electro suisse

Cybersecurity

bei kleinen und mittleren Elektrizitätsversorgungsunternehmen

Electrosuisse hat bei kleinen und mittleren Elektrizitätswerken untersucht, wie es um deren Fähigkeit steht, den Bedrohungen des digitalen, global vernetzten Zeitalters zu begegnen.

Autor Levente J. Dobszay

Bezugsquelle Electrosuisse, Luppmenstrasse 1, 8320 Fehraltorf
T: +41 44 956 11 11
www.electrosuisse.ch/cybersecurity

Inhalt

Hintergrund

Die immer noch oft anzutreffende Annahme, aus irgendwelchen Gründen nicht zum Ziel von Cyber-Attacken zu werden, macht Unternehmen zur besonders leichten Beute. Gerade bei Betrieben, die zur kritischen Infrastruktur gehören, kann dies verheerende Folgen haben. Der Hackerangriff auf die Wasserversorgung von Ebikon im November 2018 konnte glücklicherweise durch das im Herbst installierte Sicherheitssystem vereitelt werden. Aus der Tatsache, dass ein Unternehmen bisher noch keine Sicherheitsprobleme feststellen konnte, lässt sich vor allem in Anbetracht der oft weitgehend fehlenden Visibilität der Vorgänge im Netzwerk nicht automatisch darauf schliessen, dass es bisher alles richtiggemacht und noch nicht Opfer eines erfolgreichen Angriffs geworden ist. Es kann gut sein, dass der Feind sich bereits tief im System eingenistet hat und nur darauf wartet, loszuschlagen. Untersuchungen haben gezeigt, dass Infektionen mit Schadsoftware im Schnitt länger als ein Jahr unentdeckt bleiben. Davon zeugt auch der Spionagefall bei der Ruag. Immer mehr kleine und mittlere Unternehmen erkennen, dass auch sie für Cyber-Attacken weder zu klein noch zu wenig interessant sind.

Neue Risiken durch Vernetzung

Im Zuge der fortschreitenden Digitalisierung sehen sich immer mehr Bereiche der «Operational Technology» (OT), d.h. der Informationstechnologie (IT) für die Steuerung von Maschinen in industriellen Herstellungs- und Logistikprozessen, mit den Herausforderungen der digitalen Sicherheit konfrontiert. Infrastrukturen, die ursprünglich nie dafür konzipiert wurden, werden zunehmend mit der Aussenwelt vernetzt und sind dadurch auch digitalen Risiken ausgesetzt. Damit wird neben dem Nutzenpotenzial zugleich auch ein zusätzliches Gefahrenpotenzial erschlossen.

Bei der Konvergenz von OT und IT wachsen technisch verwandte Welten zusammen, die sich jedoch hinsichtlich der Sicherheitsprioritäten, Lebenszyklen und Sicherheitskulturen sowie auch in den aktuellen technischen Möglichkeiten für digitale Sicherheitsmassnahmen unterscheiden. Während die Schutzziele «Vertraulichkeit», «Integrität» und «Verfügbarkeit» in der Welt der klassischen IT in eben dieser Prioritätenfolge adressiert werden, sind die Prioritäten in der OT-Welt gerade umgekehrt. Hier steht in der Regel die Verfügbarkeit an oberster Stelle, während die Vertraulichkeit eine weit weniger wichtige Rolle spielt, weil die zu schützenden Daten sowie die diese Daten verarbeitende Hardware und Software nur einen geringen bis gar keinen Personenbezug aufweisen. Vertraulichkeit ist hier in erster Linie im Zusammenhang mit Industriespionage relevant.

Cybersecurity gewinnt zunehmend an bedeutung

Vor allem für Unternehmen der kritischen Infrastrukturen wie Energie- und Wasserversorgung ist das Management der digitalen Risiken von ganz besonderer und zunehmend existenzieller Bedeutung. Mit der Umsetzung der Energiestrategie 2050 wird durch den flächendeckenden Einsatz von «Smart Metern» das Thema Cybersecurity bis in die Haushalte und Betriebe der Stromkunden und der Betreiber von Photovoltaikanlagen getragen. Aber auch Fertigungsanlagen sowie Gebäudetechnik und -automation sind immer mehr den Bedrohungen der vernetzten digitalen Welt ausgesetzt.

Auch kleinere Elektrizitätswerke werden sich zunehmend bewusst, dass auch sie in den Fokus von Cyber-Attacken geraten und zum Zielobjekt in der globalen, digitalen Kriegsführung werden können. Ein einzelnes Werk für sich mag kein strategisches Ziel sein, alle auch noch so kleinen

Werke in der Summe sind es sehr wohl. Entsprechend ist kein Werk zu klein, um sich nicht mit mehrstufigen Schutzmassnahmen auf allen Ebenen gegen Cyber-Attacken zu schützen. Cybersecurity muss daher auf die Liste der Top-Prioritäten von Unternehmen der kritischen Infrastruktur! Dies ganz unabhängig von ihrer Grösse.

Cybersecurity Standards in der Schweiz

Als Ergebnis der vom Bundesrat 2012 beschlossenen Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) hat das Bundesamt für wirtschaftliche Landesversorgung BWL 2018 mit dem «Minimalstandard zur Verbesserung der IKT-Resilienz» (IKT-Minimalstandard) basierend auf dem NIST Cybersecurity Framework einen Standard publiziert und ein Bewertungstool für Unternehmen zur Beurteilung ihrer IKT-Resilienz bereitgestellt. Parallel dazu hat auch der Verband Schweizerischer Elektrizitätsunternehmen VSE das Handbuch «Grundschutz für Operational Technology (OT)» in der Stromversorgung publiziert. Dieses adressiert die Netzebenen 1 bis 4 (überregionale Verteil- und Übertragungsnetze) und Energieerzeugungsanlagen, welche bereits weitgehend durch digitale Systeme überwacht und gesteuert werden. Die darunterliegenden Netzebenen 5 bis 7 (regionale und lokale Verteilnetze und ihre Unterwerke) sind heute noch weniger digitalisiert und ein manueller Betrieb mit einer Bedienung vor Ort wäre im Notfall in der Regel immer noch möglich. Grundsätzlich sind die kleineren Elektrizitätsversorgungsunternehmen jedoch den gleichen Bedrohungen ausgesetzt wie die grossen und deren Cyber-Resilienz gewinnt mit der zunehmenden Digitalisierung, nicht zuletzt im Zuge der flächendeckenden Einführung von Smart Metering, stark an Bedeutung. Daher ist es sinnvoll, die im VSE Handbuch beschriebenen Empfehlungen in einer angepassten Weise auch auf die Netzebenen 5 bis 7 anzuwenden.

Electrosuisse Cybersecurity Quick Assessment

Electrosuisse wollte wissen, wie es um die «Cyber-Resilienz» bei kleinen und mittleren Elektrizitätswerken steht, und hat diese im Zeitraum September bis Dezember 2018 mit einem Cybersecurity Quick Assessment erhoben. Dafür wurden die einzelnen Themen des NIST Cybersecurity Frameworks zu Schlüsselelementen verdichtet und mit zusätzlichen Aspekten zu Budgetierung und Führungskennzahlen ergänzt. In einem ca. 2-stündigen Interview wurden die Betriebsleiter und IT- und OT- beziehungsweise Cybersecurity-Verantwortlichen von 30 Werken mit 4 bis 600 Mitarbeitern befragt. Nachweise wurden keine gefordert. Daher ist davon auszugehen, dass die Selbsteinschätzung der Teilnehmer als eher zu optimistisch einzustufen ist. Nichts desto trotz kann angenommen werden, dass die Verteilung der Maturitätsstufen der Realität entspricht, auch wenn die effektive Maturität tendenziell tiefer liegen dürfte. Die Unterscheidung zwischen kleinen und mittleren Werken wurde anhand der Anzahl Mitarbeiter vorgenommen, wobei Werke mit 60 Mitarbeitern und weniger als klein eingestuft wurden.

