الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

حماية شبكات الكهرباء

تقرير الأمن السيبراني في قطاع الكهرباء
2020

تصنيف الوثيقة: متاح
إشارة المشاركة: أبيض

مركز الدراسات الاستراتيجية للأمن السيبراني

www.nca.gov.sa

عن الهيئة الوطنية للأمن السيبراني (NCA)

تأسست الهيئة الوطنية للأمن السيبراني (NCA) في عام 2017. الهيئة الوطنية للأمن السيبراني هي الجهة الحكومية المسؤولة عن الأمن السيبراني في المملكة العربية السعودية وهي بمثابة السلطة الوطنية في جميع الشؤون ذات الصلة. لديها وظائف تنظيمية وتشغيلية تتعلق بالأمن السيبراني وتعمل عن كثب مع الجهات العامة والخاصة لتحسين وضع الأمن السيبراني في المملكة من أجل حماية مصالحها الحيوية والأمن القومي والبنى التحتية الحيوية والقطاعات ذات الأولوية العالية والخدمات والأنشطة الحكومية.

يحتوي هذا التقرير على آراء عدة جهات وأفراد ، مع ملاحظة أن جميع المعلومات الواردة في التقرير هي إرشادية فقط. أيضًا ، لا تتحمل الهيئة الوطنية للامن السيبراني أي مسؤولية - تحت أي ظرف من الظروف - تجاه أي طرف نتيجة لأي قرار أو إجراء تم اتخاذه أو سيتخذه هذا الطرف بناءً على محتوى هذا التقرير. تؤكد الهيئة الوطنية للامن السيبراني أنها ليست مسؤولة كليًا أو جزئيًا عن أي خطأ أو تقصير مباشر أو غير مباشر قد يحدث.

© 2020. الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية. مركز الدراسات الاستراتيجية للأمن السيبراني.

المحتويات

الملخّص التنفيذي

الملخّص التنفيذي

تمّ إعداد هذه الدراسة بالاستناد إلى الأبحاث والمؤلفات الرائدة في مجال حماية شبكات الكهرباء، بالإضافة إلى العديد من المقابلات مع الخبراء في قطاع الكهرباء والأمن السيبراني بهدف استخلاص مجموعة من التوصيات وتقديمها للمهنيين العاملين في قطاع الكهرباء ومؤسسات القطاع العام و الجهات الوطنية و التنظيمية وشركات القطاع الخاص.

يحتل قطاع الكهرباء أهمية فائقة بالنسبة لكلّ القطاعات الأخرى الأمر الذي يتطلب توفير مستوى متقدم في الأمن السيبراني. فعلى الصعيد الدولي، يتمّ فرض لوائح وأنظمة الأمن السيبراني بدرجات متفاوتة في مختلف المناطق الجغرافية، ويُلاحظ وجود علاقة إيجابية بين مستوى نضج الأمن السيبراني ودرجة تطبيق اللوائح والأنظمة ذات العلاقة.

مشهد التهديدات

يزداد مشهد التهديدات السيبرانية تعقيدًا مع ارتفاع معدل الهجمات المتقدمة ضد شبكات أنظمة التحكم الصناعية وشبكات التقنية التشغيلية، تستهدف هذه الهجمات قطع إمدادات التيار الكهربائي وتعطيل المعدات والأجهزة في البنية التشغيلية، وقد نجحت في بعض الأحيان في تحقيق ذلك. من ناحية أخرى، تتعرض شبكات أنظمة التحكم الصناعية وشبكات التقنية التشغيلية لحملات استطلاع من قبل مجموعة من البرمجيات الضارة التي تستهدف الوصول إلى البيانات المتعلقة بشبكات الكهرباء وتسريبها إلى أجهزة حواسيب بعيدة تحت إشراف وسيطرة المهاجمين.

التحديات

من أكبر التحديات الشائعة التي يعاني منها قطاع الكهرباء هي افتقاره لقدرات الحماية المتقدمة بسبب إعتماد القطاع على بنية تحتية قديمة لشبكات الكهرباء وحاجتها لفترات صيانة طويلة وتزامن ذلك مع ارتفاع تكلفة استبدال المعدات الرئيسية، الأمر الذي جعل من مواقع توليد وتوزيع الكهرباء هدفًا للهجمات السيبرانية. كما يعاني القطاع من تحديات تتعلق بارتباط شبكات أنظمة التحكم الصناعية وشبكات التقنية، حيث يتم استهداف أنظمة تقنية المعلومات واستغلالها كطريق للمهاجمين إلى شبكات الكهرباء الرئيسية والتي تنشأ غالباً من حملات التصيّد الإلكتروني وهجمات التصيّد الاستبقائي.

من ناحية أخرى، تزداد سلسلة التوريد تعقيدًا أكثر من أي وقت مضى مع اعتماد مؤسسات الكهرباء على تقنيات الشبكة الذكية، الأمر الذي يجعل من الصعب ضمان أمن البرمجيات وأنظمة البنى التشغيلية والخدمات المقدمة من المورّدين.

وهذا ما يجعل من الصعب تطبيق متطلبات الأمن السيبراني مع محاولة المسؤولين في هذا المجال لتحقيق التوازن بين متطلبات الحماية المتقدمة ومتطلبات تقنية المعلومات وشبكات أنظمة التحكم الصناعية وشبكات التقنية التشغيلية في مؤسساتهم.

مما يضاعف الفجوة في كودار الأمن السيبراني في القطاع هو افتقار مؤسسات الكهرباء للخبراء الذين يجمعون بين المعرفة بشبكات أنظمة التحكم الصناعية وشبكات التقنية التشغيلية من جهة ومهارات الأمن السيبراني من جهة أخرى، الأمر الذي يقف حجر عثرة أمام جهود قادة قطاع الكهرباء الرامية إلى الارتقاء بمستوى النضج السيبراني في مؤسساتهم.

التوصيات

يحتوي هذا التقرير على مجموعة من التوصيات بهدف التعاون في مواجهة التحديات السيبرانية في القطاع متمثلة بالقدرات البشرية والعمليات والجوانب التقنية والحوكمة.

إن تعزيز ثقافة الأمن السيبراني في قطاع الكهرباء تعتبر عاملًا أساسيًا لرفع مستوى الوعي بأهمية تحقيق متطلبات الأمن السيبراني في القطاع. توصي الدراسة مؤسسات الكهرباء بمقترحات لسدّ الفجوة في قدرات كوادر الأمن السيبراني وذلك من خلال العمل على رفع مهارات مهندسي البنية التشغيلية لقطاع الكهرباء في مجال الأمن السيبراني، والذي يتطلب دعم الإدارة العليا في مؤسسات القطاع لبرامج الأمن السيبراني بالإضافة إلى أهمية إسناد مسؤولية إداراة شبكات أنظمة التحكم الصناعية وشبكات التقنية التشغيلية إلى موظفين خبراء في هذا المجال. كما يحتوي هذا التقرير على مجموعة من التقنيات والممارسات التقنية التي من شأنها تعزيز الصمود السيبراني لمؤسسات الكهرباء ضد التهديدات السيبرانية ورفع قدرات الحماية من الهجمات السيبرانية والكشف عنها.

يوصي هذا التقرير بأهمية سنّ لوائح وسياسات متوافقة في مجال الأمن السيبراني لتعزيز التنسيق المتبادل في قطاع الكهرباء في مختلف المناطق ودول العالم، وكذلك، كما يحث التقرير على أهمية اتباع المعايير والتشريعات الدولية ذات الصلة للارتقاء بمستوى النضج السيبراني. أخيرًا، يوصي هذا التقرير بضرورة التعاون بين مختلف منظومات الكهرباء لتحسين تبادل المعلومات ومساعدة بعضها البعض في الاستجابة للتهديدات السيبرانية على المستوى الدولي.

مقدمة

يعمل الاتصال المتزايد للنظام البيئي للكهرباء على ربط أنظمة التحكم الصناعية بشبكات تقنية المعلومات، مما يمثل هدفًا جذابًا للجهات الفاعلة في التهديد.

يدين العالم الحديث للتقدم المتسارع في القرن العشرين الى إمكانية الوصول للكهرباء بشكل جدير بالثقه. فبينما شهد النصف الأول من القرن العشرين التطور الصناعي والكهربائي في القطاعات كافة، كان النصف الثاني المستند على هذا الأساس سبيلًا للترابط والاتصال بين القوى التجارية وما كان ليحدث كل ذلك بدون الكهرباء.

تحتل الكهرباء أهمية فائقة على المستوى العالمي بالنسبة لقطاعات البنية التحتية الوطنية الحساسة مثل قطاع الاتصالات والنقل والتصنيع والدفاع والخدمات المالية وذلك نظرًا للاعتماد الكلي لهذه القطاعات على قطاع الكهرباء، والذي يتطلب من منظومة القطاع وضع إداراة المخاطر السيبرانية في مقدمة أولوياته.

فمنذ تأسيسه في القرن التاسع عشر، ظل قطاع الكهرباء يركز بشكل كبير على المخاطر المتعلقة بالأمن والسلامة، الجدير بالذكر أن مجال المخاطر السيبرانية التي تهدد شبكات الكهرباء احتلت مركزًا متقدماً في الآونة الأخيرة. فقد شكلت المخاطر السيبرانية الناجمة عن الربط بين شبكات الكهرباء المحلية والدولية، مجال رئيسي يستحوذ على اهتمام صنّاع القرار وأصحاب المصلحة الرئيسيين في قطاع الكهرباء (في مجالات التوليد والنقل والتوزيع والاستهلاك).

إن انقطاع التيار الكهربائي على نطاق واسع ولفترة طويلة سيترك آثاره السلبية على قطاع الأعمال التجارية والحكومات والمجتمعات بشكل عام، ومن الواضح أن الهجمات السيبرانية التي تستهدف قطاع الكهرباء تتزايد من حيث عددها وحدّتها حيث أن خبراء الأمن السيبراني بدأوا يلاحظون زيادة في عدد منفذي الهجمات السيبرانية على القطاع، وتطوراً ملحوظاً في قدرات المهاجمين. فعلى سبيل المثال، يُعتبر قطاع الكهرباء في الولايات المتحدة أحد القطاعات الثلاثة الأولى المستهدفة من قبل الهجمات السيبرانية، مسجلاً بعد قطاعي الصناعات الحساسة والاتصالات، أعلى نسبة حوادث سيبرانية[1]. كما لاحظت الدول في أوروبا والشرق الأوسط وآسيا والمحيط الهادئ زيادة في مستوى قدرات منفذي الهجمات السيبرانية، ممّا يشير إلى أن هذه المخاطر السيبرانية أصبحت تحديًا عالميًا.

وقد أعطت الهجمات السيبرانية التي تعرضت لها شبكة الكهرباء في أوكرانيا في عامي 2015 و 2016 مؤشرًا على تحوّل نموذجي في قدرة المهاجمين على إلحاق الضرر بالبنية التحتية الوطنية الحساسة.

تهدف هذه الدراسة إلى إعطاء صانعي القرار في كلّ من القطاعين العام والخاص نظرة واضحة حول التحديات السيبرانية في القطاع.

بداية، يستعرض هذا التقرير لمحة عامة عن منظومة قطاع الكهرباء بشكل عام وفي المملكة العربية السعودية والنمو الذي شهدته منظومة الكهرباء المعاصرة وأهمية اللوائح ذات الصلة في هذا المجال. تنتقل الدراسة بعد ذلك إلى تقييم المخاطر السيبرانية المتزايدة في قطاع الكهرباء حيث تستعرض التهديدات والثغرات السيبرانية المتزايدة. كما يتطرق التقرير إلى التحديات الرئيسية أمام تحسين نضج الأمن السيبراني في قطاع الكهرباء في مجالات عدة أبرزها متطلبات تعزيز قدرات الحماية السيبرانية والنقص في مهارات الأمن السيبراني وأهمية دور الشركاء في سلسلة التوريد في القطاع.

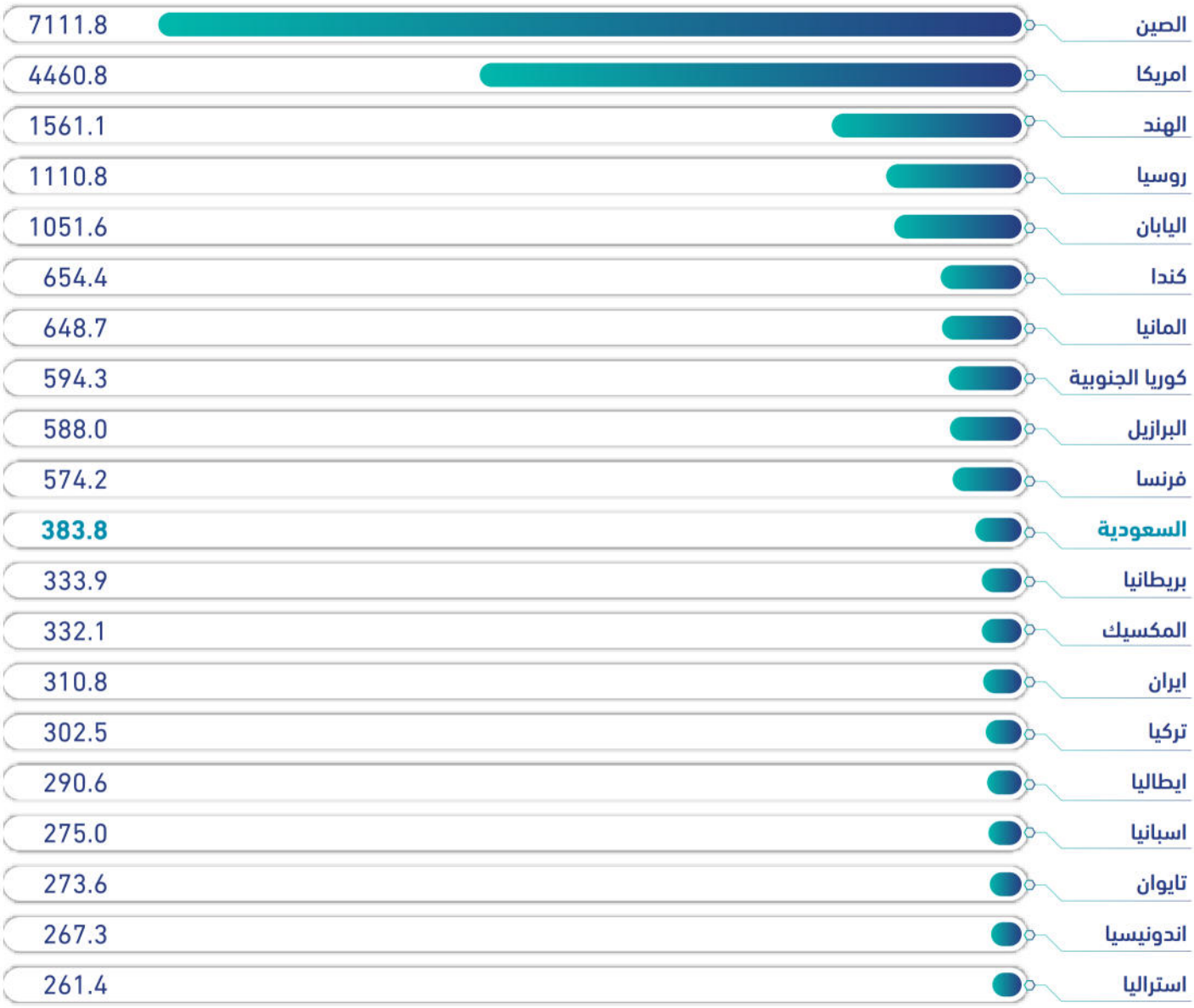
أخيرًا، يقدم التقرير مجموعة من التوصيات الرامية إلى تعزيز قدرات الأمن السيبراني، كما تستشرف الدراسة الاتجاهات المستقبلية بما في ذلك التقنيات"الذكية"التي قد تعزز الأمن السيبراني أو تفرض تحديات جديدة.

