Von Versorgungs- und Informationssicherheit

Autor(en): **Collenberg, Gian / Nuderscher, Jürgen**

Objekttyp: **Article**

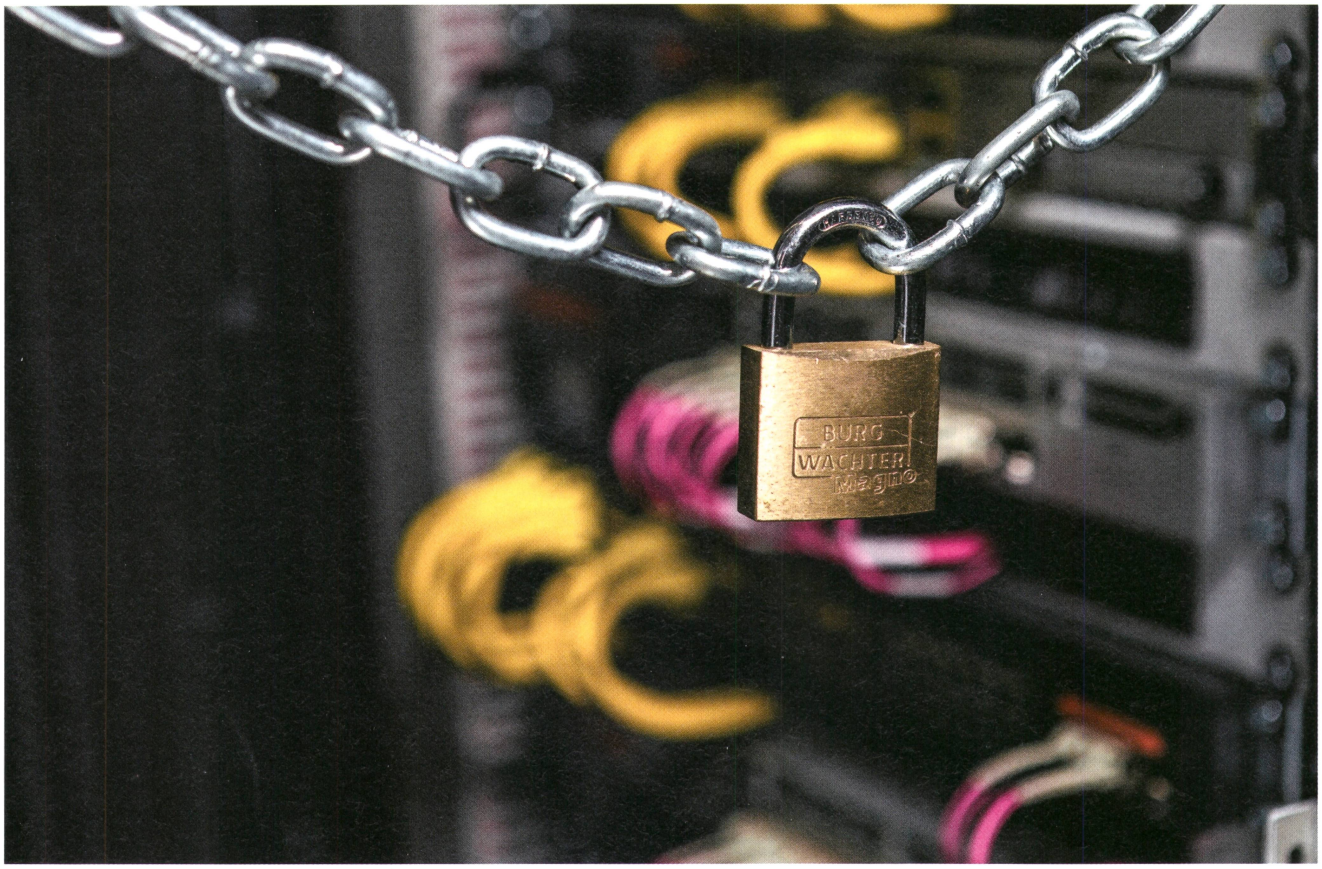
Zeitschrift: **Bulletin.ch : Fachzeitschrift und Verbandsinformationen von Electrosuisse, VSE = revue spécialisée et informations des associations Electrosuisse, AES**

