desto wichtiger werden diese für die Aufrechterhaltung der Wasserversorgung. Bedrohungen die früher ignoriert werden konnten, werden immer mehr zur Gefahr.
- Die IT-Sicherheit wird zu einem immer wichtigeren Bestandteil einer Wasserversorgung.

2.3 Wohin geht die Reise

Künftig werden die Systeme immer näher zusammenrutschen und Daten miteinander austauschen. Hardware wird immer häufiger von verschiedener Software gemeinsam genutzt, die Systeme werden also immer häufiger virtualisiert. Sei dies im Bereich der Datennetze oder der Serverhardware.
Dies bedeutet, dass die Hardware nicht mehr zwingend im eigenen Betriebsgebäude steht, sondern sich irgendwo auf der Welt in einem Rechenzentrum befinden kann. Somit ändern sich auch die Anforderungen an die Sicherheit massgeblich. Dies bedeutet, die Systeme von morgen werden komplexer und immer wichtiger, so dass der Sicherheit entsprechendes Gewicht verleiht werden muss.

2.4 Rolle des Brunnenmeisters

IT-Sicherheit ist nicht nur Sache der Informatiker. Diese können sich nur den technischen Problemen im Unternehmen annehmen. Die technischen Systeme wie ein Leitsystem bedienen kann nur die Fachperson.

Wo kommt der Brunnenmeister mit der IT-Sicherheit in Berührung und was bringt das für Verantwortung mit sich?

Bedienen von Systemen, am Beispiel des Leitsystems

- Schutz der persönlichen Zugangsdaten
  Das Arbeiten am Leitsystem bedingt viele Rechte des Benutzers für die Bedienung und Steuerung am System. Rechte bedeuten aber immer auch Pflichten: Die Zugangsdaten sind persönlich und müssen geschützt werden.
- Physischer Schutz
  Arbeitsplätze und Steuerungen (in den Wasserbauwerken) müssen geschützt werden. Denn die Sicherheitskonzepte der Lieferanten gehen davon aus, dass die Systeme unbefugten Personen nicht zugänglich sind. Die Räume sind also entweder abzuschliessen oder der Gebäudezutritt als solches zu überwachen.

Nutzen von Fernzugriffen

Heutige Systeme können oft auch über das Internet mit mobilen oder privaten Geräten erreicht werden. Das ist praktisch, nimmt den Benutzer aber auch in die Pflicht.

- Mobile Geräte wie Laptop, Tablet oder Smartphone
    - Mobile Geräte werden immer vielseitiger und können für die verschiedensten Aufgaben benutzt werden. Die Anwendungen hinter den Aufgaben haben aber andere Anforderungen an die IT-Sicherheit, was zu Problemen führen kann. Einfach Anwendungen können ein Einfallstor für Viren und Schadsoftware sein, welche anschliessend auch für Anwendungen mit einem hohen Sicherheitsbedarf zum Problem werden. Der Benutzer muss sich dessen bewusst sein und allenfalls auf nicht benötigte Anwendungen verzichten.
    - Mobile Geräte können abhandenkommen. Somit müssen mobile Geräte besonders gut gegen unbefugte Benutzung gesichert werden.
    - Mobile Geräte sind oft mit dem Internet verbunden. Das Internet ist öffentlich und jeder kann theoretisch mitlesen. Es ist dafür zu sorgen, dass vertrauliche Daten verschlüsselt übertragen werden.
- Heimcomputer
    - Heimcomputer können grundsätzlich auch für Fernzugriffe verwendet werden. Da diese auch für privates genutzt werden, muss durch den Benutzer sichergestellt werden, dass andere Benutzer nicht die Sicherheit gefährden.
    - Die Verantwortung für die privaten Geräte liegt beim Besitzer, er kümmert sich um Antivirusprogramme, Updates und entscheidet, ob zu installierende Software vertrauenswürdig ist.

Ein Brunnenmeister kann und muss sich somit aktiv an der IT-Sicherheit beteiligen. Seine Rolle ist in einigen Bereichen sogar zentral.