نظرة على قطاع الكهرباء

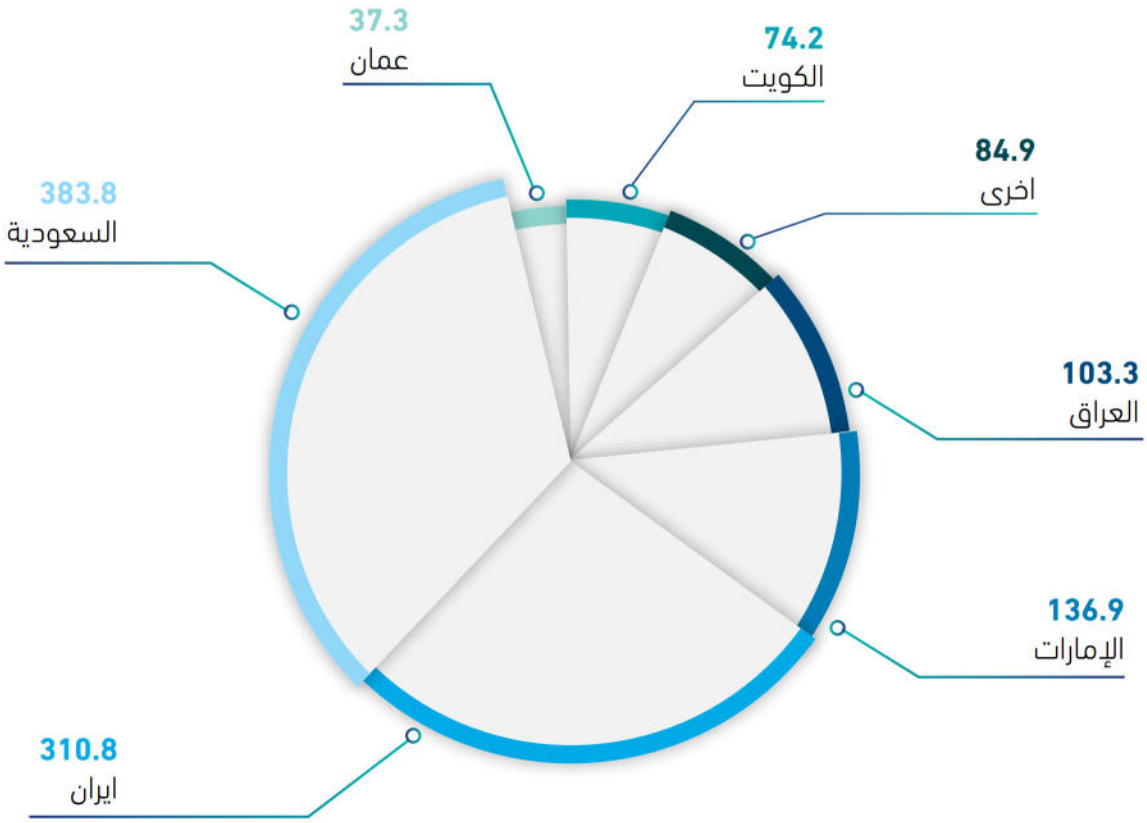
نستعرض نظرة عامه على قطاع الكهرباء على المستوى العالمي وفي المملكة العربية السعودية، والمكوّنات الرئيسية والبنية التحتية لمنظومة الكهرباء. والتي سيكون لها دور في تحليل المخاطر السيبرانية التي تهدد قطاع الكهرباء.

تحتل المملكة العربية السعودية المرتبة الحادية عشرة في إنتاج الكهرباء في العالم حيث بلغ إنتاجها 384 تيراواط في الساعة عام 2018، وتشكل هذه الكمية 31% من إجمالي توليد الكهرباء في الشرق الأوسط برمته. وعلى سبيل المقارنة، يبلغ توليد الكهرباء في الدولتين الأولى والثانية في توليد الكهرباء في العالم، وهما الصين والولايات المتحدة 7,112 و4,461 تيراواط بالساعة على التوالي[2].

الشكل 1: الناتج الإجمالي من توليد الكهرباء في الدول العشرين الأولى في العالم لعام 2018 (تيراواط)



الشكل 2: ناتج توليد الكهرباء في الشرق الأوسط حسب الدولة لعام 2018 (تيراواط)



تسعى المملكة العربية السعودية، لتلبية احتياجاتها المستقبلية من الكهرباء، وزيادة طاقتها التوليدية لتصل إلى 1,420 تيراواط سنويًا كحدٍ أقصى بحلول عام 2040. وبناءً على ذلك، تهدف الخطط الاستراتيجية في القطاع لاستثمار 5 مليار دولار في توليد الكهرباء، بالإضافة إلى 4 مليارات دولار في نقل وتوزيع الكهرباء سنوياً من أجل الوصول إلى إجمالي الإنتاج المستهدف[3].

من منظور الأمن السيبراني، تواجه قطاعات الكهرباء على المستوى العالمي خطرين رئيسين يتناولان أمن البيانات وحماية أنظمة التحكم الصناعية. في المجال الأول، تحتفظ منظومة الكهرباء ببيانات ذات أهمية عاليه تتمثل بمعلومات ذات قيمة تجارية بالإضافة إلى بيانات العملاء. لذلك، فإن أي اختراق لسرية وسلامة وتوافر هذه البيانات من شأنه أن يتسبب بأضرار مالية وتشغيلية فادحة لمؤسسات الكهرباء بالإضافة إلى إلحاق الأذى بسمعتها.

في المجال الثاني، يزداد اعتماد شركات الكهرباء في مختلف دول العالم على أنظمة التحكم من أجل إدارة عمليات إنتاج وتوزيع الكهرباء ومراقبتها، حيث أن توافر وسلامة شبكات الكهرباء يلعبان دوراً رئيسياً في توفير إمدادات عالية الجودة وموثوقة من الكهرباء للسكان وكذلك في سلامة العاملين في قطاع الكهرباء.

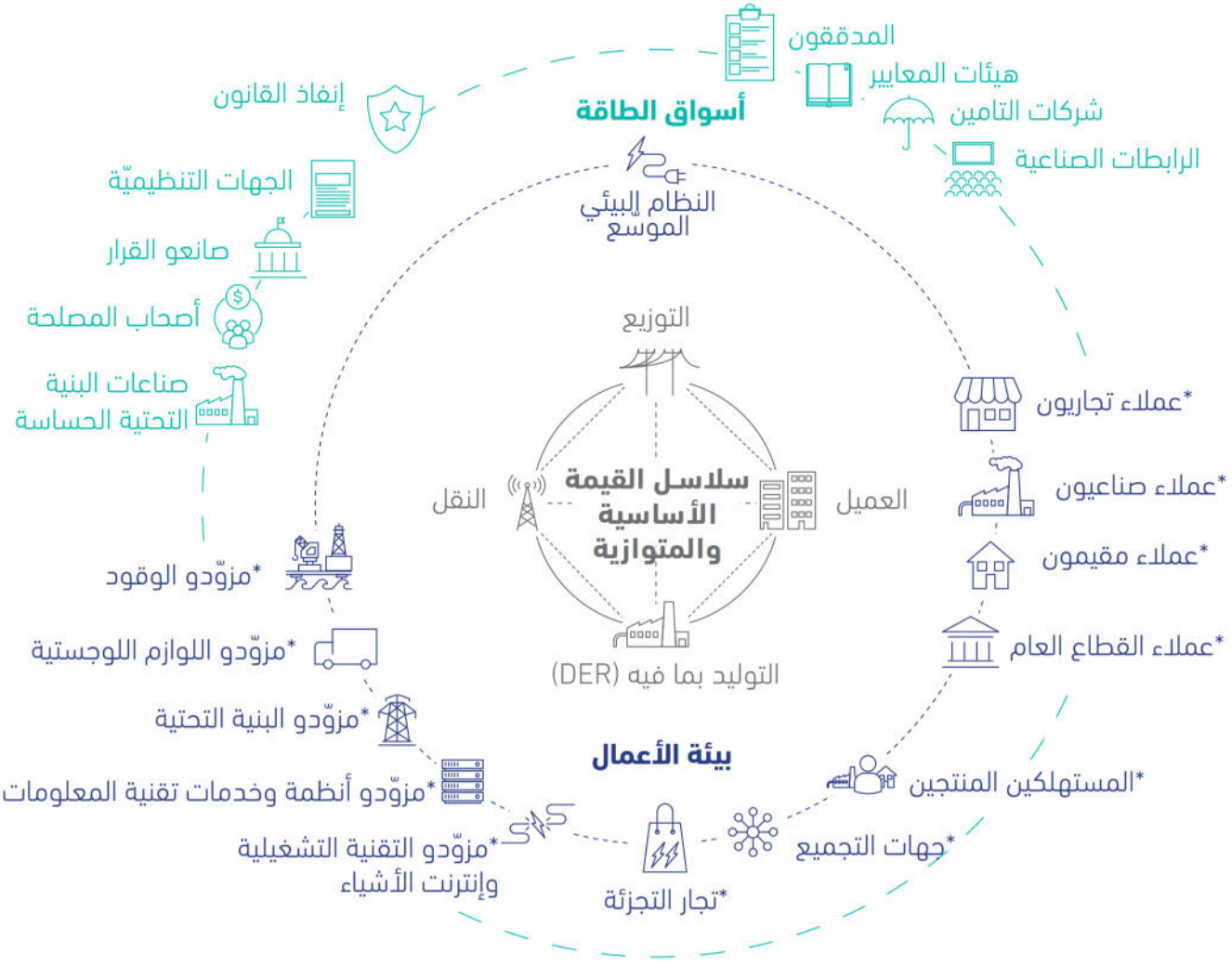
يستعرض التقريرفي الجزء الخاص بـ "التحديات لتعزيز القدرات السيبرانية"،مقارنة تفصيلية بين الأهداف التي من شأنها تعزيز الحماية السيبرانية (بما في ذلك السرية والسلامة والتوافر) في أنظمة تقنية المعلومات وتقنيات أنظمة التحكم الصناعية / التقنيات التشغيلية.

بينما يستعرض الجزء التالي منظومة الكهرباء المعقدة بمزيد من التفصيل.

البنية التحتية لقطاع الكهرباء

تمتاز منظومة الكهرباء بضخامة حجمها حيث أنها تضم مجموعة واسعة من أصحاب المصلحة بدءًا من توليد الكهرباء ومرورًا بالمستهلكين والهيئات التشريعية وانتهاءً بشركات التأمين كما هو موضح في الشكل 3. تعتمد منظومة الكهرباء بقوة على المورّدين لتوريد الوقود وقطع الغيار الحساسة، وبالتالي، يساهم هؤلاء المورّدين بجزء كبير من المخاطر السيبرانية على منظومة قطاع الكهرباء.

الشكل 3: منظومة قطاع الكهرباء الحديثة[4]



* لكلّ كيان نظامه البيئي

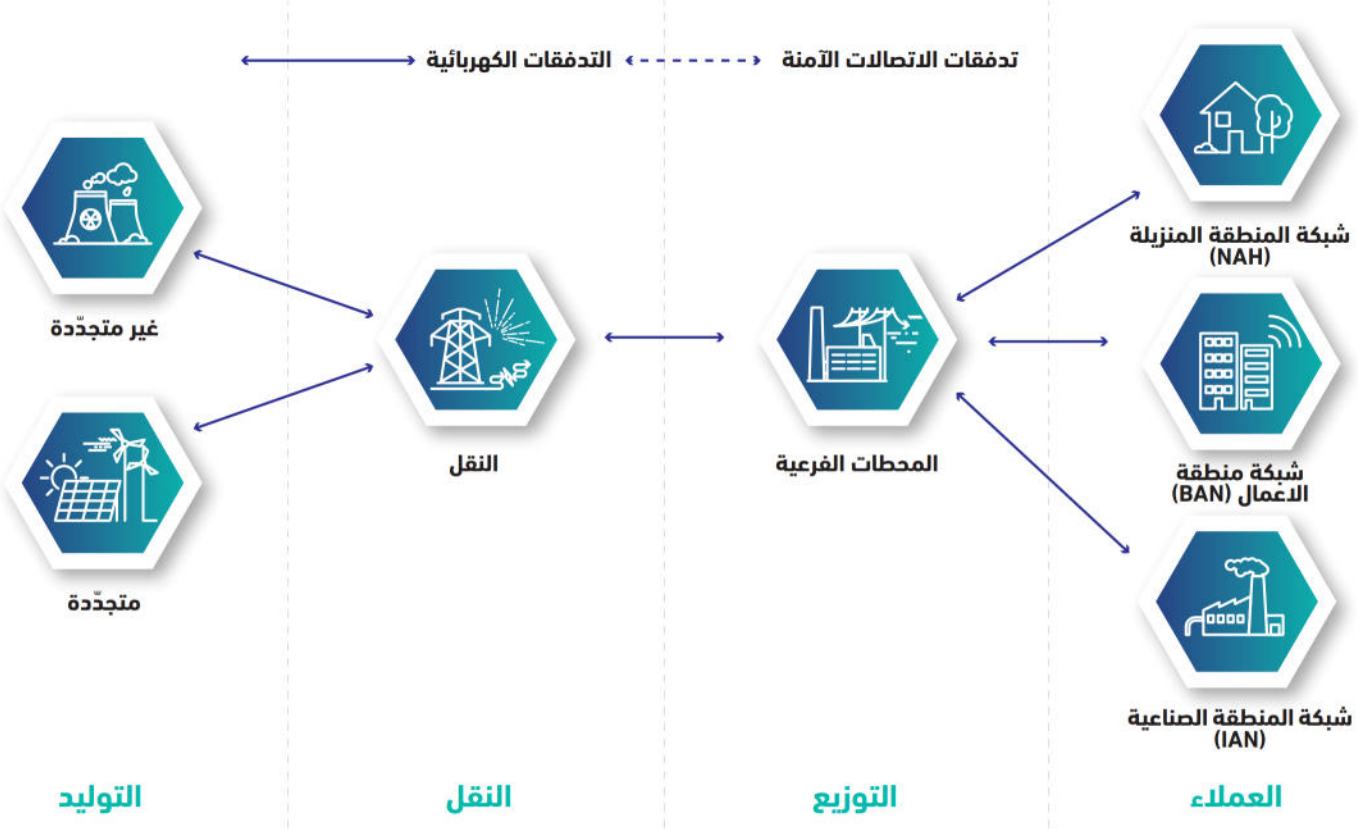
مكن تقسيم منظومة قطاع الكهرباء إلى أربعة مجالات واضحة، والتي تشكل مجتمعة جوهر البنية التحتية الكهربائية وهي: التوليد والنقل والتوزيع والاستهلاك.