Band (Jahr): **109 (2018)**

Heft 11

PDF erstellt am: **10.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-857014



Von Versorgungs- und Informationssicherheit

IT-Strategie | Die primäre Absicht von Energieversorgungsunternehmen ist die Gewährleistung von Versorgungssicherheit für ihre Kunden. Mit der zunehmenden Vernetzung und Digitalisierung erweitert sich jedoch das Pflichtenheft für EVUs: Sie müssen auch die Sicherheit und den Schutz von Kundendaten garantieren. Individuelle IT-Strategien sind daher unerlässlich.

TEXT GIAN COLLENBERG, JÜRGEN NUDERSCHER

Informationssicherheit ist Chefsache. Es geht um Image und um das Vertrauen von Kunden. Beinahe täglich erscheint ein neuer Bericht über Informations- und Datensicherheit. Neue gesetzliche Vorgaben, Branchenempfehlungen und verschiedenste Standards, wohin das Auge reicht. Für EVUs sind dies schwierige Zeiten. Steht man hier erst vor der Qual der Wahl oder doch schon in der Pflicht? Wie sicher soll man in welchem Bereich sein? Wie kann man sich überhaupt schützen? Wie geht man vor, und welche Hilfsmittel können einen dabei unterstützen?

Das Thema Sicherheit ist heutzutage überall anzutreffen. Dabei wird jedoch eine Vielzahl an Begriffen verwendet, deren Bedeutung nicht immer ganz klar scheint. Um sich effektiv zu schützen, ist es aber zentral, die relevanten Bereiche in Bezug auf Sicherheit zu kennen.

Datenschutz regelt den Schutz personenbezogener Daten. Er basiert auf dem schweizerischen Datenschutzgesetz respektive der EU-Datenschutzverordnung. Datenschutz kann als digitaler Personenschutz betrachtet werden. Das schweizerische Datenschutzgesetz wird aktuell in zwei Etappen überarbeitet und mit der Datenschutzgrundverordnung der EU konform gemacht.

Datensicherheit beschreibt Anforderungen und Massnahmen, um die Sicherheit von Daten zu gewährleisten. Hierfür müssen zuerst der Schutzbedarf respektive die Kritikalität der

Bilder: Swibi AG

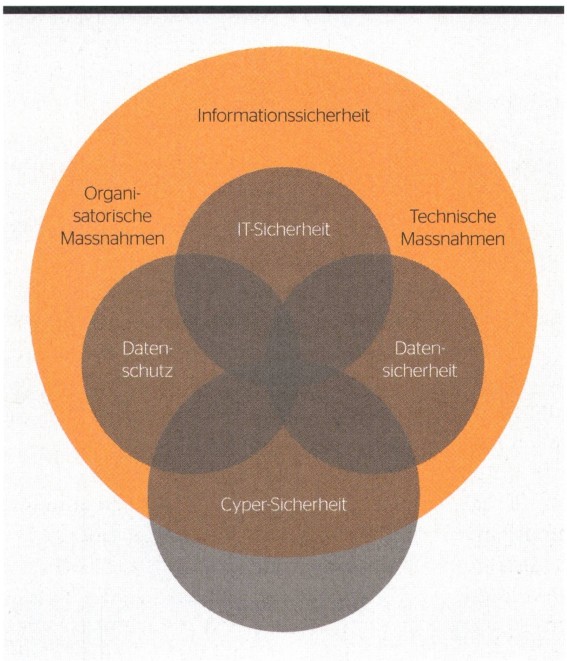
Daten eruiert werden. Generell versteht man unter Datensicherheit sämtliche technischen Aspekte, die dem Schutz aller möglichen Arten von Daten dienen. Dabei werden in Bezug auf Bedrohungen (zum Beispiel Verlust und Manipulation) Ziele wie Verfügbarkeit, Integrität und Vertraulichkeit verfolgt.