3 Gefahren und Bedrohungen

Will man mithelfen, etwas sicherer zu machen, muss man zuerst die Gefahr erkennen. Diese kann als Produkt von Bedrohungen und Schwachstellen betrachtet werden.

Bedrohung x Schwachstelle = Gefahr

Einige Beispiele:
Hacker x keine Firewall = unbefugter Systemzugriff
Festplattendefekt x kein Backup = Datenverlust
Schadsoftware x sorgloser Umgang mit E-Mail = Cyberangriff

Im übertragenen Sinn:
Druckschläge x altes Netz = Rohrbruch

In der IT-Sicherheit werden folgende Bedrohungen grob unterschieden. Die Gefahren müssen laufend neu beurteilt werden und bei Bedarf sind entsprechende Massnahmen zu ergreifen.

Ausfall der Technik

- Gerätedefekt
- Äussere Einflüsse, z.B. Feuer oder Wasser
- Kommunikationsausfälle
- Stromausfälle
- Systemabstürze, Softwarefehler

Faktor Mensch

- Fehlmanipulation
    - Unabsichtlich, z.B. durch Unwissenheit oder Unachtsamkeit
    - Absichtlich, z.B. durch frustrierte Mitarbeiter
- Krankheit eines für das IT-System wichtigen Mitarbeiters

Bedrohungen durch den «Faktor Mensch» betreffen uns alle. Wir alle können für den Betrieb der Systeme ebenso eine Störquelle darstellen wie die Technik.

Cyberkriminalität

- Erpressen, z.B. Lösegeldforderungen
- Stören / Lahmlegen, z.B. das Image schädigen, politische Botschaften
- Spionage, z.B. Betriebsgeheimnisse stehlen

Die Bedrohungen durch Cyberkriminalität sind real und nehmen ständig zu. Jede Sekunde werden weltweit unzählige Systeme Opfer eines Virus oder eines Schadprogramms. Solche Angriffe sind heute an der Tagesordnung, wie uns folgende Homepage auf eindrückliche Art aufzeigt:

map.lookingglasscyber.com
Weltweite Weiterverbreitung von bekannten Viren, in Echtzeit aufbereitet.

Wie die folgende Tabelle zeigt, nehmen Bedrohungen zu, die auf den Endbenutzer als Schwachstelle setzen.

Nr. (Nr. alt)	Top 10 2016
1 (3)	Social Engineering und Phishing†
2 (2)	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
3 (1)	Infektion mit Schadsoftware über Internet und Intranet
4 (5)	Einbruch über Fernwartungszugänge
5 (4)	Menschliches Fehlverhalten und Sabotage
6 (6)	Internet-verbundene Steuerungskomponenten
7 (7)	Technisches Fehlverhalten und höhere Gewalt
8 (9)	Kompromittierung von Extranet und Cloud-Komponenten
9 (10)	(D)DoS Angriffe
10 (8)	Kompromittierung von Smartphones im Produktionsumfeld

Top 10 Bedrohungen für die IT-Sicherheit (Quelle: Industrial Control System Security, BSI, 2016)

Am grössten innerhalb der Cyberkriminalität ist sicherlich die Gefahr einer Erpressung durch gezieltes Lahmlegen eines Systems. Doch schlimmer als der finanzielle Verlust wiegt für die Firmen meist der Imageschaden bei den Kunden, sollte das Sicherheitsproblem an die Öffentlichkeit gelangen.
In einem solchen Fall muss die Kommunikation gegenüber den Kunden gut überlegt und der Geschäftsleitung überlassen werden.