التوليد – بشكل عام، يتم توليد الطاقة من المصادر الحرارية، والكهرومائية، والشمسية ومن الرياح. تستخدم المحطات الحرارية الحرارة الناجمة عن احتراق الوقود لتحويل الماء إلى بخار لدفع وتحريك مولدات الرياح (التوربينات) التي تقوم بدورها بتوليد الكهرباء. أغلب محطات توليد الطاقة هي محطات حرارية تعتمد بدرجة عالية على الوقود. لذلك، فإن أي انقطاع في إمدادات الوقود سوف يؤدي إلى خفض الطاقة الإنتاجية في هذه المحطات. تقع المحطات النووية ضمن فئة المحطات الحرارية، ورغم عدم وجود أي محطات نووية لتوليد الطاقة حالياً على المستوى الوطني، إلا أن المملكة تسعى لتفعيل هذه المحطات في السنوات القادمة [5].

في سبتمبر 2019، رصدت محطة الطاقة النووية 'كونداكولان' بالهند برمجية ضارة أطلق عليها (DTRACK) تهدف لسرقة المعلومات والاستطلاع في شبكاتها. على الرغم من أنّه لم يتمّ تصميم هذه البرمجيات على نحو خاص لاستهداف أنظمة التحكم الصناعية، غير أنها وفرت آلية فعالة لمراقبة المعلومات وجمعها حول البرمجيات المستخدمة في هذه المحطة والثغرات في الشبكة وذلك من أجل استخدام هذه المعلومات في هجمات مستقبلية [6]. إنّ الطابع الذي تتسم به هذه البرمجيات الضارة يمكّنها من البقاء غير مكتشفة لفترات زمنية طويلة في البيئة التقنية التي لا تتوفر فيها إجراءات وتقنيات متقدمة في الأمن السيبراني.

النقل – في هذه المرحلة، يتم نقل الكهرباء من موقع التوليد إلى محطات التوزيع الفرعية عبر طاقة عالية جداً، حيث توفر شبكات النقل نقاط ربط بين مختلف أجزاء شبكة الكهرباء مما يجعلها عرضة للهجمات السيبرانية، تشتمل البنية التحتية للنقل على الأبراج وخطوط الطاقة والنواقل وقواطع الدارات الكهربائية. عام 2016، تم استهداف محطة النقل الفرعية في أوكرانيا عبر هجوم سيبراني متطور ومعقد جداً باستخدام البرمجية الضارة (INDUSTROY-ER/CRASHOVERRIDE)،وهي البرمجية الأولى من نوعها التي تم تصميمها خصيصاً لاستهداف قطاع الكهرباء [7].

الشكل 4: نموذج لمنظومة شبكة الكهرباء

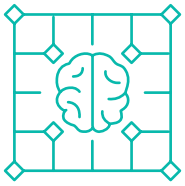


يوضح الشكل 4 التفاعلات بين هذه المجالات الأربعة لمنظومة الكهرباء.

يشهد نموذج منظومة شبكة الكهرباء تطوراً من نظام هرمي تنازلي إلى نظام الشبكة الذكية – وهي منظومة أكثر ديناميكية تمتاز بزيادة تبادل البيانات وظهور "المستهلك / المنتج"، أي المصدر الذي ينتج ويستهلك الطاقة [9].

التوزيع – تستقبل المحطات الفرعية الكهرباء عالي الجهد من شبكة النقل وتقوم بخفض القوة تدريجيًا وفق متطلبات شبكات المستهلكين المتنوعة. بعد ذلك، يمكن توزيع الكهرباء إلى المستهلكين عبر الكابلات تحت الأرضية أو الأسلاك العلوية وذلك اعتمادًا على قرب مناطق المستهلكين والكثافة السكانية في تلك المناطق. عام 2015، تعرضت ثلاثة مواقع توزيع في أوكرانيا لهجوم سيبراني بواسطة البرمجية الضارة (BLACK-ENERGY3)، والذي نتج عنه انقطاع التيار الكهربائي عن حوالي 225,000 مستهلك لمدة ست ساعات على الأقل.[8]

المستهلكون – يمكن تقسيم المستهلكين، بحسب المعهد الوطني للمعايير والتقنية (NIST)، إلى عدة فئات، هي: المنازل والشركات وشبكات المناطق الصناعية، حيث تمتاز كل واحدة من هذه الفئات بمتطلباتها الخاصة من حيث الأولوية وطاقة التوريد.



نحو شبكة الكهرباء الذكية

تشكل الكفاءة الدافع الأساسي وراء التوجه نحو الشبكات الذكية. ففي الماضي، كانت شبكات الكهرباء تُبنى بطاقة استيعابية فائضة حتى تتحمل حمولات الذروة، الأمر الذي كان يؤدي إلى عدم فعالية الأنظمة خارج فترات الذروة. لكن مع توفر شبكات الكهرباء الذكية أصبح لدينا العديد من الفوائد التي لم تكن موجودة في الشبكات التقليدية من قبل، وهي:

- الموثوقية من خلال تحسين آليات الأتمتة الخاصة بالرقابة الآنية والتحكم.
- تحقيق المستوى الأمثل من توليد ونقل وتوزيع الطاقة مما يؤدي إلى تقليص النفقات التشغيلية ونفقات الصيانة.
- تحسين مستوى الأمن السيبراني من حيث التحكم بالدخول، والتحقق من هوية المستخدم، والتصريح، والخصوصية وكشف حالات الاختراق.
- استيعاب مجموعة متنوعة من خيارات توليد الكهرباء: التوليد المركزي، الموزع، المتقطع، والمتحرك.
- تبني شبكات تنبؤية وذاتية المعالجة التي يمكنها اتخاذ إجراءات تصحيحية بشكل تلقائي.[10,11]

تُعدّ البنية التحتية لعدادات القياس المتقدمة (IMA) من التقنيات الرئيسية المطلوبة في أي شبكة ذكية وتُستخدم هذه البنية التحتية لمراقبة استهلاك الطاقة من خلال عدادات ذكية تقيس بشكل آني والذي يضمن توفير إمدادات آمنة وموثوقة من الكهرباء.[10] ففي حال الشبكة الذكية المثالية، تعمل الأجهزة الذكية ومعدات التوليد الموزعة (مثل الألواح الزجاجية للطاقة الشمسية) على نقل معدلات الاستهلاك ومعدلات الانتاج، على التوالي، إلى العدادات الذكية المتصلة بها لإمدادات الكهرباء. تقوم العدادات الذكية بعد ذلك بشكل آني بتغذية هذه البيانات وإرسالها إلى مزوّد الطاقة الذي يقوم بدوره بتحليل هذه البيانات حتى يتنبأ بشكل دقيق بمعدل الطلب عبر الشبكة بأكملها.

ومن شأن هذا التواصل المتبادل مع العدادات الذكية تمكين موزّدي الطاقة وشركات المرافق العامة من تعديل مقاييس مستوى الخدمة المقدمة للعملاء. ففي الواقع، يعمل هذا التواصل على تسهيل القدرة على تقليص إمدادات الطاقة أو قطعها عن المستهلكين الذين لا يقومون بدفع الفواتير. ولقد كانت شركات المرافق العامة في الماضي تعاني من صعوبات جمّة في تحقيق التوازن بين حمولة التيار الكهربائي وجمع الإيرادات. لذلك، فقد وفرت البنية التحتية للعدادات المتقدمة حلاً لكلا المشكلتين. علاوة على ذلك، لم تعد شركات الطاقة بحاجة لقراءة عدادات المستهلكين شخصيًا (عن طريق موظف) بعد أن أصبحت العدادات الذكية تنقل بدقة بيانات الاستهلاك والسجلات التشخيصية إلى مزودي الطاقة، الأمر الذي يساهم في توفير التكلفة، والتخلص من أسلوب الفواتير التقديرية.[12]

غير أنّه في حال تمكّن أحد منفّذي البرمجيات الضارة من الوصول إلى هذه البنية التحتيّة وإصدار أمرًا "مفتوحًا" لآلاف العدادات الذكيّة، فقد يؤدّي ذلك إلى تعطيل محطّة توليد الطاقة.

إنّ العناصر الجديدة في الشبكة الكهربائية الذكية، كالبنية التحتية للعدادات المتقدمة وازدياد الأطراف الجديدة في سلسلة التوريد المرتبطة بشكل مباشر بالشبكة الذكية، سيكون لها أثرًا في زيادة المخاطر السيبرانية، حيث تشكل هذه العناصر أهدافاً جاذبة للمهاجمين. لذلك، يركز هذا التقرير بشكل

رئيسي على التحديات في معالجة هذه المخاطر مع التوصيات العملية لمواجهتها.

لا شكّ أن ظهور الشبكات الذكية ودخول لاعبين جدد إلى سوق الكهرباء سوف يزيد من تعقيد المشهد التشريعي الذي لا يخلو بالأصل من التعقيدات. حيث سيتناول القسم التالي نظرة مقارنة أولية للوائح في كلّ من المملكة المتحدة والولايات المتحدة، وهما دولتان تتميزان بمستوى عالٍ من النضج السيبراني.

المشهد التنظيمي المتنوع

تُعتبر اللوائح التشريعية في العديد من القطاعات أداة فعالة لتحقيق التوافق بين مختلف ممارسات الأعمال وتحسينها. لقد ظلت اللوائح التشريعية في قطاع الكهرباء منصبّة لغاية هذا التاريخ على السلامة. غير أن الابتكارات التقنية الحديثة – بما في ذلك الانتقال نحو الشبكات الذكية – والمخاطر السيبرانية الناشئة عن ذلك استدعت تركيزًا مماثلًا على لوائح الأمن السيبراني والتي تهدف لتعزيز حماية القطاع و الأثر الذي قد ينتج عن ذلك من انقطاع التيار الكهربائي على نطاق واسع[13].

ساهمت اللوائح التشريعية والالتزام الداخلي لها في تحسين مستوى الحماية السيبرانية في قطاع الكهرباء، غير أن هذه اللوائح لا تكفي لوحدها لضمان مستوى حماية متقدم.[12] لذلك، وانطلاقًا من المنظور القائم على إدارة المخاطر السيبرانية، تتبع الدول سبل مختلفه لأنظمة ولوائح الأمن السيبراني وتعتمد فعالية هذه الأنظمة على درجة تطبيقها. علاوة على ذلك، يمكن لشركات الكهرباء أن تطبق أطر ومعايير إدارة المخاطر السيبرانية بطرق مختلفة اعتماداً على مستوى نضج هذه اللوائح التشريعية في كل دولة.

تتبنى المملكة المتحدة نهجاً قائماً على المخاطر السيبرانية في صياغة لوائحها التنظيمية التي تأخذ في الاعتبار مشهد التهديدات السيبرانية التي تواجه شركات الكهرباء. وتقيّم هذه اللوائح الأصول بحسب أهميتها وحساسيتها وذلك اتباعاً لمعايير مركز حماية البنية التحتية الوطنية، حيث توصي باتباع مجموعة من الضوابط السيبرانية بما فيها ضوابط الأمن المادي والشخصي بالاستناد إلى إطار التقييم السيبراني.

أما النهج الذي تتبعه الولايات المتحدة يعتبر أكثر إلزاماً وتفصيلاً في تحديد الإجراءات والضوابط السيبرانية، وقد شهد تطورًا كبيرًا في السنوات الأخيرة. على سبيل المثال، الأنظمة السابقة كانت توصي بتنصيب جدران الحماية في مختلف واجهات الشبكة دون أية توجيهات، بينما تحدد الأنظمة الحالية متطلبات إعدادات مخصصة ومفصلة لتهيئة جدران الحماية.

تفرض الولايات المتحدة هذه اللوائح والأنظمة بصرامة وتشترط على شركات الكهرباء الامتثال لها للحصول على رخصة التشغيل والاحتفاظ بها. بينما لا تتشدد المملكة المتحدة بفرض هذه اللوائح، كما أنها توفر حوافز أقل لشركات الكهرباء للاستثمار في الضوابط السيبرانية (التي قد تكون مكلفة). علاوة على ذلك، تبذل شركات عديدة في القطاع جهوداً كبيرة سعياً لتنفيذ المعايير والإرشادات السيبرانية والامتثال لها و الذي قد يصعب عليها فهم متطلباته وذلك نظرًا لافتقارها للمهارات الداخلية أو الموارد اللازمة للحصول على خبرات خارجية.[14,15]

من جهة أخرى، يزداد التعقيد بالنسبة للشركات المتعددة الجنسيات التي تعمل في دول مختلفة والتي تواجه تحدياً يتمثل في الاضطرار للامتثال لمزيج من الأطر والأنظمة السيبرانية في كل دولة. لذلك، فإن تبني النهج القائم على إدارة المخاطر السيبرانية على نطاق المنظمة والذي يعتمد على الموائمة بين الضوابط السيبرانية وأوليات الأعمال يعد النهج الأفضل لمواجهة هذا التحدي.[15]

بيئة الحماية السيبرانية المتغيرة

"يواجه قطاع الكهرباء عددًا متزايدًا من الهجمات الإلكترونية المتطورة."