Als Fachverband möchte Electrosuisse einen Beitrag leisten, die allgemeine «Cyber-Resilienz» zu stärken. Mit Angeboten zu Prüfungen, Zertifizierungen, Schulungen und Beratungen sollen insbesondere jene Unternehmen mit Fachkompetenz und praxistauglichen Lösungen unterstützt werden, welche nicht über die nötigen personellen Ressourcen mit Fachwissen verfügen, um eine hinreichende Cybersecurity sicherzustellen.

Hauptbefunde Gesamterhebung

- Unvollständiges Asset Management.
- Zu wenig Risikobasiertheit bei Massnahmen und Budgetierung.
- Fokus primär auf Schutzmassnahmen.
- Cybersecurity oft Blindflug mangels Visibilität.
- Reaktionsbereitschaft, Notfallvorbereitung und -übung ungenügend.
- Lieferantenrisiken oft unbekannt und vernachlässigt.
- Mensch als grösste Schwachstelle zu wenig behandelt.
- Fehlende Fachkompetenz und Ressourcen.
- Cybersecurity kein geführter Prozess.

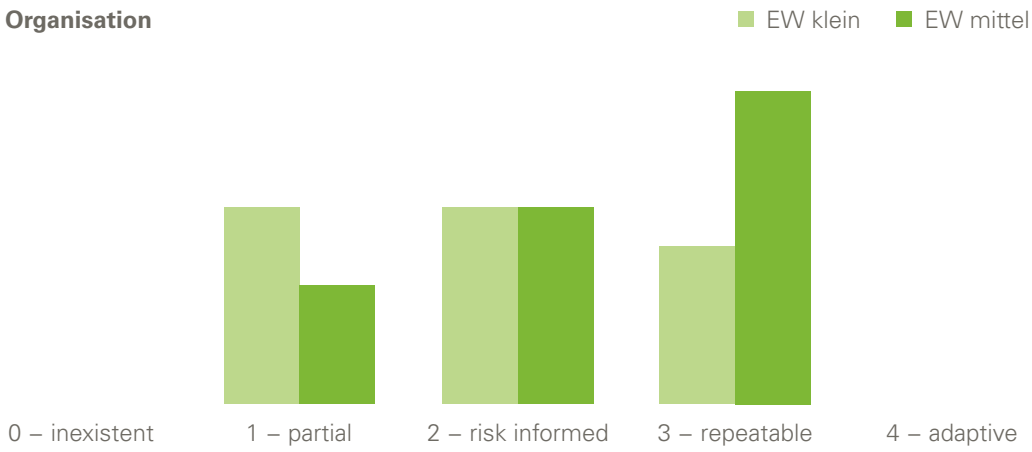
NIST Cybersecurity Framework Maturitätsstufen

Maturitätsstufe	Beschreibung
0 – inexistent	• Thema/Risiko ist nicht adressiert
1 – partial	• Risiken sind nur teilweise bekannt und Massnahmen werden nur partiell umgesetzt. • Risikomanagement ist nicht definiert, ad-hoc, oft nur reaktiv und nicht priorisiert.
2 – risk Informed	• Risiken sind bekannt, Massnahmen werden priorisiert, aber nicht systematisch umgesetzt. • Risikomanagement und Massnahmen sind definiert, aber noch nicht in der Organisation verankert.
3 – repeatable	• Risikomanagement ist in Standards und Richtlinien vollständig definiert und in der Organisation verankert. • Massnahmen sind auch als Prozesse beschrieben und werden systematisch umgesetzt.
4 – adaptive	• Risikomanagement wird auf Basis von Erfahrungen und Kennzahlen/Indikatoren regelmässig angepasst. • Massnahmen werden den Risiken und der Bedrohungslage laufend angepasst.

Untersuchungsergebnisse

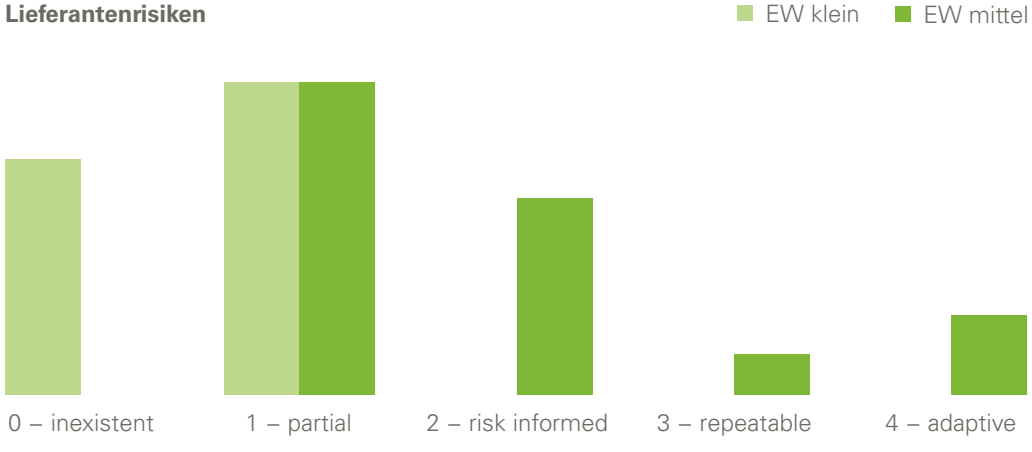
Erfreulich war festzustellen, dass Cybersecurity bei allen Werken mehr oder weniger thematisiert wird, auch wenn die Aufgaben bei den kleineren noch wenig systematisch angegangen werden. Die kleinsten Unterschiede zwischen kleinen und mittleren Werken zeigten sich bei der Organisation und den Verantwortlichkeiten betreffend der Cybersecurity, wobei hier auch bei einigen mittleren Werken noch Optimierungspotenzial besteht. Aufgaben, Kompetenzen und Verantwortlichkeiten für die Cybersecurity sind oft nur vage definiert. Oft fehlt eine zentrale Anlaufstelle für Cyber-Vorfälle.

Organisation



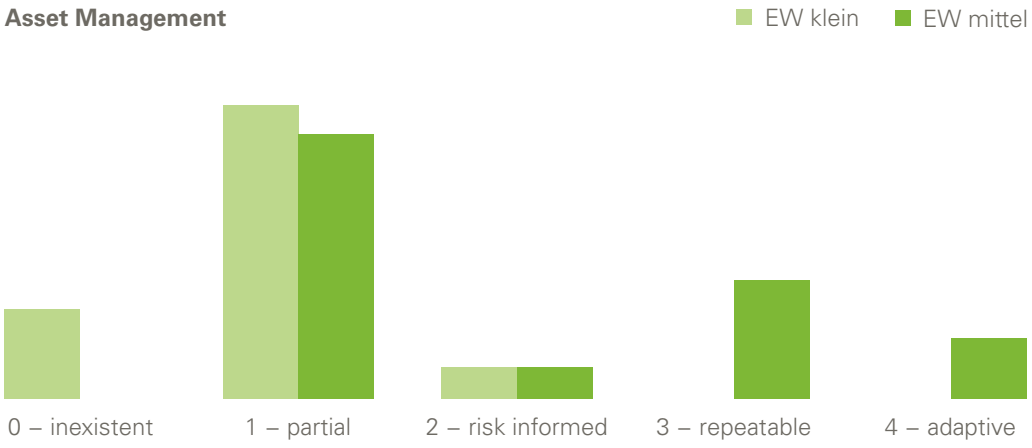
Die Abhängigkeit von Lieferanten und Dienstleistern ist gross und daher auch die damit verbundenen Risiken. Trotzdem werden Lieferantenrisiken und dies nicht nur hinsichtlich der Cybersecurity oft nur ansatzweise bis gar nicht bewirtschaftet. Stattdessen wird auf eine gute Beziehung und das Vertrauen abgestellt, das durch die bisherige Zusammenarbeit entstanden ist. Fehlende Risikobewertungen, Leistungsspezifikationen und Nachweispflichten sowie die fehlende Definition von Prozessen und Verantwortlichkeiten zur Behandlung von Sicherheitsproblemen konnten als die wesentlichen Schwachpunkte der Lieferantenbeziehungen identifiziert werden.