Informationssicherheit ist ein Überbegriff für Sicherheit und Schutz aller Informationen in digitalen und nicht-digitalen Systemen, also zum Beispiel auf Papier oder in Form von Know-how. Die Informationssicherheit betrifft digitale und nicht-digitale Systeme sowie komplette Organisationen. Entsprechende Vorgaben und betriebliche Organisation gewähren den Schutz und die Sicherheit sämtlicher Unternehmensdaten, und zwar gemäss den Schutzzielen «Vertraulichkeit», «Integrität» und «Verfügbarkeit». In Zeiten der Digitalisierung kommt daher dem Schutz von Informationssystemen durch IT-Sicherheit grosse Bedeutung zu. Dabei liegt der Fokus nicht nur auf der technischen, sondern auch der menschlichen Komponente.

Cyber-Sicherheit erweitert die IT-Sicherheit auf den gesamten Cyber-Bereich, zum Beispiel auf das Internet der Dinge (IoT, vom englischsprachigen Internet of Things). Darunter versteht man ein Netzwerk, welches virtuelle und physische Gegenstände respektive Geräte – oft auch cloud-basiert – miteinander vernetzt. Es wird darum auch das «Allesnetz» genannt. Cyber-Sicherheit befasst sich somit unter anderem auch mit der Sicherheit dieser globalen Infrastruktur, bei der es sich oft auch um Geräte ohne Bezug zu Informationen oder Daten handelt.

Sicherheit als permanenter Prozess

Die grundsätzliche Verantwortung zum Eigenschutz liegt bei jedem Unternehmen. So steht es auch im Vorwort des IKT-Minimalstandards des Bundesamtes für wirtschaftliche Landesversorgung (BWL), welcher Ende August 2018 erschienen ist.[1] Die Verantwortung für die Informationssicherheit liegt beim Management und kann nicht delegiert werden. Ein Patentrezept gibt es dafür allerdings nicht. Jedes Unternehmen muss den für sich geeigneten Weg finden. Das Wichtigste ist, damit anzufangen, denn «Sicherheit ist ein Prozess, kein Produkt» [2].



Bereiche der Informationssicherheit.

Mit welchen Gefahren müssen Unternehmen heutzutage rechnen?

Um den Einstieg in dieses Thema zu erleichtern, stehen verschiedene Hilfsmittel zur Verfügung. Als guter Startpunkt sei hier auf den Cyber-Security-Schnelltest für KMU des Dachverbands ICT Switzerland verwiesen.[3] Mittels eines Fragebogens werden die wichtigsten Themenbereiche abgefragt. Anhand der eigenen Antworten erhält man direktes Feedback zu den jeweiligen Bereichen in Bezug auf das eigene Unternehmen sowie Verweise zu weiterführenden Quellen.

Der Bund unterstützt Unternehmen in der Schweiz beim Schutz vor Cyber-Risiken. Das BWL hat einen Minimalstandard zur Verbesserung der IKT-Resilienz [1] entwickelt. Dieser richtet sich insbesondere an Betreiber kritischer Infrastrukturen,

ist aber grundsätzlich für jedes Unternehmen anwendbar und frei verfügbar. Anhand der fünf Funktionen des Nist Framework Core (Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen) werden Aufgaben zur Umsetzung des IKT-Minimalstandards beschrieben.