استناداً لتقارير تهديدات الأمن السيبراني، أصبح جليًا أنّ قطاع الكهرباء يواجه عددًا متزايدًا من الهجمات السيبرانية المتطورة. وقد أظهرت الدراسات الحديثة أن قطاع الطاقة والموارد هو القطاع الأكثر استهدافاً في العالم من قبل هذه الهجمات. فقد احتلت منطقة الشرق الأوسط وأفريقيا المرتبة الخامسة بين المناطق المستهدفة في هذا القطاع.[16] ومن شأن الربط الإلكتروني المتنامي لمنظومة الكهرباء تجسير الهوة بين تقنيات أنظمة التحكم الصناعية والتقنيات التشغيلية بشبكات تقنية المعلومات، غير أنّ هذا الربط الإلكتروني يجعل من هذه الشبكات هدفاً لمنفذي الهجمات السيبرانية.

التهديدات السيبرانية المتزايدة

يتزايد عدد منفذي التهديدات السيبرانية القادرين على شن هجمات سيبرانية ضد قطاع الكهرباء، ويتراوح هؤلاء المنفذين ما بين مجموعات التهديد المتقدم (Advanced Persistent Threat APT) ذات المهارات العالية إلى المجرمين والإرهابيين ومخترقي الأنظمة الداخليين. ويعتبر هذا الأمر مصدر قلق كبير حاليًا بين خبراء الأمن السيبراني العاملون في القطاع، حيث أثار 64% من المشاركين في أحد الاستطلاعات مخاوفًا بشأن إمكانية وقوع هجمات متطورة، وتوقع 54% هجوماً على البنية التحتية الوطنية الحساسة خلال العام 2020. ويبدو أن هذه المخاوف صحيحة، نظراً لأن 25% من المجيبين ادعوا أيضاً أنهم تعرضوا لهجمات واسعة النطاق كانت مرتبطة بدول.[15]

تمتلك مجموعات التهديد المتقدم (APTs) أكبر قدر من الموارد لتطوير وتنفيذ الهجمات السيبرانية، ولكن المهاجمين من داخل المنظمة لا يزالون مصدر قلق كبير لفرق الأمن السيبراني، نظرًا لقدرتهم على فهم كيفية الوصول إلى أنظمة الكهرباء. وقد أظهرت الأبحاث كيف تُعزى الحوادث السيبرانية بشكل متزايد إلى مجموعات الجريمة المنظمة والدول، وأحيانًا بالتعاون مع بعضهم البعض.[1,15]

إن الاعتماد على الأجهزة والأنظمة التجارية الجاهزة والبروتوكولات المفتوحة في قطاع الكهرباء إلى جانب الربط بين البيئة التحتية لتقنية المعلومات وبيئة التقنية التشغيلية، سمح أيضًا للمهاجمين الأقل مهارة بالمشاركة في تنفيذ الهجمات السيبرانية حيث أصبح في متناول ايديهم العديد من الأدوات التي طورتها مجموعات التهديد المتقدم (APT).

فاليوم يواجه قطاع الكهرباء مهاجمين لديهم ثلاثة دوافع لشن الهجمات السيبرانية، حيث يتم استُهداف شبكات تقنية المعلومات في القطاع (عن طريق هجمات برامج الفدية) وذلك من قبل مجموعات الجريمة المنظمة التي تسعى لتحقيق مكاسب مالية، في حين يشن منفذون آخرون عمليات التجسس والتضليل السيبراني.

ومن المعروف أن المجموعات باتوا يستهدفون أنظمة التحكّم الصناعيّة وشبكات التقنية التشغيليّة ساعين إلى القيام بعمليات استطلاع قبل الهجوم أو التسبب في أضرار وتعطل واضحين.[17]

ونظراً لأن البنى التحتية الحديثة مثل الاتصالات السلكية واللاسلكية والخدمات المالية فضلاً عن البنى التحتية الوطنية الحساسة الأخرى، تعتمد بشدة على الكهرباء، فإنه من الممكن أن يكون لانقطاع التيار الكهربائي مجموعة واسعة من الآثار السلبية، والتي تتراوح من الإضرار بالسمعة إلى تعريض سلامة الإنسان للخطر. بالرغم من أن الشركات تعتمد على حلول طاقة احتياطية للتخفيف من آثار حالات الانقطاع، إلا أنها ليست مصممة للعمل لفترات زمنية طويلة.

في حين أن مشهد التهديدات السيبرانية أصبح أكثر غموضًا، إلا أن التقنيات والإجراءات الاستباقيّة يمكنها أن تساهم في الربط بن منفّذي الهجمات وعمليات الاختراق والهجمات السيبرانية. ويقدم الشكل 5 لمحة عامة عن أهم التهديدات السيبرانية التي تواجه قطاع الكهرباء.

ستستمر التهديدات السيبرانية المتطورة، وذلك مع استمرار التطور المتسارع للبرمجيات الخبيثة التي تستهدف أنظمة التحكم الصناعي ICS والتي يتم إعادة استخدامها واستغلالها بشكل متزايد ما يجعل من عملية معرفة مصدرها أكثر صعوبة.

بالتالي من المهم جدًا تقييم وتحديد نقاط الضعف والثغرات السيبرانية في البيئة التقنية في القطاع وتطبيق ضوابط الأمن السيبراني ذات العلاقة.

في هذا الصدد، هنالك مجالين رئيسين يثيران القلق: الأول، البنية التحتية القديمة غير الآمنة، والتي توفر نقاط دخول للمهاجمين وثغرات سيبرانية متزايدة خاصةً حين ترتبط بيئة تقنية المعلومات والبيئة التشغيلية. والثانية، سلسلة التوريد، والتي قد تكون عرضة للثغرات السيبرانية (مثل الأجهزة أو البرامج المقدمة من مزودي الخدمه الخارجيين) وإمكانية استغلالها من طرف ثالث.

يقدم الشكل 5 لمحة عامة عن أهم التهديدات السيبراني التي تواجه القطاع.

الشكل 5: أبرز التهديدات

البرمجية الضارة: TRISIS

تستهدف البرمجية الضارة TRISIS/TRITON أنظمة أدوات السلامة ((SIS، وتحديدًا وحدات التحكم في Triconex 3008 من إنتاج شنايدر إلكتريك. إن الاستغلال الناجح للثغرات سمح لمنفذي الهجمات بالحصول على امتيازات مرتفعة على النظام، والتي يمكن استخدامها بعد ذلك للتعامل مع أنظمة إيقاف التشغيل في حالات الطوارئ.[16]

البرمجية الضارة: INDUSTROYER/CRASHOVERRIDE

تستهدف هذه البرمجية الضارة، التي أثرت على شبكة الكهرباء في عام 2017، أنظمة ICS المستخدمة في شبكة الكهرباء. يمكن لهذه البرمجيات الضارة أتمتة انقطاع التيار الكهربائي الشامل. تتضمن البرمجية مكونات الاختراق التي تسمح لها بأن تتكيف مع أنظمة المرافق الكهربائية المختلفة، ومن الممكن أن يعاد استخدامها بسهولة، وكما يمكنها أن تهاجم أهداف متعددة في وقت واحد. تستطيع هذه البرمجية السيطرة على مفاتيح وقواطع الدوائر الكهربائية. هذه البرمجية الضارة هي البرمجية الضارة الأولى والوحيدة التي تم تطويرها خصيصاً لشبكة الكهرباء.

البرمجية الضارة: JOANAP / BRAMBUL

تستهدف برمجية Joanap وRAT Brambul لبروتوكول server mes- (SMB sage block)، البنية التحتيّة الحساسة. تسمح سلالتي البرمجية الضارة للمهاجمين بإجراء الاستطلاع السيبراني وتنفيذ الأوامر والتحرك عبر الشبكة[18]

البرمجية الضارة: STONEDRILL

يحتوي برنامج Stonedrill على وحدة مسح يمكنها محو البيانات خارج دليل ويندوز وأداة الوصول عن بعد (RAT). كما لديها أوجه تشابه مع البرمجيات الضارة Shamoon 2.0 التي استهدفت سابقاً مؤسسات في المملكة العربية السعودية ودول أخرى في الشرق الأوسط [19]

البرمجية الضارة: HAVEX

لقد تم توزيع برمجية Havex من خلال رسائل البريد الإلكتروني غير المرغوبة، ومواقع الموردين الإلكترونيّة المخترقة واستخدام أدوات الاختراق السيبراني. تقوم هذه البرمجية الضارة باستطلاع شبكة خوادم اتصالات المنصة المفتوحة (OPC) المستخدمة للتحكم في الأجهزة، وارسال معلومات عن الأنظمة إلى خوادم خارجية تحت سيطرة المهاجمين [20,21]

البرمجية الضارة: AGENT TESLA

صُممت هذه البرمجية الضارة لسرقة المعلومات، بما في ذلك بيانات التحقق من هوية المستخدم، صور من شاشة المستخدم، وكاميرا الويب، ومدخلات لوحة المفاتيح. يتم توزيع البرمجية الضارة عادة عن طريق رسائل التصيد الإلكترونية التي تحتوي على مرفق ضار بصيغة MS Word. و الذي يشكل تهديداً خطيراً على أنظمة التحكم الصناعية/التقنية التشغيلية لأن المعلومات التي يتم جمعها يمكن استخدامها لتخطيط وتنفيذ الهجمات السيبرانية. [22]

البرمجية الضارة: GREYENERGY

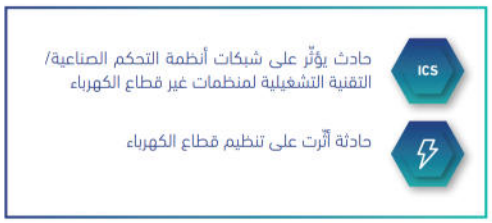
ويشتبه في أن هذه البرمجية الضارة هي من سلالة البرمجية BlackEnergy. في عام 2018، كشف الباحثون عن عملية ضد مؤسسات الطاقة في بولندا وأوكرانيا. هذه البرمجيات الخبيثة قادرة على استخراج البيانات الحساسة مع إزالة آثار أفعالها [16]

البرمجية الضارة: IMECAB / SORGU

لقد لوحظ وجود هذه البرمجية الضارة في شبكات قطاع الطاقة في الشرق الأوسط في منتصف عام 2018، فضلاً عن القطاعات المالية والحكومية وقطاع النقل. وغالباً ما يتم تثبيت البرمجية الضارة عبر هجمات استباقيّة، وتوفر للمهاجمين إمكانية الوصول عن بُعد للتسلل إلى الشبكات المستهدفة واستخراج البيانات الحساسة [16]

وقد استهدف المهاجمون الثغرات الأمنية في الأنظمة عالية الأهمية، بما في ذلك محطات الطاقة النووية، كما هو مبين أدناه، مما يوضح أثر الربط البيني المتزايد للشبكات حتى إلى أكثر المرافق أمنًا.

الشكل 6: الجدول الزمني لأبرز الحوادث السيبرانية في قطاع الكهرباء والقطاعات ذات الصلة



مارس 2000

محطة إدارة المياه الأسترالية

كان (Maroochy Shire) في أستراليا أول هجوم سيبراني مؤكد فعلياً على أنظمة التحكم الصناعية الرقمية. حيث تلاعب أحد الموظفين المسيئين بأنظمة التحكم وتحصيل البيانات لإطلاق كميات كبيرة من مياه الصرف الصحي في المنتزهات والممرات المائية العامة.[13]

يناير 2003

محطة الطاقة النووية الأمريكية

تسببت دودة (Slammer) بإغلاق نظام العرض في محطة ديفيس بيس للطاقة النووية، ما منع المشغلين من رؤية المعلومات الحساسة حول قلب المفاعل.[11]

يوليو 2010

منشأة نووية إيرانية

تسببت البرمجية الضارة (Stuxnet) بأضرار مادية لا يمكن إصلاحها على أجهزة الطرد المركزي لتخصيب اليورانيوم.[1]

أغسطس 2012

جهة في المملكة العربية السعودية

تسببت البرمجية الضارة (Shamoon/Disttrack) بمحي البيانات من نحو 30,000 جهاز حاسوب على شبكة تقنية المعلومات.

يناير 2014

العديد من شبكات أنظمة التحكم الصناعية الأمريكية والأوروبية المختلفة

تمت ملاحظة برنامج ضار يستهدف أنظمة التحكم الصناعي ومصمم خصيصاً للقيام بحملات تجسس سيبراني، تم الكشف عنه في الولايات المتحدة وأوروبا.[16]

يناير 2014

محطة الطاقة النووية اليابانية

عانت محطة الطاقة النووية (Monju) في اليابان ومحطة (Gori) في كوريا الجنوبية من سرقة المعلومات بسبب هجوم سيبراني باستخدام برمجيات خبيثة.[13]

ICS

ديسمبر 2014

مصنع الصلب الألماني

عطّل الهجوم السيبراني على معمل الصلب الألماني أنظمة إغلاق المصنع، ما تسبب بأضرار مادية جسيمة.[13]

ديسمبر 2015

شبكة الطاقة الأوكرانية 1 (الطاقة السوداء)

تم استخدام إطار الهجوم السيبراني المعقد المعروف باسم BlackEnergy3 لتوزيع البرنامج الخبيث KillDisk ، ما تسبب بإخراج الشبكة عن الخدمة لست ساعات.[1]

ICS

مارس 2016

سد مياه في الولايات المتحدة

هجوم سيبراني استهداف سد للمياه في الولايات المتحدة الأمريكية والدخول إلى نظام التحكم فيه.[23]

ICS

مارس 2016

محطة معالجة مياه لم يتم الكشف عنها

قام منفذو الهجوم السيبراني بتغيير المواد الكيمائية المضافة إلى إمدادات المياه، وتمكنوا من استغلال ثغرات ويب لم يتم إصلاحها في بوابة دفع العملاء المتاحة للجميع عبر الإنترنت.[16]

ICS

نوفمبر 2016

جهة في المملكة العربية السعودية

ظهرت البرمجية الضارة (Shamoon/Disstrack) مجدداً من عام 2012 واستهدفت 21 مؤسسة في المملكة العربية السعودية من بينها اثنتان للبتروكيماويات. ومع ذلك، لم يؤثر هذا الهجوم إلا على أنظمة تقنية المعلومات.

ديسمبر 2016

شبكة الطاقة الأوكرانية 2 (Industroyer)

أدى هجوم سيبراني إلى قطع الكهرباء لأكثر من ساعة. تم تطوير برنامج (Industroyer/Crashoverride) الخبيث لمهاجمة شبكات الكهرباء.[1]

ICS

أغسطس 2017

جهة في المملكة العربية السعودية

استهدفت البرمجية الضارة (TRITON/TRISIS) – عن بُعد – وحدات التحكم في نظام أدوات السلامة، حيث تسبب الخطأ في رمز التطبيق في فشل عملية التحقق من الصحة ما أدى إلى إطلاق التشغيل الآمن.