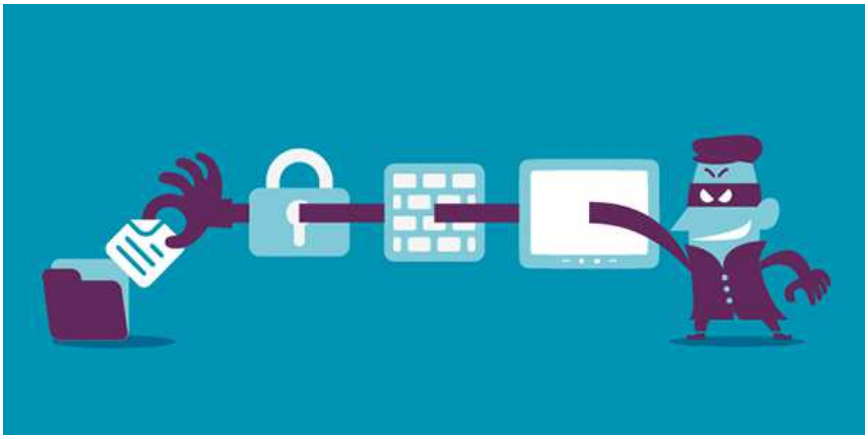
4 Beispiele aus der Praxis

Die folgenden zwei Beispielen zeigen, welche Gefahren von Cyberkriminalität ausgehen und welche Massnahmen durch den Brunnenmeister dagegen getroffen werden können.

4.1 Beispiel 1 - Hacken eines Systems

«
Kein System ist ohne Schwachstelle. Das bewies ein Hacker, der den Energieversorger der Stadt Liestal hackte.
»

SRF Kultur – Blackout – Ein Hack und der Strom ist weg

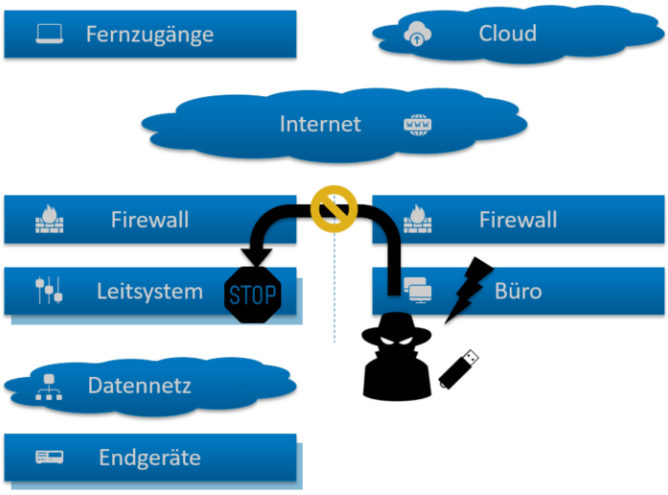


Symbolbild Hacker (Bild: http://searchsecurity.techtarget.com/definition/hacker)

Im Zuge der Doku «Blackout» des Schweizer Fernsehens wurde eine Sicherheitsfirma beauftragt, in das Leitsystem eines Energieversorgers einzudringen und die Kontrolle über das Stromnetz zu übernehmen.
Die Hacker brauchten zwei Versuche bis sie erfolgreich waren. Denn ein System hackt man nicht in wenigen Minuten. Es braucht einiges an Recherche und Planung, so dass anschliessend menschliche und technische Schwachstellen ausgenutzt werden können. Ein bevorzugter Weg, in ein System einzudringen, ist mittels Spionagesoftware.
Das in der Folge beschriebene Vorgehen ist stark vereinfacht, zeigt aber dennoch die typischen Schwachstellen und wie in etwa von Hackern vorgegangen wird. Zudem ist der Ablauf etwas angepasst, um auch das Gefahrenpotenzial über E-Mail zu verdeutlichen.