Weltweit existiert eine Vielzahl von verschiedenen Standards und Informationsquellen zum Umgang mit Informationssicherheit:

- Cobit 5 ist ein umfassendes Regelwerk von weltweit anerkannten Prinzipien, Praktiken, analytischen Instrumenten und Modellen, die Unternehmen helfen, geschäftskritische Fragestellungen im Zusammenhang mit Governance sowie dem Management von Informationen und Technologie wirksam anzugehen.[4]
- Die vier IT-Grundschutzkataloge des BSI (Bundesamt für Sicherheit in der Informationstechnik) erläutern die Grundlagen zur Erstellung eines IT-Sicherheitskonzepts. Der Aufbau eines Informationssicherheits-Managementsystems (ISMS), die Vorgehensweise nach IT-Grundschutz, die Erstellung einer Risikoanalyse für hohen und sehr hohen Schutzbedarf sowie eines Notfallmanagements werden beschrieben.
- Die ISO/IEC-27000-Reihe bietet ein sehr weit gefasstes Informationssicherheits-Framework, das auf Organisationen aller Arten und Grössen angewendet werden kann. Man kann es als Äquivalent der Informationssicherheit zum Qualitätsstandard ISO 9000 sehen. Nach diesem Standard können sich Unternehmen zertifizieren lassen, um auch den Nachweis der Sicherheit gegenüber Dritten zu erbringen. Aktuell besteht als EVU zwar noch keine Verpflichtung zu einer solchen Zertifizierung, doch erlangt man einen Nachweis, der die Einhaltung gewisser Schutzmassnahmen beweist.

Faktoren der Informationssicherheit

Informationssicherheit beruht zu je einem Drittel auf technischen, organisatorischen und menschlichen Faktoren. Obwohl die technischen Risiken von IT-Systemen ein wichtiger Aspekt der Informationssicherheit sind, sollte ein Unternehmen seinen Fokus nicht auf diesen Teil der Risiken beschränken oder gar die IT-Abteilung als alleinigen Risikoträger definieren.[5] IT-Sicherheit sollte in sinnvoller Relation zum Schutzbedarf stehen (Angemessenheit), darf die Geschäftstätigkeit nicht behindern und muss von allen als Notwendigkeit verstanden werden (Akzeptanz). Eine sichere IT, etablierte Sicherheitsprozesse und eine Sensibilisierung der Mitarbeitenden verringern die Verwundbarkeit und schaffen eine bessere Verfügbarkeit sowie einen Wettbewerbsvorteil und Kundenzufriedenheit.

Aktuelle Bedrohungslage

Doch mit welchen Gefahren müssen Unternehmen heutzutage überhaupt rechnen? Eine allgemeine Aussage dazu ist schwierig, weil sich die Bedrohungslage laufend verändert. Dies zeigt auch ein Blick auf potenzielle Angreifer: Waren früher vor allem einzelne Hacker am Werk, agieren heute professionell organisierte Gruppen.

Das können einerseits Hackergruppen mit unternehmensähnlichen Strukturen sein, welche ihre Dienstleistungen auch Dritten anbieten und primär finanzielle Interessen verfolgen. Anderseits rüsten auch Staaten ihr IT-Arsenal und ihre Cyber-Armeen auf, um sich für einen Cyber-Krieg zu wappnen. Zwar können potenzielle Ziele mit umfassenden Schutzmassnahmen versuchen, die Hürde für einen erfolgreichen Angriff so hoch wie möglich zu setzen, eine hundertprozentige Sicherheit kann dennoch nie gewährleistet werden.

Besondere Aufmerksamkeit muss den sogenannten Crypto-Trojanern oder Ransomware gewidmet werden. Diese verschlüsseln in einem infizierten System gezielt Dateien und erpressen den User. Gegen Bezahlung eines Lösegelds (oftmals in Kryptowährung) werden die Dateien wieder entschlüsselt. Die Verbreitung solcher Schadprogramme erfolgt meistens via E-Mail. Diverse Unternehmen wurden bereits Opfer davon.