ICS

مارس 2019

مصنع ألمنيوم في النرويج

أصاب برنامج الفدية LockerGoga شبكات مصنع Norsk Hydro وأسفر عن عملية تشفير واسعة لمحركات الأقراص الصلبة في أجهزة الحاسوب.[24]

ICS

أبريل 2019

شركة النفط والغاز الفيتنامية

تم اكتشاف برنامج للتسلل إلى البيانات، يدعي SILKBUILDER، على الشبكات، وكان الغرض من الهجوم السيبراني هو سرقة بيانات ذات ملكية فكرية للجهة. [16]

ICS

مايو 2019

شبكات أنظمة التحكم الصناعية في الشرق الأوسط

تم اكتشاف البرمجية الخبيثة (FlushTunnel) المصممة لعملية الدخول الأولي، في شبكات أنظمة التحكم الصناعية في الشرق الأوسط. [16]

سبتمبر 2019

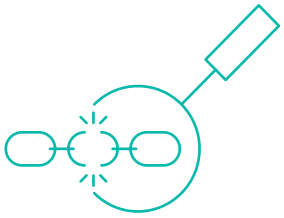
محطة للطاقة النووية في الهند

أصيبت شبكات الحاسوب في محطة كودانكولام للطاقة النووية ببرمجية ضارة لاستخلاص البيانات، تم ربط الهجوم بكوريا الشمالية. تشير التحليلات الى أنه تم إلحاق الضرر بشبكات تقنية المعلومات والتقنية التشغيلية [25]

مايو 2020

مشغّل سوق الكهرباء في المملكة المتحدة

أدّى هجوم مشبوه لبرمجيات الفدية ضدّ أنظمة تقنية المعلومات الخاصة بمشغّل ضخم لسوق الكهرباء في المملكة المتحدة إلى الكشف عن وثائق سرية على الشبكة المظلمة بما في ذلك نسخ عن جوازات السفر وسجلات مالية. ويُعتقد أنّ خدمة شبكة خاصة افتراضية (VPN) قديمة كانت المسار الذي أدّى إلى الدخول إلى المؤسسة.[26,27]



البنية التحتية القديمة غير الآمنة

لم يتم تصميم أنظمة التحكم الصناعي مع أخذ الأمن السيبراني بالاعتبار. في الواقع، لم يحظى مصطلح "الأمن السيبراني" بالإهتمام إلا في منتصف تسعينيات القرن الماضي، أي بعد 30 عامًا من بناء أنظمة التحكم الصناعي.[28] يعتبر التوافر والسلامة العاملين الرئيسيين عند تطوير أنظمة التحكم الصناعي، ممّا أدى إلى تطوير بيئة غير آمنة بطبيعتها. لا تزال البنية التحتية القديمة سائدة في قطاع الكهرباء في جميع أنحاء العالم وذلك بسبب التكاليف المالية لبناء البنية التحتية وصعوبة تحقيق متطلبات الانقطاع الضرورية لتطبيق وتفعيل التحسينات والترقيات اللازمة. على مر السنين، تمّ إدخال أنظمة تقنية المعلومات لأغراض تشغيلية وتجارية، مما أضاف طبقة أخرى من التعقيد والمخاطر السيبرانية.

مع تطور أنظمة التحكم الصناعي لتقديم الكفاءة التشغيلية والاتصالات ذات الاتجاهين مع الأجهزة والمعدات، أصبحت هذه الأنظمة أكثر عرضة للهجوم السيبراني، كما أنّ الانتقال من أجهزة الملكية الخاصة إلى البرمجيات التجارية الجاهزة، ومن البروتوكولات المغلقة إلى المفتوحة، يزيد من سطح الهجوم في القطاع.[14] غالبًا ما يتفاقم هذا الوضع بسبب انعدام التشفير أو المصادقة أو الدخول الآمن، بالإضافة إلى استخدام كلمات المرور السائدة للشركة المصنّعة للمعدات والأجهزة في شبكات التقنية التشغيلية.[29]

حيثما وجدت البنية التحتية القديمة، كانت الأنظمة المنعزلة من أولويات اهتمام مشغلي المصانع. في حين قد يشكّل العزل نوع من الانفصال عن الإنترنت، فما ينتج عن هذا العزل هو انعدام الرؤية عن هذه الاجهزة والقدرة على التحكم والادارة عن بعد او التحري عن وجود أي انشطة سيبرانية مشبوهة او ضارة. علاوة على ذلك، تبقى العديد من الأجهزة الطرفية في الشبكة غير آمنة إما بسبب القيود المالية أو الافتقار إلى الضوابط المناسبة.[14,15] فثمة توجه متزايد لتعريض الأجهزة في شبكات تقنية المعلومات والتقنية التشغيلية بشكل مباشر إلى الإنترنت، إما عن قصد أو غير ذلك، ما يمثل مدخل لجهات التهديد السيبراني التي تسعى إلى إيجاد طريقها إلى الشبكة.

تُعتبر مواقع التوليد والتوزيع موطنًا لكل من أنظمة تقنية المعلومات ومعدات السلامة المهمة مثل مرحلات الحماية. يُمثل التقاء التقنيات في تلك الأماكن هدفًا جاذبًا بشكل خاص لجهات التهديد السيبراني كونها توفر كلا المسارين إلى الشبكة وتحقق أكبر أثر ممكن.

أهداف للتهديد السيبراني: مواقع توليد وتوزيع الكهرباء

تستفيد مواقع توليد الطاقة الحرارية عادةً من الأمن المادي المتين الذي يضمن سلامة الإنسان ويهدف لحماية الخدمات العامة من المخاطر. غالباً ما تعاني مواقع توليد الطاقة النائية او البعيدة، مثل مولدات الرياح الموزعة على نطاق واسع، من مستوى منخفض من الأمن المادي، وذلك يتطلب الاتصال عن بُعد، ما يمثل طريقًا إضافيًا لدخول المهاجمين.

أثبتت الهجمات السيبرانية على المولدات أنها قد تتسبب بتدمير مادي (مثلًا أثناء التجارب الخاضعة للرقابة) في حين أن التأثير أو فقدان منشأة التوليد قد تسبب ضغطًا كافيًا على الشبكة ما يؤدي إلى انقطاع الكهرباء محليًا. في مثل هذه الحالة، قد تكون الاستجابة الأولى لمهندس التحكم هي التخلص من الحمل ما يقلل من الناتج أكثر. بالتالي، ليس من الضروري أن يتعين على منفذي الهجوم السيبراني تجاوز أنظمة التحكم مباشرةً لينجحوا في إحداث التعطيل، وإنما بإمكانهم تحقيق أهدافهم عبر خلق ظروف تُجبر مهندسي التحكم على التقليل من الناتج.[29]

دوكو (Duqu)

إنّ دوكو هو عبارة عن جزء من برمجية ضارة مصممة بشكل يعتمد على البرنامج الخبيث الشهير Stuxnet الذي أُستخدم لتعطيل عملية التخصيب النووي الإيراني. يمتلك "دوكو" القدرة على مراقبة سلوك الأجهزة وتحديد الثغرات السيبرانية فيها، و يمكن للبرمجية القيام بهجوم سيبراني عبر إصدار الأوامر ومراقبة تأثيرها. تم العثور على هذه البرمجية في شبكات توليد الكهرباء وشبكات النقل والتوزيع ويمكنه القيام بهجوم مخصص عبر إصدار الأوامر ومراقبة تأثيراتها.[27]

تواجه شركات توزيع الكهرباء مهمة صعبة تتمثل في حماية الأجهزة الطرفية والأنظمة والشبكات، ماديًا ومنطقيًا، وذلك بسبب انتشار أصولها على مساحات جغرافية واسعة. إنّ عملية التوزيع، بالاقتران مع عملية النقل، توفّر الكهرباء لشريحة كبيرة من السكان وبالتالي قد يكون للهجوم السيبراني أثر على نطاق واسع. كما أن التحول الرقمي خلال السنوات الماضية لا سيما في عملية التوزيع، يتطلب توفير مستوى متقدم للحماية من الهجمات السيبرانية.

من جانب آخر، قد يكون مهندسو التحكم في مواقع التوليد والتوزيع النائية أقلّ دراية بضوابط الأمن السيبراني من أولئك الذين يعملون في مواقع توليد كبرى حيث يتم تطبيق ضوابط الأمن السيبراني بمستوى أعلى. إن أجهزة الحاسوب المحمولة الخاصة بالمهندسين هي غير آمنة بطبيعتها وقد تتسبب بثغرات ونقاط ضعف عند الاتصال بالشبكة، إما بسبب تصفح مواقع الكترونية ضارة أو بسبب عدم تطبيق التحديثات والإصلاحات الأمنية للبرمجيات.

قد تعتمد بعض الأنظمة على الدخول الفعلي لتثبيت تحديثات البرامج أو الإصلاحات الأمنية، وبالتالي قد تبقى عرضه للثغرات السيبرانية لأشهر أو سنوات، وذلك بحسب أولويات جدول الصيانة. إن أنظمة تقنية المعلومات في مواقع التوليد والتوزيع توفر رابطًا مهمًا لشبكات التقنية التشغيلية والشركة بشكل أوسع وكذلك للوصول للإنترنت. وفي حين أن هذا الربط ضروري للعمليات التجارية الفعالة في عالم اليوم، إلا أن ذلك يمنح جهات التهديد السيبراني فرصة للوصل للشبكة.

مدخل للوصول: أنظمة تقنية المعلومات

تُعتبر أنظمة تقنية المعلومات هدفًا سهل الوصول له نسبيًا كونها تحتوي أنظمة تشغيل وأجهزة تجارية، وعادة تكون متصلة بالإنترنت. وفي حين أن أنظمة تقنية المعلومات يتم تطبيق التحديثات والإصلاحات الأمنية عليها أكثر من نظيرتها في التقنية التشغيلية، إلا أنها تكون مبنية على بنية تحتية قديمة ولذلك يمكنها تحقيق مستوى نسبي من الحماية السيبرانية.

هنالك توجه رئيسي في قطاع الكهرباء لزيادة الربط بين بيئة تقنية المعلومات وشبكات التقنيات التشغيلية/ أنظمة التحكم الصناعية من أجل رفع مستوى القدرة على الإدارة على نطاق واسع. غير أنّه على الرغم من تنفيذ ضوابط الأمن السيبراني، يمكن لمنفذي الهجمات السيبرانية الاستفادة من أي اتصال فعلي أو منطقي للانتقال من شبكة لأخرى.

تمثل أنظمة التشغيل التي لم تطبق الإصلاحات الأمنية خطرًا على البيئة التقنية وتعتبر أحد أبرز نقاط الضعف في إدارة الأمن السيبراني. حيث يمكن لهجوم سيبراني مثل التعرض لبرمجيات الفدية أن يتسبّب بتعطيل حقيقي في الأعمال، ومجددًا، قد يجد المشغلون أنفسهم مجبرون على إنهاء الخدمة أو التقليل منها لمنع انتشار التهديد السيبراني حتى لو كان الاحتمال ضئيل في عبور البرمجيات الضارة إلى شبكات التقنية التشغيلية وخلق مخاطر تتعلق بالسلامة.[29] وقد يكون التعافي من هجوم برنامج الفدية أكثر فعالية عندما يتم استعادة الأنظمة من النسخ الاحتياطية غير المتضررة. ومع ذلك، في حال لم يتم المحافظة على النسخ الاحتياطية واختبارها، قد تصبح عملية التعافي طويلة ومكلفة وذات أثر كبير.

تعدين العملة الرقمية المشفرة (Cryptojacking)

إنّ تعدين العملة الرقمية المشفرة هي عبارة عن هجوم يشكل خطرًا على شبكات البنية التحتية الحساسة، حيث تستخدم برمجيات تعدين العملة الرقمية المشفرة الضارة قوة معالجة الحاسوب لتعدين (أو الحصول على) العملة الرقمية المشفرة ما يؤدي إلى تحقيق مكاسب مالية لمنفذ الهجوم السيبراني. إن عملية التعدين المشفرة هي عملية ذات استهلاك عالي للطاقة، وبالتالي يسعى منفذ الهجوم السيبراني بطبيعة الحال إلى تفادي هذه التكلفة عبر اختراق أجهزة الحواسب التي تعود لأشخاص أو مؤسسات.

ارتفعت قيم العملة الرقمية المشفرة بشكل خاص في النصف الأول من عام 2019، ما انعكس على زيادة حالات الإصابة ببرمجيات التعدين الرقمي المشفرة الضارة. في الربع الأول من عام 2019، ارتفع نشاط برمجية التعدين الرقمي المشفرة بنسبة 629% في حين انخفض نشاط برمجية الفدية بنسبة 32%.[16]

تنتشر برمجيات تعدين العملة الرقمية المشفرة الضارة في جميع أنحاء العالم حيث تم العثور عليها في شبكات التقنية التشغيلية في جميع أنحاء آسيا، حيث كان يسعى المهاجمون للاستفادة من قوة الأنظمة والأجهزة المشتركة لمكونات نظام التحكم الصناعي.[16] في روسيا، كانت جهات التهديد السيبراني مسؤولة عن تثبيت 6000 جهاز تعدين مشفر في منشأة طاقة مهجورة.[30] لذلك يُنصح المسؤولين عن البنية التحتية في قطاع الكهرباء بتوخي الحذر من برمجيات تعدين العملة الرقمية المشفرة الضارة لأنها من الممكن أن توفر نقطة دخول لهجمات سيبرانية أكثر خطورة.

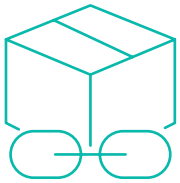
هدف لتحقيق الأثر الأكبر: مرحّلات الحماية (PROTECTIVE RELAYS)

تُعتبر مرحلات الحماية مكونات ذات قيمة عالية في أنظمة الأمان في بيئات أنظمة التحكم الصناعية وقد صمّمت لتنبيه مهندسي التحكم بالترددات والتيارات الخطيرة في الأجهزة والمعدات الكهربائية. بالرغم من ذلك، فإنه نادرًا ما يتم تطبيق ضوابط الأمن السيبراني عليها.[29] قد يعتبر من الصعب شن هجوم سيبراني مباشر على مُرحّلات الحماية نظراً لأنّ ذلك يتطلّب معرفة عميقة بتصميم النظام وخصائص المرحلات والتصاميم الإلكترونية والبرامج. مع ذلك، فإنه من المرجح أن يمتلك مهندسو التحكم اليوم الذين هم على دراية بهذه الأنظمة بعض الخبرة في تطوير البرمجيات الخبيثة، والتي قد تمكّنهم من تطوير برمجية ضارة مستهدفة أو أن يتم توفير بيانات تصميم النظام لجهات التهديد السيبراني الأخرى، الأمر الذي يسلط الضوء على الحاجة إلى إجراء المسح الأمني للعاملين في الوظائف ذات الصلاحيات الهامة والحساسة وتطوير ثقافة إيجابية للأمن السيبراني في المؤسسة.