Lieferantenrisiken



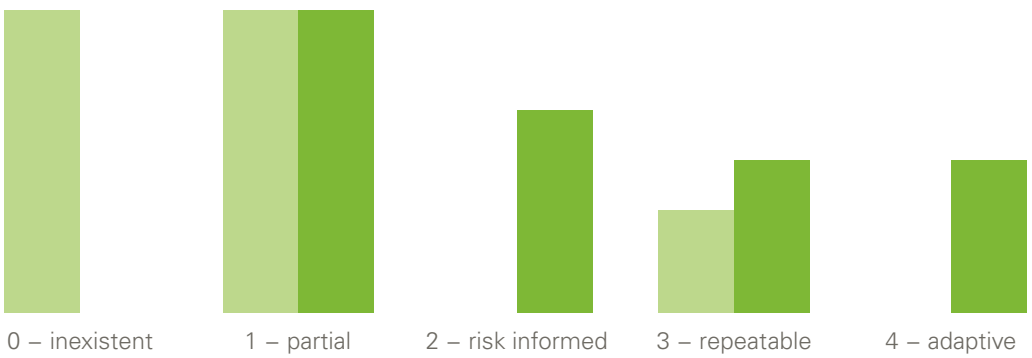
Das Asset Management hinsichtlich Cyber-Risiken, d.h. die Inventarisierung, Klassierung und Risikobewertung von Hardware, Software und Daten, kann nur bei wenigen mittleren Werken als zufriedenstellend bezeichnet werden. Auch wenn ein mehr oder weniger vollständiges Inventar geführt wird, unterbleibt jedoch eine systematische Klassierung und Risikobewertung der Assets mehrheitlich. Am häufigsten wird die Hardware und am seltensten werden Daten inventarisiert. Die Software-Inventarisierung erfolgt meist im Rahmen des Lizenz- und Patch-Managements. Als häufigstes Werkzeug für das Asset Management wurde Microsoft Excel genannt. In der Regel werden dafür Daten aus verschiedenen Quellen zusammengeführt. Diese Art der Datenbewirtschaftung ist aufwendig und fehleranfällig. Allerdings müssen Angebote für entsprechende Softwarelösungen, welche ein ganzheitliches Asset Management für die OT-Welt erlauben, als Mangelware bezeichnet werden. Klassische Asset Management Tools bieten keine Funktionen für Cybersecurity-Aspekte und Inventarisierungslösungen aus der klassischen IT- und Netzwerkwelt bieten kaum befriedigende Funktionen für andere wichtige Aspekte wie Lifecycle Management und betriebsorganisatorische Anforderungen. Da das Asset Management die Grundlage für ein zielgerichtetes und risikobasiertes Management von Cyber-Risiken bildet, sollte dieses Thema ganz oben auf die Prioritätenliste gesetzt werden.

Asset Management



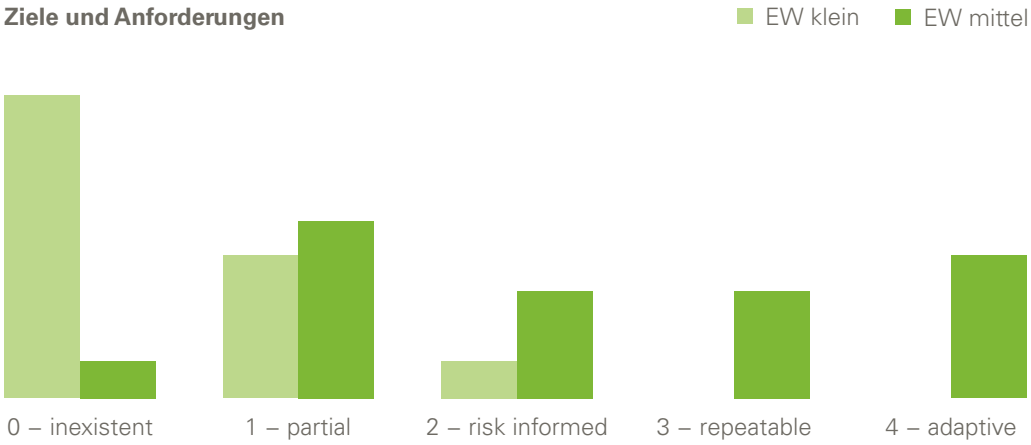
Sofern eine Risikoanalyse hinsichtlich der Cybersecurity durchgeführt wird, erfolgt diese oft nur gesamthaft als ein wenig prominenter Punkt im Rahmen einer jährlichen Gesamtrisikobetrachtung oder höchstens für einzelne Cyber-Szenarien. Ein standardisierter Prozess dafür fehlt bei kleineren Werken weitgehend. Nur wenige Werke verwenden standardisierte Checklisten für die Analyse von Cyber-Risiken.

Risikoanalyse

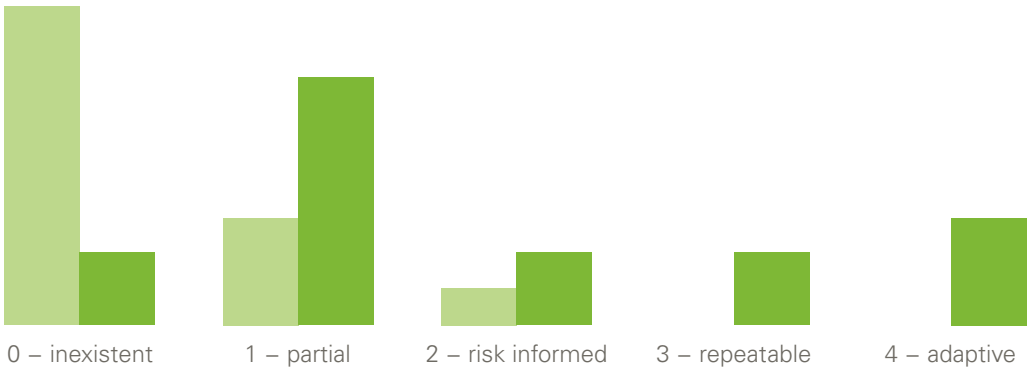


Die Definition von Zielen und Anforderungen zeigt ein gleiches Bild wie die Festlegung der Cybersecurity Strategie und liegt gesamthaft etwas unter dem Reifegrad der Risikoanalyse. Eine Strategie und Ziele kennen nur wenige kleinen Werke und auch dies nur ansatzweise, während von den mittleren Werken auch nur weniger als die Hälfte solche definiert hat. Daraus lässt sich schliessen, dass Cybersecurity noch zu wenig als Führungsaufgabe wahrgenommen wird. Dies zeigt sich auch beim Thema «Führungsgrössen und Kennzahlen», wo die grössten Defizite festgestellt werden konnten. Sicherheit ist ein relativer Zustand der Gefahren- und Störungsfreiheit zu einem bestimmten Zeitpunkt und ist daher nicht als Produkt sondern als Prozess zu verstehen. Cybersecurity ist bei der grossen Mehrheit der untersuchten Elektrizitätswerke jedoch noch kein geführter Prozess, sondern wird noch zu sehr als eine statische Angelegenheit wahrgenommen. Der Grundsatz «you can not control what you can't measure» gilt ganz besonders auch für den digitalen Sicherheitsbereich.