Zugang via Büronetz auf Leitsystem

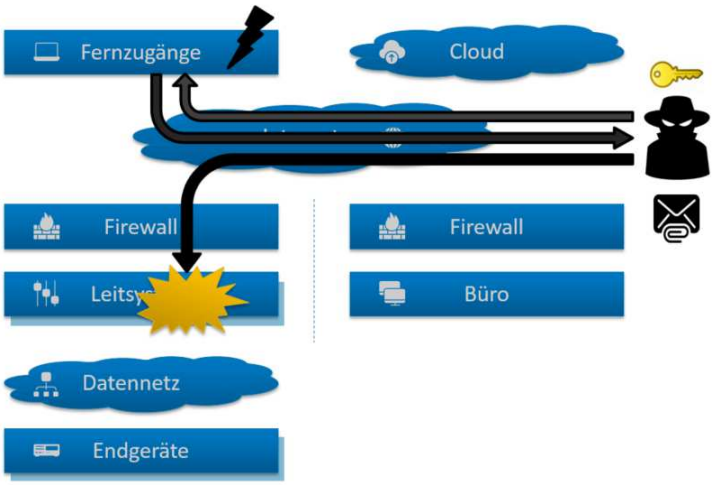
1. Hacker lädt Schadsoftware auf PC im Sitzungszimmer
2. Passwort des Systemadministrators wird gestohlen
   ⇨ Kontrolle über sämtliche Computer der Firma wird erlangt
3. Versucht, aus der Büroumgebung auf das Leitsystem zu gelangen
   ⇨ Die Netze waren gut getrennt, Misserfolg



Versuch 1- Zugang via Büronetz auf Leitsystem

Zugang über den Fernzugriff

1. E-Mail oder Datenträger mit versteckter Schadsoftware im Anhang oder einem Link wird unter dem Vorwand, diesen bitte sofort (also via Pikettlaptop) zu öffnen versendet. Nun kann beispielsweise die Tastatur oder der Bildschirm des Pikettlaptops mitgelesen werden.
2. Mitlesen der Zugangsdaten während dem Einloggen ins Leitsystem, z.B. durch eine falsche Störungsmeldung an den Pikett, um ein Einloggen in die Systeme zu erwirken.
3. Eigene Fernverbindung aufs Leitsystem herstellen ➔ ERFOLG



Versuch 2 - Zugriff über den Fernzugriff

Der «Blackout»-Hackerangriff im Detail erklärt:
srf.ch/kultur/wissen/ein-hack-und-der-strom-ist-weg

Welche Massnahmen kann der Brunnenmeister in diesem Fall treffen?
Viele der erwähnten Schwachstellen scheinen auf den ersten Blick technischer Natur. Dennoch gibt es Möglichkeiten, wie der Brunnenmeister der Bedrohung aktiv entgegentreten kann.

- Bewusstsein für Social Engineering (Manipulation von Personen) aufbauen. Denn leider wollen einem nicht alle nur Gutes.
  - Skeptisch bleiben bei E-Mails
  - Sich nicht unter Druck setzen lassen
  - Niemals fremden Personen den Zugriff auf das System gewähren oder Benutzterdaten überlassen
    ⇨ melani.admin.ch/socialengineering
- Unberechtigten Personen den Zugang zu den Systemen verwehren
- Benutzerverwaltung
  - Separates Passwort für jeden Account
  - Keine Steuerung ab Fernwartung zulassen, wenn betrieblich nicht nötig
  - Die aktuellsten Empfehlungen der MELANI (Melde- und Analysestelle Informationssicherung) befolgen
    ⇨ melani.admin.ch/verhaltensregeln
- Pikettlaptop nur für technische Anwendungen verwenden, wenn möglich keine Mails darauf bearbeiten und keine USB-Sticks einstecken.
  ⇨ Mit der Informatik die Möglichkeiten besprechen
- Mobile Geräte vor Diebstahl oder unbefugtem Benutzen durch Dritte schützen.
  ⇨ Fällt ein mobiles Gerät in die Hände eines Dritten, muss sichergestellt sein, dass dieser mit dem Gerät keinen Zugriff auf sensible Systeme erhält.
- Zwei-Faktor-Authentifizierung (mit SMS-Code, Codekarte oder App, wie beim E-Banking bekannt) für den Fernzugriff verwenden. Diese Massnahme erhöht die Hürde für einen Angreifer bereits wesentlich.
  ⇨ Falls nicht vorhanden, mit der Informatik die Möglichkeiten besprechen

Fazit
Der Fall zeigt auf, dass die IT-Sicherheit nicht an einzelne Systeme gebunden ist. Es muss immer die gesamte Systemlandschaft betrachtet und analysiert werden.