أظهرت الهجمات السيبرانية على شبكة الكهرباء الأوكرانية واقع التهديدات السيبرانية على هذا القطاع وإمكانياتها في تقويض الإجراءات القياسية لاستعادة الطاقة.

الهجوم السيبراني على أوكرانيا عام 2016

تسبّب الهجوم السيبراني عام 2016 على شبكة الكهرباء الأوكرانية في انقطاع التيار الكهربائي لمدة ساعة واحدة. استهدف أحد أجزاء الهجوم ثغرة سيبرانية في أربع مُرحّلات حماية رقمية غير محمية. يعتقد المحللون أن انقطاع التيار الكهربائي كان سيسمح للمهندسين بإعادة تنشيط المعدات بهدف استعادة الشبكة، ولكن مع خروج مُرحّلات الحماية من الخدمة، كان سيؤدي ذلك إلى أضرار مادية كارثية على خطوط الطاقة والمحولات. لحسن الحظ، لم ينجح هذا الجزء من الهجوم بسبب خطأ في تهيئة الشبكات.[31]



تداخل سلسلة التوريد

في حين من الممكن أن تقدم مواقع التوليد والتوزيع طرقاً مباشرة إلى الشبكة في قطاع الكهرباء، فكذلك توفر سلسلة التوريد والأطراف الخارجية مجموعة واسعة من الطرق إلى البنية التحتية الوطنية الحساسة في القطاع حيث ثبت أنها أحد الأسباب الرئيسية للهجمات السيبرانية. اذ من الممكن اختراق الأجهزة خلال عملية التصنيع لإضافة أبواب خفية يمكن استغلالها من قبل منفذي الهجوم السيبراني للدخول إلى شبكات التقنية التشغيلية بعد تركيب الجهاز. يوفر الموردون الخارجيون بدءاً من موردي خدمات المحاسبة إلى بائعي أنظمة التدفئة والتهوية والتكييف نقاط اتصال يمكن استغلالها في الهجمات السيبرانية أو الهندسة الاجتماعية. على سبيل المثال، تعد تقنية "Island Hopping" تهديداً شائعًا على سلسلة التوريد حيث يستغل منفذو الهجوم السيبراني الثقة والمعاملات التي تتمتع بها المؤسسة مع مورديها، من خلال طرق عدّة، للدخول إلى تلك المؤسسة.[32]

يتمّ تبادل البيانات بشكل كبير في شبكات الكهرباء الحديثة، الأمر الذي يشكل تحديًا للشركات لمراقبة إنتاج البيانات وجمعها وتحليلها وتوزيعها والتخلص منها، وخاصّة عندما تشارك أطراف خارجية في هذه العملية. ونظرًا لارتفاع حجم البيانات التي يتمّ جمعها ومعالجتها، تزداد المخاطر السيبرانية المرتبطة بانتهاك البيانات بشكل كبير.

يعكس الإنتقال التدريجي للعدادات الذكية وتوزيع إنتاج الطاقة المتجددة التوجه الجديد لتفاعل المستهلكين مع الشبكة في القطاع. تتطلب تلك التقنيات المتطورة ضوابط أمن سيبراني متقدمة وحساسات رقمية وبنية تقنية حديثة، لتعزيز الحماية من المخاطر السيبرانية المتزايدة. على سبيل المثال، يمكن استغلال ثغرة سيبرانية في نظام التحكم بالألواح الشمسية التي يتم تركيبها بشكل واسع من أجل التسبب بتعطيل الخدمة في الشبكة عبر إحداث مشكلة في موازنة الضغط والتأثير على عملية التوريد. تُعتبر العدادات الذكية فريدة من نوعها، بالاضافة لاستخدام البنية التحتية للعدادات المتقدمة اللاسلكية، وذلك من ناحية أنها توفر مدخلًا ماديًا سهلًا إلى أحد المكونات الرئيسية لشبكة الكهرباء المستقبلية. في هذا الصدد، أظهرت إحدى الدراسات كيفية استخدام فرن مايكرويف لتشويش الإشارات في شبكة الحساس اللاسلكي للبنية التحتية للعدادات المتقدمة، ما تسبّب بانقطاع الخدمة.[33]

مع تطور قطاع الكهرباء، تظهر المخاطر السيبرانية التي قد يكون مصدرها عدد من الجهات والشركات الجديدة والأقل نضجًا من الناحية السيبرانية في القطاع. من ناحية التوريد، يقوم مزودو الطاقة المتجددة بتزويد الشبكة بالطاقة ولكن إذا ما تم ذلك دون اتباع الضوابط الأساسية للأمن السيبراني فقد تتعرض الشبكة الى خطر التعرض للتهديد السيبراني من خلال الوصول الى نقاط غير آمنة في الشبكة.

إن ازدياد عدد الهجمات السيبرانية على شبكات أنظمة التحكم الصناعية وشبكات الكهرباء في السنوات الأخيرة يشير إلى أن الأمن السيبراني في قطاع الكهرباء هو بعيد عن ما يجب أن يكون عليه. فبالرغم من بدء تفهم القيادات في قطاع الكهرباء عن أهمية الأمن السيبراني، إلّا أنّه ثمة عدد من التحديات التي تحول دون تنفيذ استراتيجيات الأمن السيبراني وضوابطه.

التحديات لتعزيز القدرات السيبرانية

"التعقيد المتأصل في قطاع الكهرباء يعني تحدي الحفاظ على الضوابط التقنية للأمن السيبراني وتحديثها."

يواجه قطاع الكهرباء نفس التحديات التي تواجهها القطاعات الأخرى من حيث نقص المهارات والكوادر في مجال الأمن السيبراني وأثر المخاطر السيبرانية لسلسلة التوريد. ومع ذلك فإن طبيعة قطاع الكهرباء وأهميته تولّد منظوراً فريداً لهذه التحديات.

أولاً، إن عدد المتخصصين في الأمن السيبراني الذين هم على دراية بأنظمة التحكم الصناعي قليلون جداً. ثانياً، إن الجمع بين منظومة قطاع الكهرباء المعقدة وأهميته الحساسة على الصعيد الوطني يمثل العديد من الفرص والدوافع لأثر المخاطر السيبرانية لسلسلة التوريد والأطراف الخارجية أكثر من القطاعات الأخرى.

منذ عقود تتوفر لأنظمة وشبكات تقنية المعلومات حلول الأمن السيبراني مثل برامج مكافحة الفيروسات وجدران الحماية، إلا أنّه لم يتمّ أخذ حماية التقنية التشغيلية بالاعتبار إلا في السنوات الأخيرة. ونظراً لإزدياد وتيرة التحول الرقمي يمكن أن تصبح استراتيجيات الأمن السيبراني والضوابط قديمة في غضون بضع سنوات، حيث تُصمم البنية التحتية للتقنية التشغيلية عادةً ليتجاوز عمر خدمتها 20 عامًا.[34] بالتالي، من المهمّ فهم الدور الذي يؤدّيه عمر الخدمة من حيث متطلبات الأمن السيبراني الخاصة بكلتا التقنيتين.

الموائمة بين متطلبات الأمن السيبراني

تتطلب كلاً من تقنية المعلومات والتقنية التشغيلية مجموعة مختلفة تمامًا من متطلبات وأولويات الأمن السيبراني نظرًا لاختلاف وظائفها وأهميتها وتأثيرها المحتمل على السلامة البشرية. حيث تواجه العديد من المؤسسات صعوبات في موائمة استراتيجيات وضوابط الأمن السيبراني الخاصة بتقنية المعلومات والتقنية التشغيلية، والتي غالبًا ما تستند على الاعتقاد الخاطئ بأن ضوابط الأمن السيبراني الخاصة بتقنية المعلومات هي أيضًا فعالة للتقنية التسغيلية.[15] من الممكن أيضًا أن يفسر خبراء تقنية المعلومات والتقنية التشغيلية معايير الأمن السيبراني بشكل مختلف. بالتالي، يتعين على القيادات العليا تحديد أولويات متطلبات الأمن السيبراني الخاصة بتقنية المعلومات والتقنية التشغيلية وضمان التوافق مع المعايير ذات الصلة.

تختلف أهداف أمن البيانات في بيئات تقنية المعلومات والتقنية التشغيلية بشكل ملحوظ. فغالبًا ما تكون السرية هي الأولوية الرئيسية في أمن تقنية المعلومات حيث تكون السلامة والتوافر تمثل الأولوية في بيئة التقنية التشغيلية لأنّ نسبة السماح بالتأخر الزمني على الشبكة تعتبر منخفضة جدًا. على سبيل المثال، قد تتسبب رسائل التحكم المشوهة أو المتأخرة في حدوث انقطاع أو ضرر في الأجهزة والأنظمة. ومع ذلك، يبقى التركيز الرئيسي في بيئات التقنية التشغيلية هو على السلامة البشرية وموثوقية النظام وحماية المعدات وشبكات النقل والتوزيع، أكثر من أمن البيانات. لقد أدى هذا التركيز على العمل والسلامة إلى تطوير بروتوكولات وبيئة لشبكة التقنيّة التشغيليّة غير آمنة بطبيعتها. لذلك يجب على مديري الأمن السيبراني النظر بدقة في متطلبات الأمن السيبراني المتباينة عند الاتصال بالبنية التحتية لتقنية المعلومات والتقنية التشغيلية، على النحو المحدد في الشكل 7 أدناه.

الشكل 7: المتطلبات الرئيسية لبيئات تقنية المعلومات والتقنية التشغيلية [4,12]

التقنية التشغيلية	المتطلبات السيبرانية	تقنية المعلومات
1. التوافر 2. السلامة 3. السرية	أمن البيانات	1. السرية 2. السلامة 3. التوافر
عالية جداً، إعادة التشغيل غير مقبولة	التوافر	متوسطة، إعادة التشغيل مسموحة
حَرِجة	دقة التوقيت	التسامح مع التأخيرات
20 سنة فأكثر	العمر الزمني	3-5 سنوات
قليلة الحدوث	إدارة التحديثات	منتظمة
متقطعة	اختبارات الأمن السيبراني	محدَّدة المواعيد، محتملة الإلزام
مستقرة , هرمية التصميم	البنية التحتية	مرنة، ديناميكية، تعتمد على شبكات معرّفة بالبرمجيات
أنظمة التشغيل الخاصة، الشبكات الخاصة، بروتوكول آي إي سي 61850 و بروتوكول الشبكة الموزعة DNP	التقنية	أنظمة تشغيل متنوعة وشبكات عامة وبروتوكولات تستند إلى TCP / IP
منخفضة لكنها متزايدة	توعية الأمن السيبراني	مستوى نضج متقدم

واجهت العديد من المؤسسات تحدياً متمثلاً في الحفاظ على ضوابط الأمن السيبراني التقنية وتحديثها نتيجة التعقيد المتأصل في البنية التحتية لقطاع الكهرباء، حيث يرى بعض مدراء أمن المعلومات في القطاع أن هناك أكثر من 300 حل أمني مختلف يتطلب الإدارة. ويمكن ملاحظة أثر ذلك في الشبكة الذكية وعلى العمر الزمني للبنية التحتية.

الشبكات الذكية

قد تنطوي آثار متطلبات الأمن السيبراني المتباينة على تأثير كبير على انتشار الشبكة الذكية واستخدامها الفعال. وسيكون للانتقال إلى شبكة ذكية آمنة انعكاسات كبيرة، حيث تستوجب متطلبات أمن سيبراني إضافية، بما في ذلك التحقق من الهوية والتوافر وقابلية التدقيق وإمكانية المراجعة - لا سيما في شبكات التقنية التشغيلية - لتقليل مخاطر الاتصال بالإنترنت على نطاق واسع. علاوة على ذلك، فإن إدخال أجهزة الكشف اللاسلكية على البنية التحتية تضيف أهداف جديدة للهجمات السيبرانية. وبما أنّ التقنية تلعب دوراً مهماً في الأمن السيبراني، فقد أوصى معهد أبحاث الطاقة الكهربائية في الولايات المتحدة الأمريكية الشبكات الذكية بتطبيق سياسات الأمن السيبراني وتقييماتها وتدريباتها بالإضافة إلى حلول الأمن السيبراني التقنية. كما سيضمن استيفاء متطلبات الأمن السيبراني الإضافية هذه انتقال رسائل التحكم السليمة فقط على الشبكة وتمكين تحليل التحقيق الجنائي الكامل في مراحل الاكتشاف والاستجابة وتطبيق التوصيات عند الاستجابة لحوادث الأمن السيبراني.

من جهة أخرى، سيكون هناك تأثير إضافي على العدادات الذكية، حيث أنها أحد المكونات الرئيسية للشبكة الذكية وتتطلب آليات مصادقة قوية لتقليل مخاطر احتيال الفوترة. ويجب أن توفر هذه الآليات حلّاً إداريًا رئيسيًا قابلًا للتطوير وفعالًا وآمنًا ويمكنه توفير المصادقة ولكنه في الوقت ذاته، يوفر أيضًا سهولة إعادة التوزيع الرئيسية عندما ينتقل المستهلك بين موردي الطاقة.

لذلك، يجب على مديري الأمن السيبراني ومصنّعي المعدات مراعاة طريقة تنفيذ المصادقة في الأجهزة الصغيرة ذات القدرة الحاسوبية المنخفضة مثل أجهزة الكشف اللاسلكية المذكورة سابقًا.

إن تبادل البيانات التي يتم إنشاؤها من خلال الشبكة الذكية مع أطراف خارجية لأغراض الفوترة، واستخراج البيانات، وتشخيص المورّدين، وتحليل الاستخدام، وتطبيق متطلبات المنزل الذكي، كل ذلك يتطلب مستوى إضافيًا من التعقيد فيما يتعلق بحماية البيانات. كما يجب مراعاة متطلبات الخصوصية بما يتماشى مع توقعات العملاء والتشريعات المحلية والعالمية.[33]

العمر الزمني للخدمة

سيكون لمتطلبات الأمن السيبراني المتباينة بين بيئة تقنية المعلومات والتقنية التشغيلية أيضا التأثير في سياق العمر الزمني للبنية التحتية الوطنية الحساسة. فبينما تحسن الأمن السيبراني في قطاع الكهرباء في السنوات الأخيرة، حيث بدأت مجالس إدارة الشركات بأخذ الأمرعلى محمل الجد، إلّا أنّه لا يزال متخلفًا عن باقي القطاعات – مثل قطاع الخدمات المالية – بحوالي خمس إلى سبع سنوات.