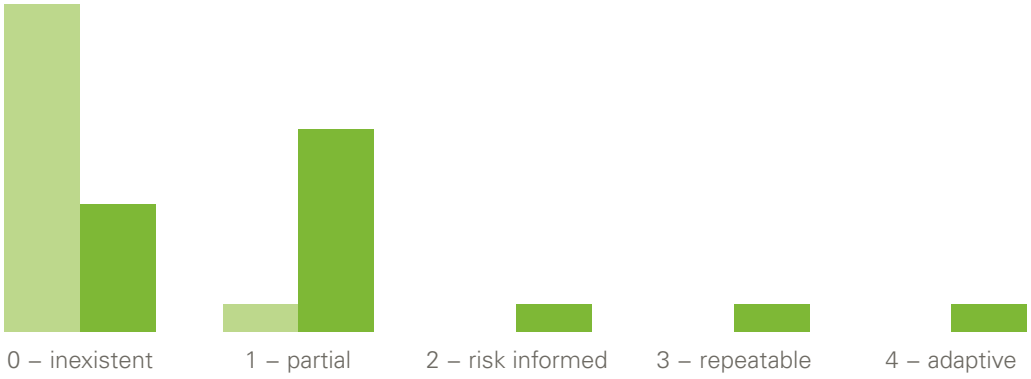
Ziele und Anforderungen



Cybersecurity Strategie

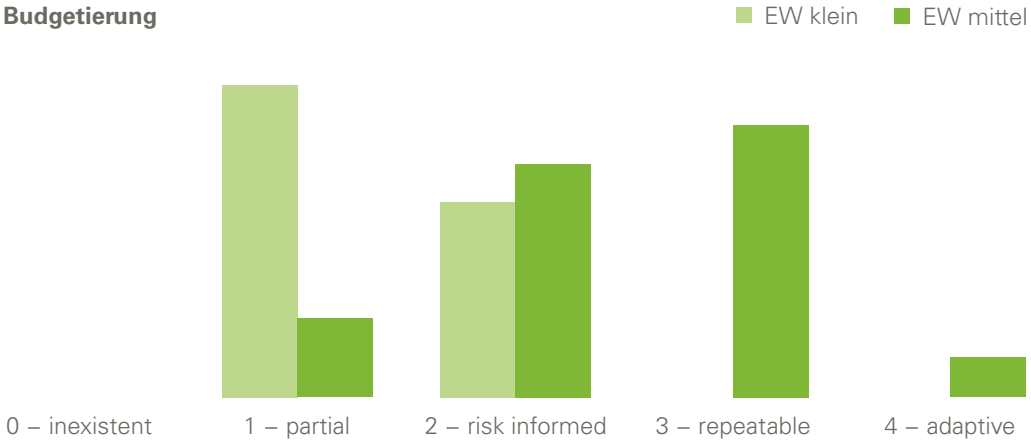


Führungsgrössen / Kennzahlen



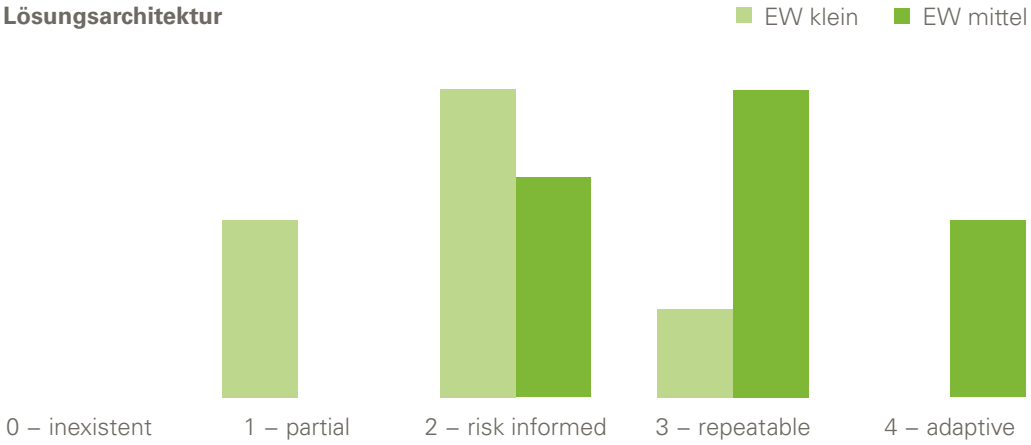
Die Budgetierung der Cybersecurity erfolgt bei den mittleren Werken mehrheitlich standardisiert wenn auch meist nicht auf Basis einer Risiko/Kosten-Analyse, da Cybersecurity-relevante Positionen in der Regel nicht explizit ausgewiesen werden. Kleinere Werke budgetieren ihre übersichtlichen Ausgaben für die Cybersecurity auf Basis der bisherigen laufenden Kosten und im Rahmen der aktuellen Projekte.

Budgetierung

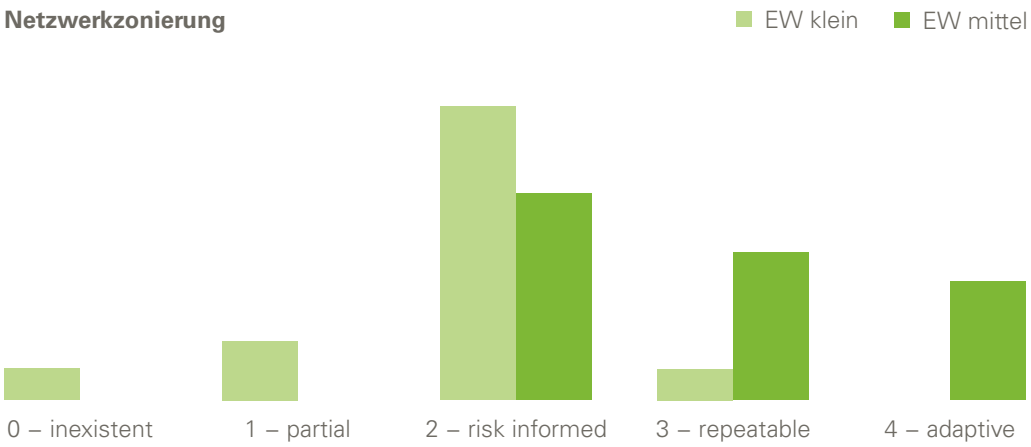


Die technische Lösungsarchitektur ist bei den mittleren Werken besser dokumentiert und wird systematischer gepflegt, als dies bei kleinen Werken der Fall ist. Während die grösseren Werke eine mehrschichtige Sicherheitsarchitektur besitzen, beschränken sich dagegen kleinere Werke immer noch auf ein eher bescheidenes Bündel an Schutzmassnahmen wie Perimeter-Firewall und Antivirus-Software. Der Systemhärtung zur Verringerung der Angriffsfläche wird nur selten Aufmerksamkeit geschenkt mit Ausnahme von einigen mittleren Werken. Es wird meist darauf vertraut, dass der Lieferant (vor allem von OT-Systemen) seine Systeme hinreichend härtet und sicher konfiguriert.