Am Beispiel Ransomware zeigt sich, dass ein effektiver Schutz alle Bereiche abdecken muss. Auf technischer Ebene ist der Einsatz von Systemen zur Erkennung von gefälschten E-Mails respektive von unsicheren Anhängen sowie der Einsatz aktueller Antivirenprogramme Pflicht. Zusätzliche Systeme können helfen, Ransomware anhand ihres Verhaltens (zum Beispiel Zugriffe auf das Speichersystem) frühzeitig zu erkennen und zu isolieren.

Da Ransomware in der Regel erst aufgrund einer Aktion eines Users ausgeführt wird, darf der Faktor Mensch nicht ausser Acht gelassen werden. Hier helfen nur die regelmässige Aufklärung und Sensibilisierung aller Mitarbeiter. Damit diese nicht auf sich alleine gestellt sind, muss auf organisatorischer Ebene definiert werden, an welche Stelle sich skeptische Mitarbeitende bei einem Verdachtsfall wenden können.

Tritt dennoch ein Befall ein und Unternehmensdaten werden verschlüsselt, bleibt als letzte Massnahme der Rückgriff auf gesicherte Datenbestände. Dank eines klar definierten Backup-Konzepts steht eine Datensicherung in möglichst kurzem Intervall zur Verfügung, welches zeitnah zurückgespielt werden kann, damit der Datenverlust minimiert wird.

EVUs als attraktive Ziele

Jedes Unternehmen sollte sich die Frage stellen, was es für mögliche Angreifer als Ziel attraktiv macht. Ein Energieversorgungsunternehmen ist hauptsächlich durch den Betrieb seines Versorgungsnetzes exponiert. Daneben besitzen EVUs aber auch eine Vielzahl an Kundendaten.

Haushaltskunden können ihren Stromversorger nicht auswählen und damit auch nicht, welchem Unternehmen persönlichen Daten anvertraut werden müssen. Umso mehr erwartet jeder Kunde mit gutem Recht, dass sein Energieversorger sorgfältig mit seinen Daten umgeht. Vielen Kunden ist aber nicht bewusst, welche Daten ihr EVU überhaupt von ihnen gespeichert hat. Sicherlich handelt es sich dabei um die zur Abrechnung nötigen Personenangaben und um allfällige Zahlungsinformationen; eventuell auch bereits um Kreditkartendaten zur Bezahlung der Stromrechnung oder von Einkäufen im Online-Shop des EVU. Kreditkarteninformationen sind begehrte Daten, doch auch Kontaktangaben wie E-Mail-Adressen oder Telefonnummern werden gerne zweckentfremdet.

Durch die Verbreitung von Smart Metern und das Aufzeichnen eines Lastprofils vergrössert sich die Datenmenge jedes Kunden. Ein viertelstündiges Lastprofil lässt Rückschlüsse auf

deren Verhaltensweisen zu. Gelangen solche Informationen in die falschen Hände, sind dem Missbrauch Tür und Tor geöffnet. Zum Beispiel kann ein Einbrecher erkennen, wann seine potenziellen Opfer in der Regel am Abend nach Hause kommen. Neben den möglichen Schäden für die Kunden entsteht durch ein solches Datenleck auch ein riesiger Imageschaden für das Unternehmen. Umso wichtiger ist daher, als Unternehmen seine Kundendaten ausreichend zu schützen.

Eine der grössten Gefahren für ein EVU stellt ein direkter Angriff auf das Versorgungsnetz dar. Erlangt ein Angreifer die Kontrolle über das Stromnetz, kann er dank intelligenter Zähler mit Steuerungsfunktion gezielt einzelne Haushalte oder dank verknüpfter Gebäudetechnik sogar einzelne Geräte steuern. Auf technischer Seite sind daher umfangreiche Schutzmassnahmen nötig. Für Steuerungssysteme sind viele Massnahmen wie eine Trennung der Netzwerkbereiche und strikte Zugriffsregeln bereits weitreichend umgesetzt und in Branchendokumenten beschrieben.[6]

Mit einem Smart-Meter-Rollout erhöhen sich auch die Gefahren. Infolge der nötigen Kommunikationsanbindung wird das Netzwerk des EVU bis in die Häuser verlängert. Ein Smart Meter muss dabei wie jedes andere Netzwerkgerät behandelt werden. Dazu gehören sowohl das Ändern von Standardpasswörtern als auch das regelmässige Aktualisieren der Software.