يعود هذا التأخير جزئيا إلى الاختبار الدقيق الذي تخضع له الضوابط والسياسات الجديدة لتفادي تعطل الخدمة للعمليات الحساسة، وينطوي هذا التفاوت في المدى العمري للبنية التحتية على طريقة التصميم، حيث اعتاد متخصصو تقنية المعلومات اليوم على مرونة الحوسبة السحابية الافتراضية التي يمكن تعديلها بسرعة وبتكلفة منخفضة نسبيا. خلافاً لذلك، يتطلب تصميم التقنية التشغيلية أنماطًا لها رؤية طويلة الأمد لتوفير متطلبات الأمن السيبراني كجزء من التصميم منذ البداية.

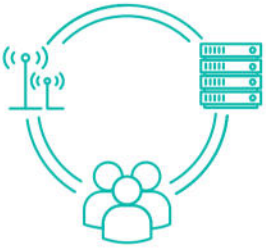
علاوة على ذلك، يعبر مسؤولو الأمن السيبراني عن عدم وجود حافز في مؤسساتهم لإعطاء متطلبات الأمن السيبراني الأولوية على متطلبات الكفاءة، حيث يُنظر إلى الأمن السيبراني غالبا على أنه كلفة يصعب قياس مردودها على الاستثمار. حيث تتطلب معالجة ثغرات الأمن السيبراني الناتجه عن البنية التحتية القديمة نفقات رأسمالية ضخمة في أغلب الأحيان، كما أن الخدمات اللوجستية الرامية للحفاظ على الشبكة بكامل طاقتها، أثناء إجراء هذا الإصلاح الشامل، ليست عملًا سهلًا.

وبما أنّ القطاع مهتم بتحقيق الأرباح وخفض التكاليف، فإن الدافع للاستثمار في الأمن السيبراني سيظل أولوية متدنية إلى أن تقوم التشريعات بفرض سياسات ومبادرات الأمن السيبراني الرئيسية.

النقص في كوادر الأمن السيبراني

يعدّ النقص الحاد في موظفي الأمن السيبراني ذو الكفاءة العالية من أبرز التحديات التي تواجه جميع القطاعات في جميع أنحاء العالم، حيث يتخطى الطلب العرض دائما.[14] وكثيرًا ما يتفاقم هذا النقص بسبب قلة الاستثمار في التدريب والطبيعة المنعزلة لقطاع الكهرباء سواء في التوليد، وشبكات النقل والتوزيع، والمعدات الاستهلاكية.[15]

أظهرت دراسة أجريت عام 2019 حول التوظيف في مجال الأمن السيبراني في قطاعات متعددة, أن المؤسسات التي لديها أقل من 500 موظف تعاني حاليا من نقص حاد في الموظفين في مجال الأمن السيبراني المتخصصين في أنظمة التحكم الصناعي/التقنية التشغيلية.[35] وتعرب المؤسسات التي يقل عدد موظفيها عن 5,000 موظف عن مخاوف تتعلق بتلبية مهام الأمن السيبراني الحساسة. وتتلخص أبرز الصعوبات فيما يلي: فهم الآثار التشغيلية لهجمات الأمن السيبراني، مستوى كفاءة أقل في إدارة الأصول الحساسة ومراقبتها، مستوى ثقة أقل في مهارات اكتشاف التهديدات السيبرانية والاستجابة لها. حيث يتطلب قطاع الكهرباء موظفين متخصصين في الأمن السيبراني وخبراء في أنظمة التحكم الصناعي وهؤلاء الموظفين المتخصصين قليلون جداً والطلب عليهم متزايد.



سلاسل التوريد المعقدة

يواكب التطور والخصخصة والعولمة في القطاع زيادة مستمرة في مستهدفات الهجوم السيبراني في منظومة القطاع. وتزداد مجالات الارتباط في منظومة قطاع الكهرباء أكثر من أي وقت مضى ابتداء من البنى التحتية المترابطة وصولًا إلى الموردين الجدد في السوق والشركات متعددة الجنسيات التي تعمل في جميع دول العالم. كما تشكل الأطراف الخارجية مخاطر سيبرانية اضافية من خلال سلسلة التوريد، حيث يقع العبء على عاتق المؤسسات في القطاع لتحمل المسؤولية للتأكد من ضمان تحقيق متطلبات الأمن السيبراني في الأنظمة والخدمات في الشبكة والبنى التحتية. [36]

يمكن أن تؤدي ملكية سلاسل التوريد المعقدة والمتنوعة على مستوى المؤسسة إلى إدارة الموارد بشكل غير فعال، وخاصة فيما يتعلق بالمعلومات الاستباقية عن المخاطرالسيبرانية في سلاسل التوريد والقدرة على تطبيق متطلبات المراجعة والتدقيق على الموردين بدقة. كما يجب على المؤسسات النظر في تحسين إدارة عمليات تقييم سلسلة التوريد وعمليات الشراء، من خلال معايير الدولية مثل IEC 62443-2-4، لتوحيد معايير المشتريات ضمن المؤسسة. [1,37]

تسعى مجالس إداراة الشركات في القطاع بشكل متزايد للانتقال إلى الحوسبة السحابية وذلك لتوفير التكاليف وتحقيق التوافقية والقابلية للتوسع في البنى التحتية والخدمات. حيث تتم استضافة حلول البرمجيات كخدمة من الطرف الثالث بشكل عام في الحوسبة السحابية، ولكن هناك العديد من الأمثلة على تسريب البيانات وغيرها من الحوداث السيبرانية بسبب تدني مستوى تطبيق متطلبات الأمن السيبراني في بيئات الحوسبة السحابية. لذلك، يجب التأكد من تطبيق موردي البرمجيات ومزودي الخدمات السحابية لسياسات ومتطلبات الأمن السيبراني وتقييمها والاخذ بعين الاعتبار مستوى تقبل المخاطر في أعمال المؤسسة[1]. الجدير بالذكر أن مزودو الخدمات السحابية يعتمدون على نماذج المسؤولية المشتركة والتي يمكن أن تختلف قليلاً بين مزودي الخدمة ومستويات الخدمة المقدمة، ولهذا يجب أن تدرك المؤسسات أن الانتقال إلى الحوسبة السحابية لا يلغي بالضرورة المخاطر السيبرانية أو مسؤوليات المؤسسة تجاه إداراة هذه المخاطر.

يتم تطوير منتجات وحلول جديدة ويتمّ تسويقها لقطاع الكهرباء بوتيرة متسارعة، وبالتالي يعدّ ضمان تحقيق متطلبات الأمن السيبراني أمراً جوهرياً عند بناء وتوسيع البنى التحتية الحساسة. حيث يرتفع مستوى الثقه بالمنتجات من البرمجيات والأجهزة التي تجتاز اختبار تحقيق متطلبات الأمن السيبراني لكونها تعمل على النحو المنشود وقد تم اختبارها وفق قائمة من الثغرات االسيبرانية المعروفة. الجدير بالذكر أنه في المملكة المتحدة، يوفر نظام "شهادة ضمان المنتج التجاري" الذي طوره مركز الأمن السيبراني البريطاني ضمانا لمستوى تحقيق متطلبات الأمن السيبراني للعدادات الذكية.[38] حيث يأكد ذلك فاعلية تطبيق الضوابط الوطنية والتي تعطي مصداقية عالية في اختبارالتحقق من متطلبات الأمن السيبراني في البنى التحتية الحساسة.

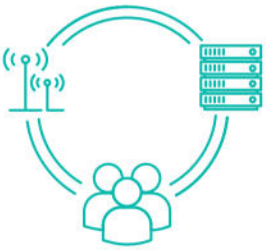
قد يكون تنفيذ التحديثات الأمنية أمراً صعباً حيث يتطلب ذلك من كل شركة مصنعة للمعدات والأنظمة التحقق من صحة التحديثات لكلّ مكون في النظام قبل توزيعها على العميل. إضافة إلى ذلك، عادةً ما تكون شروط العقد مع موردي المعدات والأنظمة مختلفة لكلّ محطة كهرباء، ممّا يجعل تنفيذ برنامج شامل لإدارة التحديث أكثر صعوبة.

في حين أن التحديات التي يواجهها قطاع الكهرباء أثرت على تقدمه من حيث النضج السيبراني، إلا أنها تحديات يمكن تجاوزها. ويقدم القسم التالي توصيات في ثلاثة مجالات رئيسية هي: العامل البشري والإجراءات والتقنيات وكذلك أهمية التعاون في منظومة قطاع الكهرباء.

التوصيات

> يوفر الأمن والتعاون والتنظيم والمعايير فرصًا لدفع قطاع الكهرباء إلى مستوى أعلى من النضج في مجال الأمن السيبراني

تدعم التوصيات التاليه إداراة المخاطر السيبرانية التي تواجه قطاع الكهرباء. حيث إنّ تطبيق توصيات الأمن السيبراني المبنية على أفضل الممارسات العالمية أدناه والتي تشتمل على العامل البشري والإجراءات والتقنيات، وتركز كذلك على تعزيز التعاون واتباع أنظمة ومعايير الأمن السيبراني من أجل تعزيز النضج في الأمن السيبراني على مستوى القطاع.



العامل البشري – تعزيز ثقافة الأمن السيبراني

يُعدّ التهديد السيبراني الذي قد يواجه مؤسسات قطاع الكهرباء من داخل المؤسسة - وبغير قصد - أكبر في بعض الأحيان من التهديد من الجهات الخارجية. حيث أن أبرز أنواع التهديدات السيبرانية تعتمد على رسائل التصيد الالكتروني والتي تهدف لإيصال البرمجيات الضارة إلى البنية التحتية لتقنية المعلومات. الجدير بالذكر أن معدل نجاح هذه التهديدات السيبرانيه يتزايد، أولاً لأنّ الكثير من الموظفين يجهلون أساليب التهديدات والهجمات السيبرانية، في حين يواصل المهاجمون استخدام رسائل التصيُّد الإلكترونية وتقنيات الهندسة الاجتماعية الأكثر تعقيدًا. توصلت دراسة أجريت عام 2020 إلى أن عدد المستخدمين الذين نقروا على روابط خبيثة في رسائل البريد الإلكتروني ارتفع بنسبة 80٪ من شهر يناير إلى شهر أبريل، ويعود ذلك جزئيًا إلى ارتفاع رسائل التصيد الإلكترونية ذات الصلة بوباء كورونا Covid-19.[39]

ثانيًا، لا يعطي غالبية العاملين في مؤسسات الكهرباء الأولوية للأمن السيبراني. لذلك فإنه من المهم تقييم المرشحين قبل التوظيف للتأكد من أن لديهم دراية وخلفية مناسبة، وعند الضرورة، قد يتطلب من المرشحين الخضوع لعملية مسح أمني أكثر شمولاً خاصة للعاملين في مجال الأمن السيبراني والوظائف الحساسة في قطاعات البنى التحتية الحساسة. لهذا السبب، قد تسعى الجهات الوطنية لبناء كوادر من الخبراء في الأمن السيبراني في مجال التقنية التشغيلية لأداء المهام إلهامه والحساسة.

إن ضمان ظروف عمل عادلة وعلاقات جيدة للعاملين والثقافة الإيجابية تساهم إلى حد كبير في زيادة ولاء العاملين للمؤسسات. علاوة على ذلك، يمكن للمؤسسات توظيف حلول الأمن السيبراني التي تعمل على تحليل سلوك المستخدمين وتساعد في الكشف عن الأنشطه المشبوهة على الشبكة.

تُعدّ برامج التوعية بالأمن السيبراني والتصيّد الالكتروني من الأساليب المهمة لرفع مستوى الوعي بالمخاطر السيبرانيه لدى جميع العاملين في قطاع الكهرباء. ويجب تقديم هذه البرامج لكلّ مستويات المؤسسة ودعمها من قبل القيادة العليا لتعزيز ثقافة الأمن السيبراني بصورة فعاله. كما أنّه من الضروري تحفيز الموظفين وإشعارهم بالثقة في المبادرة للإبلاغ عن الاشتباه بحوادث سيبرانيه أو محاولات التصيد الالكتروني إذا اعتقدوا أنهم ربما فتحوا مرفقا أو رابطًا خبيثًا دون قصد.

كما يوصى بتعزيز ثقافة الأمن السيبراني بشكل أكبر من خلال توفير دورات تدريبية متقدمة في الأمن السيبراني للموظفين المعنيين الذين يمتلكون مهارات ومعرفة وخبرات في أعمال قطاع الكهرباء. حيث إن تعليم الأمن السيبراني لمهندس التحكم الصناعي يعتبر أسهل بكثير من تعليم خريج الأمن السيبراني حول أنظمة التحكم الصناعية.[40] لذلك، تحتاج مؤسسات قطاع الكهرباء إلى تنمية مواهبها الحالية لسد فجوة المهارات حيث يمكن تدريب جميع الموظفين على المستوى الأساسي للأمن السيبراني والذي سيكون له أثر إيجابي على منظومة قطاع الكهرباء ضد التهديدات السيبرانية وحماية البيانات.

إن تطوير قدرات الموظفين في مجال الأمن السيبراني سيدعم رفع مستوى نضج الأمن السيبراني للمؤسسة، وسينعكس ذلك على تحسين أداء ورضا الموظفين. وتعتبر برامج التطوير والتدريب الداخلي للموظفين بديلاً فعالاً للتوظيف الخارجي في ظلّ فجوة مهارات الأمن السيبراني العالمية.

الإجراءات – تعزيز حوكمة الأمن السيبراني

توفر حوكمة الأمن السيبراني التوجيه والإشراف الاستراتيجي لإدارة الأمن السيبراني داخل مؤسسات قطاع الكهرباء والمنظومة بشكل كامل. كما تلعب دوراً أساسياً في موائمة برامج تقنية المعلومات والتقنية التشغيلية وأمن البيانات والأمن المادي من أجل تنفيذ استراتيجية قوية وشاملة للأمن السيبراني في منظومة قطاع الكهرباء.[4]

يجب أن يتم دعم برنامج شامل للأمن السيبراني مع ارتباط إدارة الأمن السيبراني بالإدارة العليا في المؤسسة والذي يضمن تطبيق البرنامج بفعالية أكبر[15]، كما يجب تطبيق والتزام الموظفين بسياسات الأمن السيبراني في المؤسسة.