Lösungsarchitektur

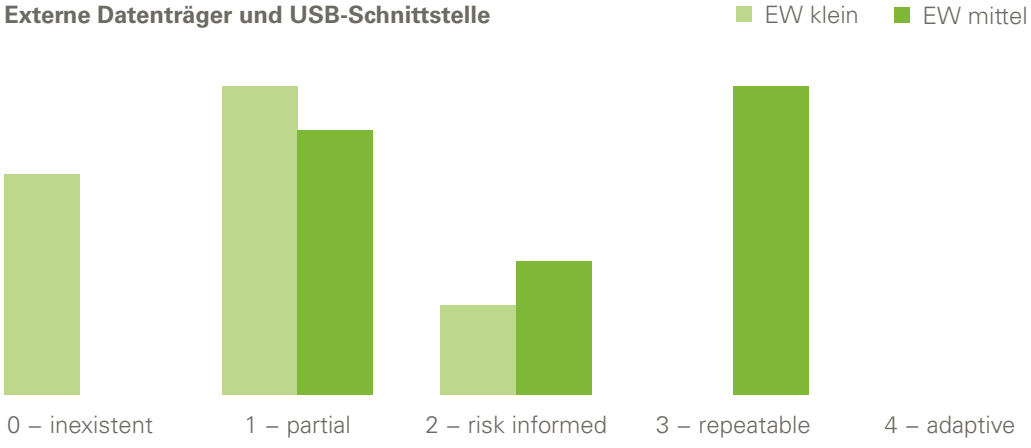


Netzwerkzonierung



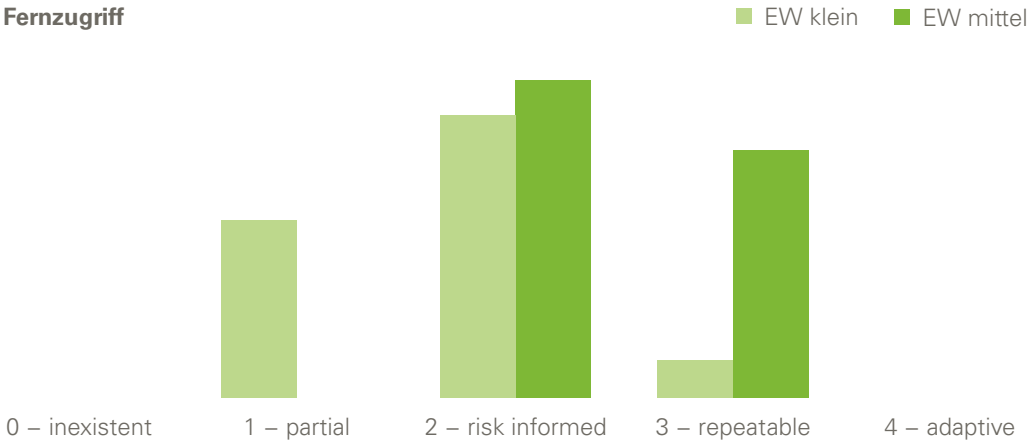
Die Wichtigkeit einer Trennung beziehungsweise Zonierung der Netzwerke wird von praktisch allen Werken erkannt, wobei dies vor allem bei den kleineren mit je einem Segment für Office-IT und OT sowie einem allfälligen Gäste-WLAN ohne eine weitere Subzonierung umgesetzt wird. Auch wenn angeführt wurde, dass OT- und IT-Netzwerk komplett voneinander getrennt sind, relativiert sich die dadurch gewonnene Sicherheit für das sicherheitskritischere OT-Netzwerk durch das Einbringen von Notebooks, die oft sogar permanent vorhandenen Fernzugriffe und den Datenaustausch über Datenträger wie USB Memory Sticks.

Externe Datenträger und USB-Schnittstelle



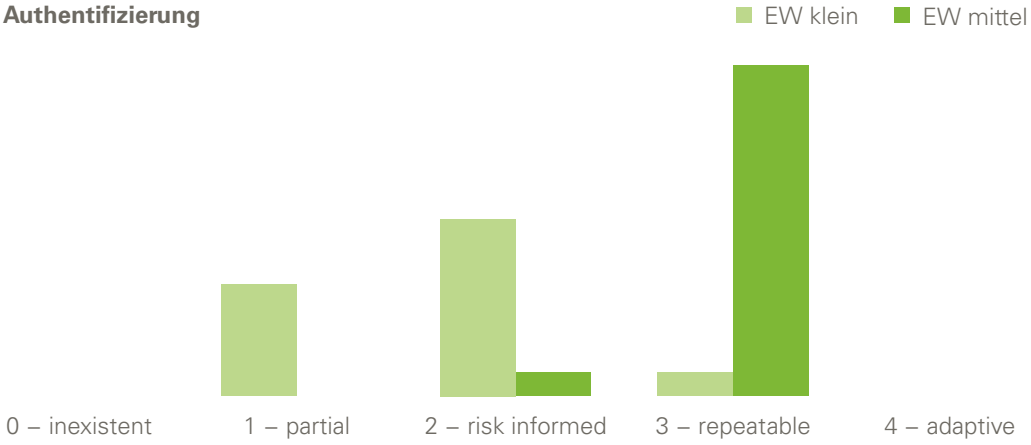
Dem Angriffsvektor über externe Datenträger und insbesondere über die USB-Schnittstelle wird nicht nur bei den kleinen Werken sondern auch bei der Hälfte der mittleren Werke zu wenig Aufmerksamkeit geschenkt. Fehlende Richtlinien betreffend den Umgang mit dem USB-Port und externen Datenträgern sowie weitgehend fehlende Schutzmassnahmen machen Elektrizitätswerke verletzlich, auch wenn dazu eine absichtliche Infektion oder die unwissentliche Mithilfe durch eine Person mit physischem Zugang zur USB-Schnittstelle nötig ist.

Fernzugriff



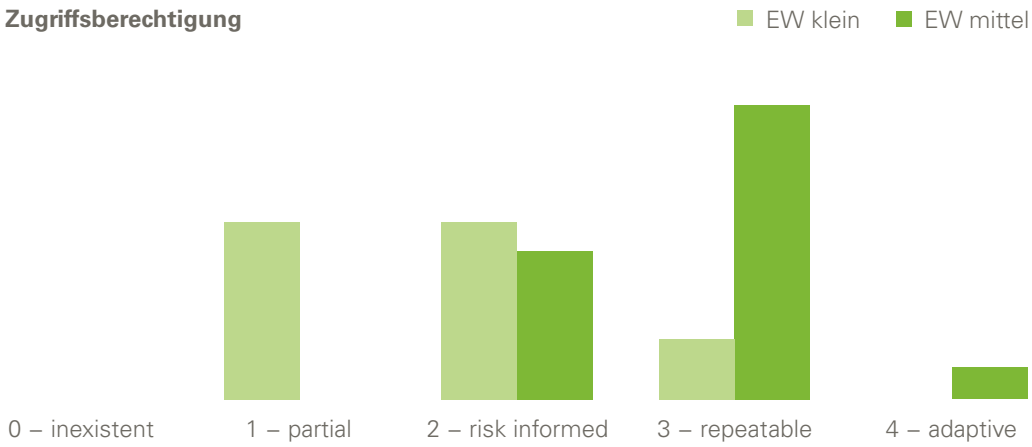
Praktisch alle Werke verfügen über einen Fernzugriff zu ihrem OT-Netzwerk, weil unter anderem die Hersteller in der Regel einen solchen Zugang für einen Wartungsvertrag voraussetzen. Wo die Office-IT von einem externen Dienstleister betreut wird, benötigt auch dieser einen Wartungszugang von extern. Die Verbindung wird in der Regel über ein Virtual Private Network (VPN) gesichert, nur teilweise mit einer Zwei-Faktor-Authentifizierung zusätzlich gesichert und selten über einen Jump Host geführt. Nur relativ wenige Werke schalten den Zugang nur bei Bedarf frei oder überwachen ihn aktiv. Die Aufzeichnung der über den Fernzugriff erfolgenden Aktivitäten beschränkt sich meist auf die Anmeldung am System.