Büronetze sind grundsätzlich als unsicher einzustufen, da viel mit fremden Daten gearbeitet wird (E-Mail, USB-Sticks, Recherchieren im Internet) Wichtige Systeme wie Leitsysteme sollten deshalb keinen direkten Zugang zu diesen haben.

Auf Geräte, welche für den Betrieb von sensiblen Systemen benutzt werden, sollten das Empfangen von E-Mails, das Surfen im Internet und das Benutzten von USB-Sticks möglichst vermieden werden, um das Risiko einer Virusinfektion zu minimieren.

Zudem sollte, wenn immer möglich eine Zwei-Faktor-Authentifizierung verwendet werden. Diese erhöht die Hürde für Hacker massiv.

4.2 Beispiel 2 - Erpressungen durch Verschlüsseln der Daten (Ransomware)

«
Die Schadsoftware «Wanna Cry» hat Hunderttausende von Computern lahmgelegt. Viele Firmen sind betroffen. Was ist passiert, und wie können Sie sich schützen? Die wichtigsten Antworten im Überblick.
»

Neue Zürcher Zeitung
nzz.ch/wirtschaft/wanna-cry

Michael Schilliger, Christian Steiner
15.5.2017, 17:00 Uhr

An der Bahnstation in Chemnitz sieht man die Folgen des Virus «Wanna Cry» für die Deutsche Bahn. (Bild: P. Goetzelt / Keystone)

Dilemma in der IT-Sicherheit (Quelle: Neue Zürcherzeitung, nzz.ch/wirtschaft/wanna-cry)

Einer der bekanntesten Verschlüsselungstrojaner ist wohl „WannaCry“ der im Frühjahr 2017 weltweit Schlagzeilen machte. Diese Art von Schadsoftware verschlüsselt die lokalen Festplatten und über USB oder Netzwerk verbundene Laufwerke, so dass diese für den Benutzer unbrauchbar werden. Das Opfer wird anschliessend zu einer Lösegeldzahlung aufgefordert, um den Schlüssel für die Entschlüsselung der Daten zu erhalten.

«WannaCry» im Detail erklärt:
wikipedia.org/wiki/WannaCry

Welche Massnahmen kann der Brunnenmeister in diesem Fall treffen?
Diese Art der Cyberkriminalität ist eher neu, jedoch bereits weitverbreitet. Hier die wichtigsten Gegenmassnahmen um dieser Bedrohung vorzubeugen:

- Wichtige Daten sollten auf zwei unabhängigen Systemen gesichert werden. Eine Kopie sollte immer offline sein, so dass diese bei einem Vorfall nicht mitverschlüsselt und somit unbrauchbar gemacht werden.
  ⇨ Beim Systemlieferanten nachfragen, wie die Datensicherung gelöst wurde.
- Vorsicht bei verdächtigen E-Mails. Meistens wird Schadsoftware über E-Mails versendet. Befolgen Sie keine Anweisungen im Text, öffnen Sie keinen Anhang und folgen Sie keinen Links.
- Halten Sie ihre Geräte und Systeme auf dem neusten Stand. Gerade Geräte für die Sie selber verantwortlich sind.
  ⇨ Stellen Sie für technische Systeme sicher, dass diese regelmässig gewartet werden. Definieren Sie, wann, wie und durch wen Updates vorgenommen werden.

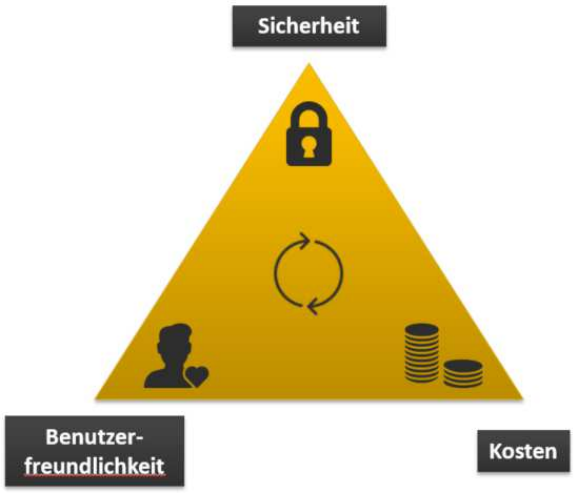
Detaillierte Tipps sind unter folgendem Link zu finden:
melani.admin.ch/Ransomware