Die Definition dieser Sicherheitsprozesse ist bereits beim Beginn des Rollouts zentral. Je mehr Geräte im Feld installiert sind, desto aufwendiger ist eine nachträgliche Implementation. Ein wesentlicher Aspekt ist beim Smart-Metering die Datenverschlüsselung zwischen Zähler und Datenkonzentrator. Der Einsatz komplexer Verschlüsselungsverfahren hilft, die Kommunikation zwischen Smart Meter und Rechenzenter zu sichern und damit unerlaubte Manipulation oder Kontrolle der Smart Meter zu unterbinden.

Die Managementaufgabe «Informationssicherheit» muss wahrgenommen und Verantwortlichkeiten müssen definiert werden. Rollen und Gremien der Daten-Governance in der Energiebranche werden unter anderem im Bericht «Data Policy in der Energiebranche» [7] praxisnah behandelt. Den Mitarbeitenden muss bewusst gemacht werden, dass ihre Zugangsdaten zu den wichtigsten und schützenswertesten Informationen gehören. Mittels Benutzername und Passwort erhält jeder, der sie kennt, die damit verknüpften Zugriffsrechte. Das Ziel muss daher sein, sicherzustellen, dass die Mitarbeitenden mit den Fähigkeiten und notwendigen Kenntnissen ausgestattet sind, um die Werte der Organisation zu unterstützen.

Referenzen

[1] «Minimalstandard zur Verbesserung der IKT-Resilienz», Bundesamt für wirtschaftliche Landesversorgung BWL, 2018.
[2] Bruce Schneier, 2000.
[3] ictswitzerland.ch/themen/cyber-security/check/
[4] www.isaca.org/COBIT/Pages/COBIT-5-german.aspx
[5] «Merkblatt Informationssicherheit für KMUs», Melde- und Analysestelle Informationssicherung Melani, Mai 2018.
[6] «Handbuch Grundschutz für ‹Operational Technology› in der Stromversorgung», Verband Schweizerischer Elektrizitätsunternehmen VSE, Juli 2018.
[7] www.strom.ch, im Download-Bereich.

Autoren

Gian Collenberg ist IT-Sicherheitsverantwortlicher bei der Swibi AG.
→ Swibi AG, 7302 Landquart
→ gian.collenberg@swibi.ch

Jürgen Nuderscher ist Informationssicherheits-Manager bei der Swibi AG.
→ juergen.nuderscher@swibi.ch

RÉSUMÉ

Sécurité d'approvisionnement et de l'information

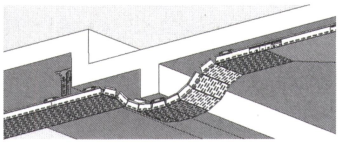
Stratégie informatique

La première intention des entreprises d'approvisionnement en énergie est de garantir la sécurité d'approvisionnement pour leurs clients. Toutefois, avec l'interconnexion et la digitalisation croissantes, le cahier des charges des EAE s'élargit : elles doivent aussi garantir la sécurité et la protection des données de leurs clients. Des stratégies informatiques individuelles sont donc indispensables.

La sécurité de l'information repose sur un tiers de facteurs techniques, un tiers de facteurs organisationnels et un tiers de facteurs humains. Bien que les risques techniques des systèmes informatiques représentent un aspect important de la sécurité de l'information, une entreprise ne devrait pas se limiter à cette partie des risques, ni encore moins désigner le service IT comme seul porteur de risques. La sécurité informatique devrait refléter le besoin de protection (adéquation), ne doit pas entraver l'activité commerciale et doit être comprise par tous comme une nécessité (acceptation). Une IT sûre, des processus de sécurité établis et une sensibilisation des collaborateurs réduisent la vulnérabilité, engendrent une meilleure disponibilité, créent un avantage concurrentiel et permettent de satisfaire les clients.