Authentifizierung



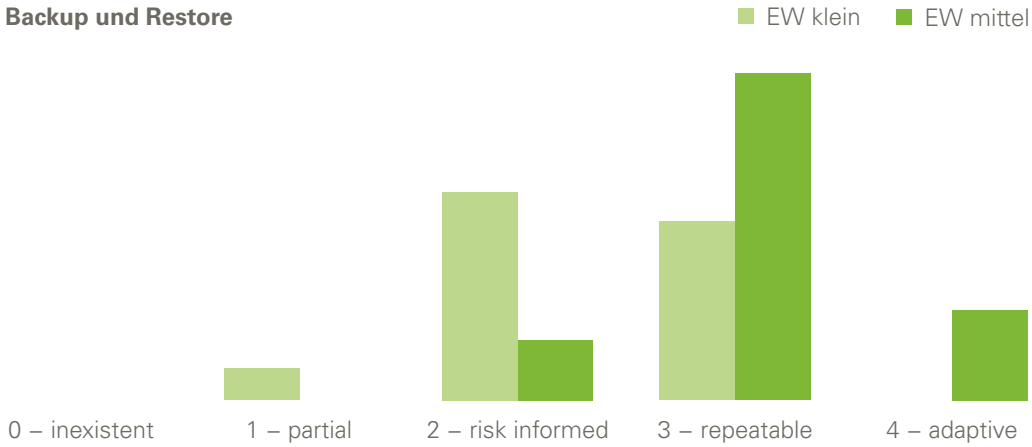
Eine Zugriffskontrolle besteht grundsätzlich überall, aber vor allem in kleineren Werken fehlt deren Dokumentation, die Prozesse dazu sind nur wenig und unvollständig standardisiert und die Zugriffsberechtigungen werden selten periodisch überprüft. Privilegierte Benutzer werden zudem allgemein nur selten mit zusätzlichen Massnahmen und Tools geschützt. Kleinere Werke verfügen auch eher selten über dokumentierte Passwortrichtlinien. Jedoch werden die Prinzipien «Least Privileges» (minimalstmögliche Berechtigungen) und «Segregation of Duties» (Gewaltentrennung) mehrheitlich konsequent umgesetzt und in der Regel personalisierte Benutzer verwendet.

Zugriffsberechtigung



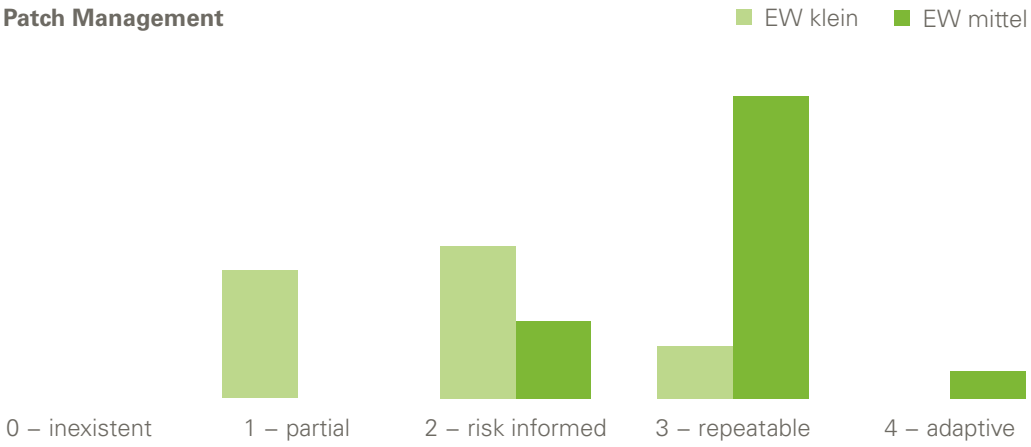
Wie zu erwarten war, schnitt das Thema Datensicherung am besten ab, da sie eine der ältesten klassischen Systemadministrations-Disziplinen darstellt. Die 3-2-1 Regel wird dabei grossmehrheitlich umgesetzt. Jedoch werden vor allem bei kleineren Werken die Backups nur selten bis gar nie auf ihre Integrität überprüft oder Wiederherstellungstest durchgeführt, wodurch nicht gewährleistet ist, dass eine Widerherstellung im Notfall auch wirklich funktioniert.

Backup und Restore



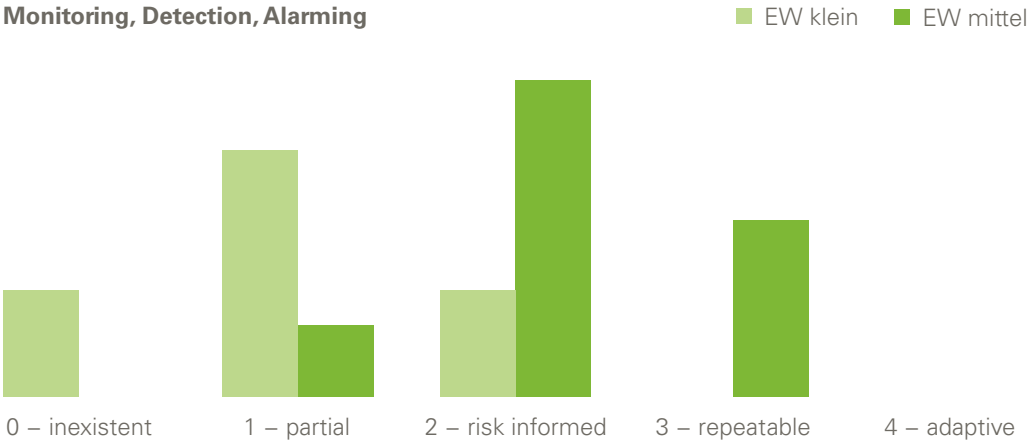
Beim Patch Management, d.h. bei der regelmässigen Aktualisierung der Systeme zur Behebung von bekannten Schwachstellen, bestehen bei den kleinen Werken mehrheitlich Mängel bei der vorgängigen Prüfung der Aktualisierungen sowie der Dokumentation sowohl der Aktualisierungsprozesse als auch der Aktualität der Systeme. Die mittleren Werke verfügen dagegen grossmehrheitlich über ein professionelles Patch Management.

Patch Management



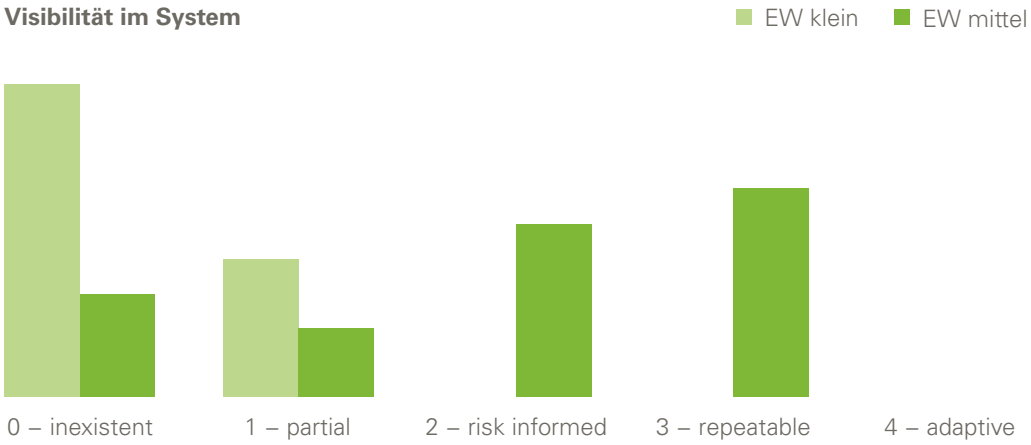
Bei der Systemüberwachung beschränkt sich das Monitoring hauptsächlich und oft ausschliesslich auf die Systemressourcen, da bei Elektrizitätswerken die Verfügbarkeit der Systeme die oberste Priorität darstellt. Ein Monitoring von darüberhinausgehenden sicherheitsrelevanten Parametern wird nur von wenigen mittleren Werken betrieben. Für ein ganzheitliches Cybersecurity-Dispositiv sollten aber auch die anderen beiden Schutzziele «Integrität» und «Vertraulichkeit» nicht vernachlässigt werden. Des Weiteren fehlt oftmals eine automatische Alarmierung im Fall von Problemen, um eine zeitnahe Reaktion auf diese sicherzustellen.