Fazit
Sind alle wichtigen Daten zuverlässig gesichert, ist die Gefahr einer Erpressung durch Datenverschlüsselung gebannt. Es muss einzig sichergestellt werden, dass die Daten innert nützlicher Frist auch wieder zur Verfügung stehen.

5 Massnahmen

5.1 Dilemma in der IT-Sicherheit

Ein Höchstmass an Sicherheit wird in der Realität auch immer massive Einschränkungen für den Benutzer mit sich bringen, was eine tiefe Effizienz zur Folge hat. Zudem ist Sicherheit mit Kosten verbunden.



Dilemma in der IT-Sicherheit

Absolute Sicherheit kann niemals erreicht werden. Das Optimum muss immer aufs Neue gesucht werden.
Die Meinung des Brunnenmeisters ist dabei sehr wichtig, denn er kennt den Schutzbedarf (Anforderungen aus Sicht Betrieb) seiner Systeme und Daten am besten und kann somit dazu beitragen, dass nur Massnahmen umgesetzt werden, die dem Gefahrenpotential angepasst sind.

Massnahmen braucht es nur, wenn die Gefahr ein Problem darstellt.

- ⇨ Man darf sich auch **bewusst** gegen eine Massnahme entschieden

Man sollte jedoch stets an folgenden an «Murphy's Law» angelehnten Leitsatz denken:

«
Ein Ausfall kommt immer im denkbar schlechtesten Moment und selten allein.
«

5.2 Massnahmen des Brunnenmeisters

Um identifizierte Gefahren zu reduzieren, können Massnahmen ergriffen werden, welche die Schwachstellen schliessen und so das Gefahrenpotenzial minimieren. Nachfolgend sind die wichtigsten Massnahmen zur Steigerung der IT-Sicherheit nochmals zusammengefasst, die auch durch den Brunnenmeister umgesetzt werden können.

1. Vermeiden von E-Mails, surfen im Internet und arbeiten mit USB-Speicher. Diese sind die häufigsten Quellen von Schadsoftware.
   - Bei Büroarbeiten kann darauf nur schwer verzichtet werden, nicht aber bei Arbeiten an technischen Systemen.
     ⇨ Auf Geräten mit Fernzugriffen auf wichtige Systeme sollte darauf verzichtet werden.
2. Die Systeme aktuell halten
   - Sicherheitsupdates möglichst zeitnah installieren.
     ⇨ Gerade die privaten und mobilen Geräte sind in der Verantwortung der Brunnenmeister
3. Pflichtbewusster Umgang mit Benutzerdaten
   - Keine allgemeinen Systembenutzer, sondern personifizierte Benutzer
   - Nie das gleiche Passwort mehrmals verwenden und Passwörter regelmässig ändern
   - Sicherstellen, dass bei Abgängen oder Funktionswechseln die Zugriffe auch wieder entfernt werden.
   - Passwort nicht aufschreiben, evtl. „Passwortsafe“ mit starkem Masterpasswort verwenden
4. Bewusstsein für Social Engineering (Manipulation von Personen) aufbauen. Denn leider wollen einem nicht alle nur Gutes.
   - Skeptisch bleiben bei E-Mails
   - Sich nicht unter Druck setzen lassen
   - Niemals fremden Personen den Zugriff auf das System gewähren oder Benutzerdaten überlassen
5. Geräteverlust führt nicht zu einem ungewollten Systemzugriff
   - Kein Autologin in die Systeme (Passwörter nicht speichern)
   - Internes Vorgehen für die Sperrung bei Geräteverlust ist klar
6. Regelmässiges Backup der Daten auf einen externen und offline aufbewahrten Datenträger (z.B. externe USB-Festplatte) an einem anderen Ort
   - Tipp für Zuhause, aber auch sicherstellen, dass die für die Wasserversorgung wichtigen Systeme und Daten solche Kopien erhalten.
7. Empfehlungen MELANI beachten (Melde- und Analysestelle Informationssicherung)