Toute entreprise devrait se poser la question suivante : en quoi peut-elle être une cible attractive pour les attaquants potentiels ? Une entreprise d'approvisionnement en énergie est exposée principalement à travers l'exploitation de son réseau d'approvisionnement. Mais les EAE sont également en possession d'une multitude de données clients.

La tâche de management de la « sécurité de l'information » doit être assumée et les responsabilités définies. Il faut faire prendre conscience aux collaborateurs que leurs données d'accès font partie des informations les plus importantes et les plus sensibles. L'objectif doit donc être de garantir que les collaborateurs soient dotés des capacités et des connaissances nécessaires pour soutenir les valeurs de l'organisation. **MR**



die platzsparenden Kabelführungen

Mit den modernen LANZ Kabelführungen montieren Sie sauber und platzsparend:

- **C-, U-, L- und G-Kanäle**
  ab 20 mm hoch
  Für kleine Kabelmengen. Preisgünstig. Platzsparende Einhängemontage/Schnappmontage.
- **LANZ Flachgitter**
  nur 22 mm hoch
  20–50 cm breit. Für Steigleitungen in EFH, MFH, Gewerbe- und Industriebauten. Einfache 1-Dübel-Montage.
- **LANZ Flachbahnen**
  nur 70 mm hoch fertig montiert
  10–40 cm breit. Verbindung schraubenlos.
  Bündig an Decken, und flachbündig (!) an Wänden.
- **LANZ Multibahnen**
  10 Multibahnen gestapelt nur 170 mm
  10–60 cm breit. Verbindung schraubenlos.
- **LANZ Teleskop-Deckenstützen**
  20–200 cm hoch, mm-genau höhenverstellbar
  Platzsparend an allen Decken.

Verlangen Sie die BIM-kompatiblen Dateien von LANZ für die Kabelführung. Rufen Sie an! 062/388 24 24.

8

lanz oensingen ag

CH-4702 Oensingen
Südringstrasse 2
www.lanz-oens.com
info@lanz-oens.com
Tel. ++41/062 388 21 21
Fax ++41/062 388 24 24

Verbandsweisheit Nr. 6

Wenn die Autos brauchen Strom, oder gar fahren autonom, helfen wir dabei zu wissen, wie sie wo auch laden müssen.

#emobile #anschlussfinden
#elektroauto

electro suisse

VSE AES electro suisse

F-46

REELTECH
Leuchten-Lifte

Difficile à joindre?

Les mini-dispositifs de soulèvement Reeltech mettent les luminaires domestiques et de bureau à hauteur de travail

Sans entretien
Ne nécessitent aucun contrôle régulier

Sécurité maximale
Le nettoyage et la maintenance des luminaires hors tension

Particullèrement compact
Les dimensions rédultes et la charge minimale

Convient aux commandes d'éclairage
Versions multicontact pour exigences complexes par ex. les commandes DALI ou le courant de secours

Mini Type
Standard et Multicontact

- Poids de levage 2-5 / 2-6 kg
- Abaissement 15 / 7 m
- Corde de suspension simple/double
- Hauteur de levage à réglage continu
- Télécommandable
- **Multicontact:** 4 contacts auxiliaires 6A 230V

Télécommande radio RCU

- 999 lifts programmable
- 433.92 MHz, jusqu'à 100 m portée
- Couplage mixte possible

Plus d'informations sur notre lift luminaires version mini-type

demelectric 50 1968 – 2018

Représentation pour la Suisse:

Demelectric SA • Steinhaldenstrasse 26 • 8954 Geroldswil
téléphone +41 43 455 44 00 • fax +41 43 455 44 11
info@demelectric.ch • www.demelectric.ch

Achat auprès des grossistes. Demandez notre documentation.