Monitoring, Detection, Alarming



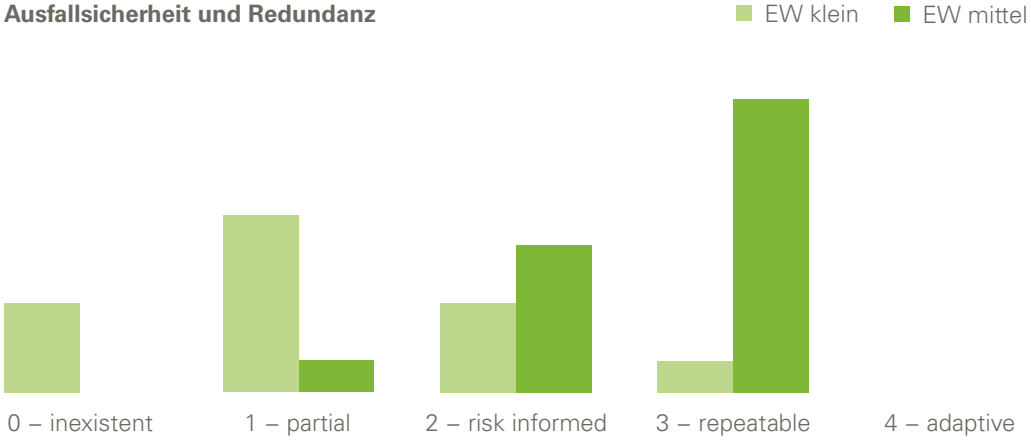
Infolge fehlender Visibilität im Netzwerk ist Cybersecurity in kleineren Werken ein Blindflug und dies teilweise auch bei grösseren. Mangels «SSL Inspection», «Intrusion Detection» oder Netzwerkzugangskontrolle kann ein Angriff im Netzwerk hinter der Perimeter-Firewall nicht erkannt werden und die Wahrscheinlichkeit ist hoch, dass es bei der Hoffnung bleibt, diesen durch eine Antivirus-Software auf einem Zielsystem zu erkennen. Ebenso bleiben Sicherheitslücken infolge fehlender Schwachstellenscans unentdeckt.

Visibilität im System



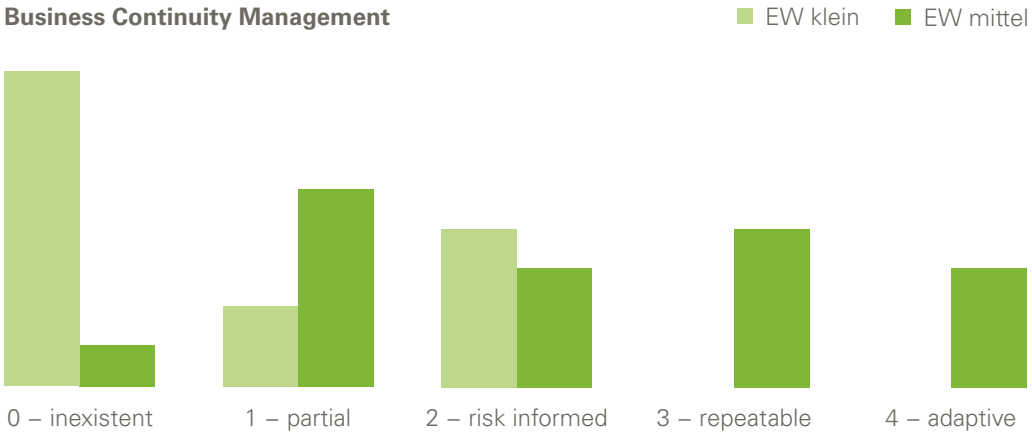
Auch wenn die Anforderungen an die Ausfallsicherheit nur bei zwei Drittel der mittleren Werke definiert sind, verfügen sie in der Regel über redundante Systeme. Bei den meisten kleinen Werken wird der Redundanz zu wenig Aufmerksamkeit geschenkt. Dies verwundert insofern, dass gerade die Verfügbarkeit bei den Elektrizitätswerken die oberste Priorität darstellt. Auch wenn bisher keines der untersuchten Werke nennenswerte Systemausfälle zu verzeichnen hatte, sollte dies nicht dazu verleiten, sich auch für die Zukunft in Sicherheit zu wiegen. Der Verfügbarkeit sollte vor allem auch in den Verträgen mit Dienstleistern und Lieferanten mehr Aufmerksamkeit geschenkt werden.

Ausfallsicherheit und Redundanz



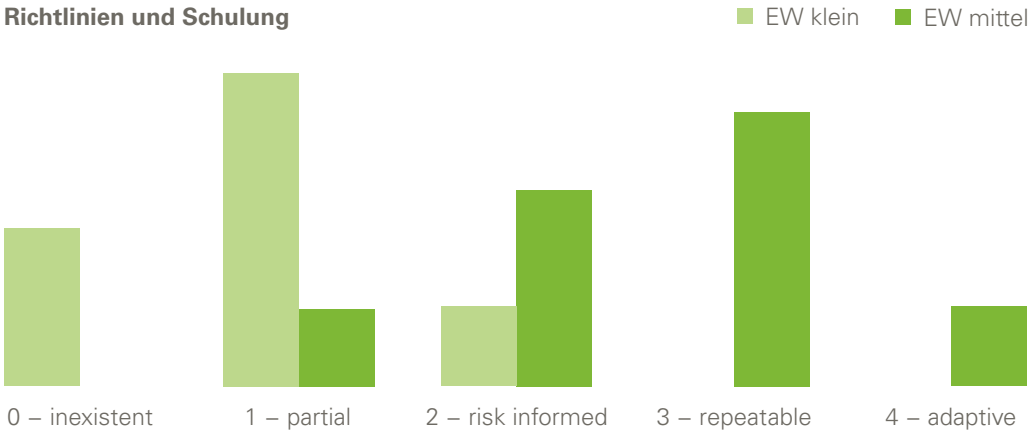
Die Fähigkeit und Bereitschaft zu einer zeitnahen und angemessenen Reaktion auf Cyber-Sicherheitsvorfälle sowie zur Wiedererlangung der sicheren Operabilität innert nützlicher Frist hat sich als eines der grössten Problempunkte herausgestellt. «Incident Response» und «Disaster Recovery» sind oft bestenfalls angedacht, aber kaum ausreichend vorbereitet und wurden in der Regel noch nie geübt. Die meisten untersuchten Werke scheinen diesbezüglich noch zu wenig in der digitalen Welt angekommen zu sein und beschränken ihr «Business Continuity Management» auf Ereignisse in der physischen Welt.

Business Continuity Management



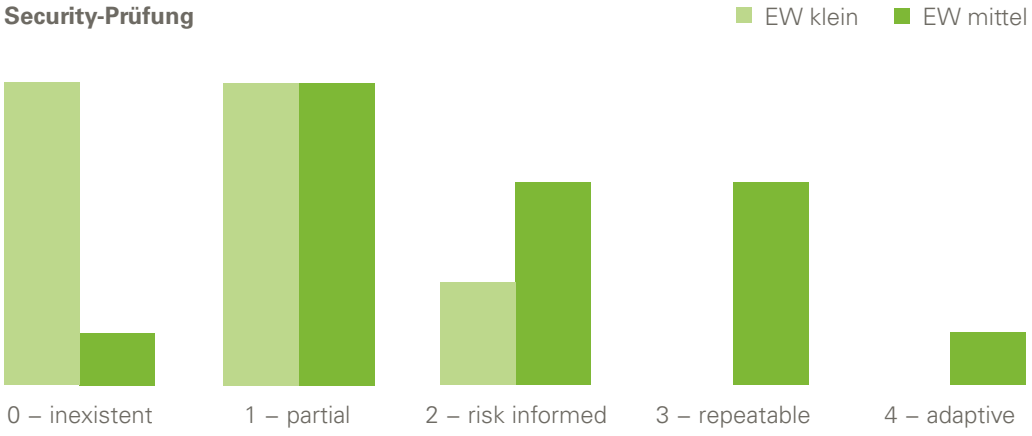
Der Mensch wurde von der Mehrheit der Teilnehmer als schwächstes Element identifiziert. Die systematische Behandlung dieses Problemfeldes steht vor allem bei kleineren Werken aber mehrheitlich noch ganz am Anfang. Über dokumentierte Richtlinien für die digitale Welt verfügen vor allem die grösseren Werke und schulen diese mehrheitlich auch systematisch und regelmässig. Bei kleinen Werken erfolgt der diesbezügliche Informationsaustausch (sofern vorhanden) hauptsächlich auf mündlichem Weg.