5.3 Operative Massnahmen im Allgemeinen

Zum Schluss eine kurze Übersicht über allgemeine operative Massnahmen in der IT-Sicherheit für Interessierte. Es soll die Vielfalt aufzeigen und kann allenfalls als Leitfaden bei einem Gespräch mit einem Systemlieferanten dienen.

Technik

- Einsetzen von Antivirus-Software und einer Software-Firewall auf Endgeräten
- Backups, periodisch auch auf externe und vom System getrennte Datenträger
- Sensible Daten verschlüsseln und vor unbefugtem Zugriff schützen. Wichtig bei mobilen Geräten
- Zonenkonzepte und einheitliche Fernzugriffe IT-Verantwortung
- Firewalls / IPS (Intrusion Prevention System), Datennetze sichern
- Protokollieren, loggen und zentral alarmieren
- Bauliche Massnahmen, z.B. Zutritt etc.
- Erhöhen der Verfügbarkeit durch Redundanzen, Batterieversorgung, etc.
- Restriktive Konfiguration, nur freischalten was auch benötigt wird
- Aktive Inhalte im Browser deaktivieren (Scripts, Makros etc.)
- Diversifikation: nicht Mainstream Produkte verwenden (für alternative Produkte existiert meist weniger Schadsoftware)

Organisation

- Schulung der Mitarbeiter (Bewusstsein für die IT-Sicherheit erhöhen)
- Patchmanagement: Wer macht bei welchem System welches Update?
- Saubere Benutzerverwaltung: Rollen/Passwörter
- Dokumentieren der Einzelsysteme und der Systemlandschaft
- Berücksichtigen der gängigen Normen und Empfehlungen

Detaillierte Infos sind unter folgendem Link zu finden:
melani.admin.ch/Merkblatt IT-Sicherheit für KMUs

6 Fazit

Der Informatik werden immer mehr Aufgaben anvertrauen weshalb sie immer wichtiger für die Unternehmen wird. Somit steigen auch die Anforderungen an den Endbenutzer und seine Pflichten werden stets umfangreicher. Dies wird durch vermehrte Angriffe auf die «Schwachstelle» Endbenutzter leider noch verstärkt.

- ⇨ **Die Endbenutzer der Systeme sind zentraler Bestandteil der IT Sicherheit** und können einen grossen Beitrag leisten.

Vielen Dank für Ihren Einsatz!

Zum Verfasser: Christian Rentsch, Sollberger Ingenieure GmbH
Seit über 25 Jahren realisiert Sollberger Ingenieure GmbH moderne Lösungen im Bereich der Netzleittechnik. Der grosse Erfahrungsschatz sowie das profunde und topaktuelle Wissen zählen zu den Hauptmerkmalen unseres Ingenieurbüros. Wir beraten, planen und realisieren absolut lieferantenneutral - vom Sensor bis auf den Bildschirm. Somit können wir Ihnen in jedem Fall die bestmögliche Lösung für Ihre individuellen Bedürfnisse garantieren.

Die IT-Sicherheit ist in unseren Projekten ein fixer Bestandteil. Unsere Erfahrung ermöglicht es uns, das Thema in allen Projektphasen und aus unterschiedlichen Perspektiven zu betrachten und passende Lösungen zu erarbeiten.

Als Techniker in Automation hatte ich schon seit jeher mit Steuerungen und Datennetzen zu tun. Mit dem Abschluss des CAS Network & Security 2016 an der Berner Fachhochschule konnte ich meine Vorkenntnisse im Bereich der IT Security festigen und vertiefen. Dies hat mir geholfen, die technischen Details zu verstehen und somit Problemstellungen lieferantenunabhängig zu erfassen und zu lösen.