Richtlinien und Schulung



Die periodische Überprüfung der Cybersecurity gehört nur bei einem Teil der mittleren Werke zum Standard. Erfreulicherweise haben aber auch schon einige kleinen Werke sich einer Überprüfung durch externe Fachleute unterzogen und wollen dies auch künftig regelmässig tun. Auch wenn ein Security Audit und Penetrationstest mit relativ hohen Kosten verbunden ist, sollte dies bei allen Unternehmen der kritischen Infrastruktur doch zumindest für die risikoreichsten Systeme zum Standard gehören.

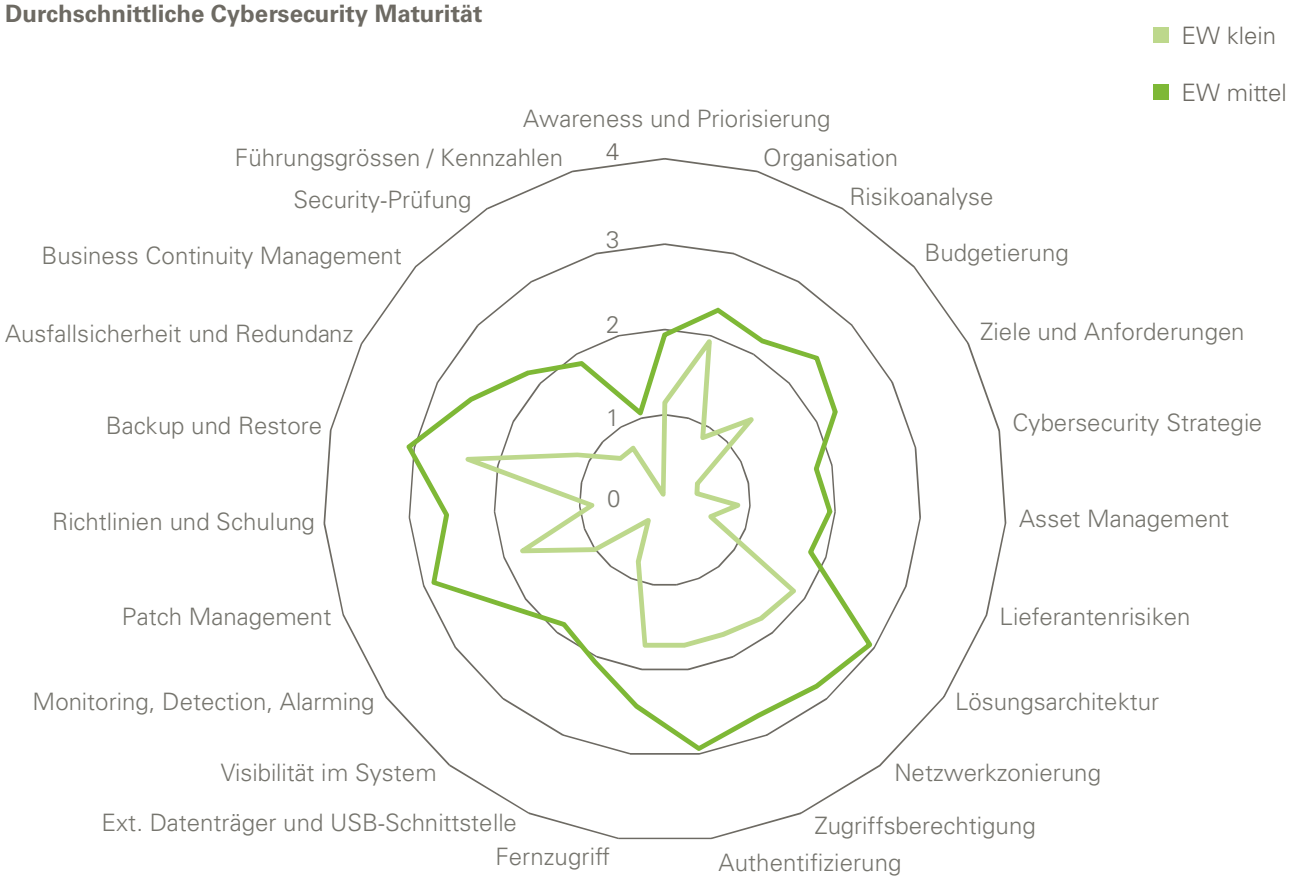
Security-Prüfung



Fazit

Während die mittleren Elektrizitätswerke im Hinblick auf die Cybersecurity mehrheitlich relativ gut unterwegs sind, zeigt sich besonders bei den kleinen, lokalen Elektrizitätsversorgungsunternehmen in vielen Disziplinen ein erheblicher Nachholbedarf.

Durchschnittliche Cybersecurity Maturität



Informationssicherheitsvorfälle sind wie Radioaktive Strahlung. Ohne die richtigen Schutz- und Erkennungsmassnahmen bemerkt man sie erst, wenn es schon zu spät ist. Trotzdem wird vor allem bei kleineren Werken dem Schutz mehr Aufmerksamkeit geschenkt als der Entdeckung von digitalen Sicherheitsvorfällen und der Fähigkeit und Bereitschaft zu einer raschen und angemessenen Reaktion auf diese. Werke mit mehr als 60 Mitarbeitern haben zu einem grossen Teil erkannt, dass neben mehrstufigen Schutzmassnahmen auch ein wirkungsvolles und verzögerungsfreies Erkennen von Sicherheitsvorfällen, eine zeitnahe und angemessene Reaktion auf diese sowie die Wiedererlangung der sicheren Operabilität innert nützlicher Frist wichtige Elemente einer ganzheitlichen Cybersecurity-Strategie sind. Dabei sollte dem Faktor Mensch als grösste Schwachstelle auch eine entsprechende Rolle zukommen. Eine vermehrte Investition in verständliche und praktikable Richtlinien sowie die regelmässige, systematische Schulung von Mitarbeitern sollte nicht als Luxus betrachtet werden. Sicherheit braucht nicht nur technische Lösungen, sondern vor allem auch eine von allen Beteiligten gelebte Sicherheitskultur.

Investitionen in Cybersecurity werden oft zu zögerlich getätigt, weil für die Budgetallokation ohne einen messbaren «Return on Investment» eine Argumentation meist schwierig ist. Kritische Infrastrukturen haben ungleich längere Lebenszyklen als die Technologien der Cyberwelt. Für die Infrastrukturbetreiber gilt es, Fähigkeiten zu entwickeln, um die Verschmelzung der OT- und IT-Welt und die damit verbundenen neuen Bedrohungen zu bewältigen.

Die identifizierten Defizite sind einerseits auf das zu wenig als Führungsaufgabe wahrgenommene Thema und die beschränkten personellen Ressourcen und andererseits auf die Verfügbarkeit der nötigen Fachkompetenz zurückzuführen. Während die ganz grossen Unternehmen Chief Information Security Officers und eigene Abteilungen haben, die sich dediziert mit dem Thema Cybersecurity befassen, wird dessen Relevanz in vielen kleinen und mittleren Unternehmen noch oft unterschätzt. Unternehmen, welche die Herausforderungen nicht aus eigener Kraft stemmen können, sind gut beraten, sich fachkompetente Hilfe ins Haus zu holen oder einzelne Dienste an entsprechende Dienstleister auszulagern. Und nicht zuletzt sollte auch die Fachkompetenz auf der Führungsebene verstärkt werden.

www.electrosuisse.ch