يتطلب نجاح برنامج الأمن السيبراني اشراف الإدارة العليا على برنامج إدارة المخاطر السيبرانية المرتبطة بمنظومة الكهرباء وسلسلة التوريد والتي تعزز الصمود السيبراني في المؤسسة.[41] علاوة على ذلك، ينبغي النظر في المخاطر السيبرانية التي تمثلها المؤسسة وثقافتها وممارساتها تجاه منظومة الكهرباء، مع التركيز على أهمية وحساسية مؤسسات المنظومة والدور الذي تلعبه البنية التحتية للمنظومة على المستوى الوطني.

يجب تطبيق سياسات الأمن السيبراني في تحديد وإدارة الأصول التقنية والتشغيلية، والالتزام بضوابط الأمن السيبراني، وإجراءات المراجعة والتدقيق بشكل مستمر[15]. بناءاً على ذلك يجب أن يتم تصميم برنامج للأمن السيبراني يهدف لحماية الأصول الهامة والحساسة و التي تشتمل على الموظفين والإجراءات والتقنيات[1]،والذي يعدّ أمراً جوهرياً لتطوير برنامج أمن سيبراني قوي لإدارة المخاطر السيبرانية الخاصة بقطاع الكهرباء على نطاق أوسع.[4]

من وجهة نظر تنظيمية، توفر ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC) في المملكة العربية السعودية ضوابط شامله للأنظمة الحساسة والتي تهدف لتعزيز قدرات الأمن السيبراني لهذه الأنظمة. وتعتبر هذه الضوابط استكمالاً للضوابط الأساسية للأمن السيبراني (ECC) من خلال توسيع نطاق الضوابط الأساسية لتوفير حماية إضافية للأنظمة الحساسة في مواجهة المخاطر [56].تينار بيسلا

التقنية – تعزيز كفاءة التقنية

يتم تبني وتطبيق عدد من حلول الأمن السيبراني التقنية في قطاع الكهرباء. حيث تم تصميم بعضًا من هذه الحلول التقنية لتحقيق متطلبات أساسية مثل عزل البنية التحتية القديمة عن الإنترنت، بينما تتوفر حلول تقنية متقدمة في الأمن السيبراني مثل تقنيات الكشف عن التهديدات السيبرانية المتقدمة والحماية منها.

بالنسبة للمؤسسات ذات مستوى نضج سيبراني متقدم، فإنه أصبح من الضروري فحص وتقييم أنماط الهجوم السيبراني الذي قد تتعرض له المؤسسة باستخدام منهجية عالمية لتصنيف الخطوات أو الأنشطة التي قد يتخذها المنفّذ أثناء تنفيذ التهديد السيبراني. إن كل من إطار عمل Mitre ATT&CK[42] و Lock-heed Martin Cyber Kill Chain [43] تعد من الأطر المتقدمة والمتخصصة في المجال والمعترف بهما عالميًا، ، والتي تدعم المؤسسات التي تتطلع إلى تحسين دفاعاتها.

يتطلب من إدارة الأمن السيبراني تطبيق حلول أمن سيبراني متقدمة، كما هو موضح أدناه، وذلك لتعزيز دفاع وقدرات الصمود السيبراني في المؤسسة.

التصميم الآمن لتعزيز الأمن السيبراني

يعد التصميم الآمن في الأنظمة والأجهزة في البنية التحتية أمراً بالغ الأهمية لتعزيز الصمود السيبراني وخاصة في البنية التحتية للقطاع والتي قد يمتد العمر الزمني لها لعقود من الزمن.

- تثبيت أجهزه وأنظمة مزدوجة للتعامل مع تعطل أجزاء من النظام، كما تدعم تطبيق التحديثات بشكل مستمر
- ضمان تنوع التقنيات المستخدمة لتجنب وجود نقطة تعطل مركزية في البنية التحتية
- الحفاظ على توفر أنظمة وأجهزة احتياطية والتي يتم فحصها بشكل مستمر
- تصميم أنظمة تحكم مقاومة للعطل لمنع الحالات الحرجة من الانقطاع في الخدمة أو الانقطاع الكلي
- تطوير أنظمة تحكم تحقق مبدأ "الفشل الآمن" fail-safe لمنع حصول الضرر المادي
- تطبيق متطلبات واجراءات التطويرالآمن للبرمجيات للحدّ من مخاطر الثغرات السيبرانية
- اختيار أنظمة التشغيل التي يتم تقديم الدعم التقني لها من قبل المورِّد، كما يتم توفير وتطبيق تحديثات أمنية لها بشكل منتظم.
- تأمين مصدر إمداد الوقود للمولدات الاحتياطية في حالة الانقطاع الكلي والذي قد ينتج بسبب تهديد سيبراني

الأمن السيبراني للشبكة

سيساعد تأمين الشبكات وعزلها في حماية البنية التحتية التشغيلية التي قد تعتبر غير محمية بطبيعتها من الهجمات السيبرانية

- استخدام الشبكات الخاصة حيثما أمكن لتقليل التعرض للهجمات السيبرانية
- استخدم الشبكات المحلية الافتراضية VLAN وتطبيق التشفير الآمن على مستوى الشبكة
- تطبيق إصدارات محدثة وآمنة من بروتوكولات الشبكة
- تطبيق ضوابط الأمن السيبراني للوصول الأمن للشبكة
- ضمان تزامن الوقت على مستوى الشبكة
- تطبيق الإعدادات الآمنة لجدران الحماية وأنظمة كشف ومنع الاختراق IDS/IPS والشبكات الفرعية لتحقيق متطلبات العزل على مستوى الشبكة والأمن متعدد المستويات (Defense in Depth)
- الحفاظ على الأجهزة آمنة مادياً مع تطبيق متطلبات الوصول الآمن لمراكز البيانات والمناطق ذات الأهمية والحساسية العالية
- استخدام جهاز الأمن السيبراني صمام البيانات (Data diode)، لنقل البيانات في اتجاه واحد عند الحاجة لتعزيز حماية المعلومات القيمة والشبكات من الهجمات السيبرانية.
- عزل أنظمة التحكم الصناعي (SCADA) وأنظمة إدارة الطاقة عن الشبكة المركزية

سياسات الأمن السيبراني المدارة مركزياً

توفر الإدارة المركزية لسياسات الأمن السيبراني رؤية وتحكم شامل في حماية البنية التحتية على مستوى المؤسسة

- تطبيق التحديثات الأمنية للأنظمة والأجهزة على مستوى البنية التحتية لتقنية المعلومات والتقنية التشغيلية بشكل دوري
- تطبيق سياسات وحلول الأمن السيبراني التقنية لحماية الأجهزة والخوادم على مستوى الشبكة
- تطبيق الاعدادات الآمنة وتحصين الإعدادات الافتراضية على مستوى الشبكة، بحيث يتم تحديد خط أساس آمن وتطبيق إجراءات إدارة التغيير في حال لزم الأمر.
- توفير نسخ احتياطية مركزية منتظمة لجميع مكونات البنية التحتية من أنظمة وخوادم وأجهزة
- تطبيق الاستخدام الآمن لوسائط التخزين على مستوى البنية التحتية
- إجراء عمليات التدقيق والمراجعة للوصول الآمن لمكونات البنية التحتية
- تطبيق أنظمة إدارة الهوية والوصول IAM الآمن وتطبيق سياسات الأمن السيبراني لصلاحيات الوصول
- تطبيق سياسات حماية الوصول للحاسبات والأنظمة والأجهزة على مستوى البنية التحتية

لوائح ومعايير الأمن السيبراني

إن التقارب بين بيئة تقنية المعلومات والتقنية التشغيلية يلغي الحدود بين متطلبات السلامة والأمن السيبراني في القطاعات الصناعية، حيث يمكن أن يكون للتهديدات السيبرانية آثاراً مباشرة وغير مباشرة على سلامة الإنسان. الأمر الذي يتطلب التنسيق والتوافق في تطوير تشريعات الأمن السيبراني مع الجهات المسؤولة عن تشريعات السلامة لضمان النتائج الأكثر فعالية وشمولية للحد من المخاطر.

ستستفيد المشاريع الدولية مثل هيئة الربط الكهربائي لدول مجلس التعاون الخليجي ومشروع الربط الكهربائي السعودي-المصري؛ وغيرها من اتفاقيات الكهرباء الدولية المستقبلية من تطوير اللوائح التشريعية والمعايير بين الدول المشاركة[44]. حيث يعد التوافق والتنسيق خطوة رئيسية نحو التكامل التنظيمي الناجح.

من ناحية أخرى، فإنه يجب تبني المعايير الدولية لتعزيز التكامل المتبادل بين مشغلي الكهرباء على الصعيد الدولي. كما يجب مراجعة أفضل الممارسات والمعايير المعتمدة بشكل دوري وتحديد إطار زمني للمؤسسات لتنفيذ هذه المعايير.

بالتالي، فإن فعالية اللوائح التشريعية والمعايير تزيد مع قابليتها للتنفيذ، كما يجب تطوير هذه المعايير بحيث تكون مرنة وقابلة للتكيف مع التحديات السيبرانية المتقدمة[14]. فعلى سبيل المثال، قد يلزم اعتماد معايير التشفير الكمي الآمن لحماية البيانات وحماية الاتصالات المستقبلية من الهجمات الحاسوبية الكمية (quantum computer-based attacks).

ينبغي تعزيز التواصل والتعاون فيما يتعلق بالشريعات والمعايير بشكل وثيق، والتنسيق على المستوى الوطني والإقليمي والدولي وزيادة القدرة على التكيف مع الفرص والمخاطر والتقنيات الجديدة.

التعاون على صعيد الأمن السيبراني

أدى تزايد الهجمات السيبرانية على قطاع الكهرباء إلى زيادة الحاجة إلى التعاون الوطني والإقليمي والدولي وتبادل المعلومات الاستباقية حول التهديدات السيبرانية. كما أصبح هذا الأمر أكثر إلحاحا نتيجة للتقارب المتزايد بين بيئة تقنية المعلومات والتقنية التشغيلية، مما أوجد متطلبات متجددة للأمن السيبراني والسلامة والتي باتت ذات أولوية عالية لقطاع الكهرباء.

من المستبعد أن تتم مواجهة التهديدات السيبرانية المتطورة والمعقدة بمعزل عن البيئة المحيطة بها. حيث تعتمد استراتيجية الأمن السيبراني القوية والناضجة بشكل متزايد على التعاون الوثيق بين أصحاب المصلحة، وأهمهم:[45]

- منتجي وموزعي الكهرباء،
- مصنّعي العتاد والبرمجيات،
- الخبراء في في مجال الأمن السيبراني،
- الحكومات، و الجهات التشريعية.

يسهم التعاون في توفير استجابة أكثر فعالية للتهديدات السيبرانية تعود بالفائدة على المنظومة بشكل كامل .حيث يمكن أن يشمل ذلك تبادل لمعلومات مثل الثغرات السيبرانية وبيانات التهديد السيبراني، بالإضافة إلى الدروس المستفادة من الاستجابة للحوادث السيبرانية.[46]

تحديات التعاون

توجد تحديات عديدة أمام التعاون الفعال بين أصحاب المصلحة، والتي يُنصح المسؤولين في المؤسسات في قطاع الكهرباء بدراستها لتعزيز مجالات الشراكة. وتشمل هذه التحديات ما يلي:

تزايد عدد الجهات في القطاع

لا يزال من الضروري أن يقوم قطاع الكهرباء على المستوى الدولي بتعزيز مشاركة المعلومات حول المعلومات الاستباقية والتهديدات السيبرانية بحيث تشمل جميع أصحاب المصلحة المعنيين في القطاع.

بالرغم من التعاون القائم بين عدد محدود من الجهات الرئيسية في القطاع، إلا أن عدد الجهات وأصحاب المصلحة في القطاع في تزايد. ويلعب العديد منهم أدوارا مهمة في إنتاج الكهرباء وتوزيعها واستهلاكها، وذلك يدعو إلى إدراج هذه الجهات في التعاون في مجال الامن السيبراني. كما يجب مشاركة المعلومات الاستباقية للتهديدات السيبرانية بطريقه موثوقه , وتوفير الحماية اللازمة عند مشاركة هذه المعلومات الهامة لتجنب التعرض للمخاطر السيبرانية.

حماية البيانات التجارية

يعتمد التعاون الفعال على المستويات الوطنية والإقليمية والدولية بشكل كبير على التفاعل بين القطاعين العام والخاص[47] وتختلف العلاقة بين القطاعين العام والخاص اختلافاً كبيراً بين البلدان، وكذلك الحال بالنسبة لتوقعات الشركات والمسؤولين الحكوميين الذين يتبادلون معلومات حساسة تجاريًا (على سبيل المثال كجزء من استراتيجية صناعية). إن تبادل المعلومات الاستباقية المتعلقة بالتهديدات السيبرانية ، تتطلب الأخذ بعين الاعتبار الالتزام بضوابط لضمان حماية المعلومات الحساسة تجارياً.[48]

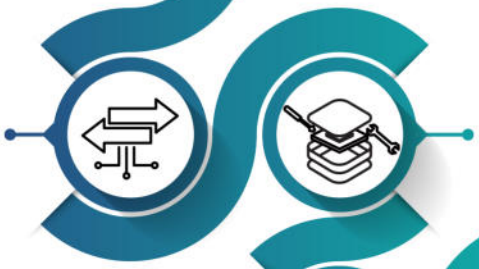
الاتفاق على إطار عمل مشترك

سعيًا لتحقيق تعاون فعال، فإن ذلك يتطلب من أصحاب المصلحة تطوير إطار عمل مشترك لهيكلة وحوكمة مشاركة المعلومات وتحليلها والذي يشتمل على الطرق والنماذج والأدوات اللازمة لتحقيق أهداف أصحاب المصلحة.[47]

يجب على أصحاب المصلحة الاتفاق على تصميم نموذج موحد لمشاركة المعلومات، الأمر الذي قد يكون صعبًا خصوصًا عندما يؤيد كل صاحب مصلحة النموذج الذي يناسبه أكثر من غيره. وقد يصبح هذا تحدياً في بعض الأحيان (على الأقلّ ليس في المراحل الأولى من التعاون)، ولكن وضع إطار عمل مشترك للتعاون سيسهل بناء برنامج التعاون المشترك وسيساعد في المحافظه عليه وتحقيق الأهداف المرجوه منه.

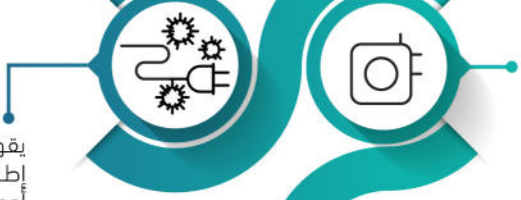
أمثلة على التعاون في مجال الأمن السيبراني

على الرغم من التحديات والقيود المذكورة أعلاه ، فقد ظهر عدد من الأمثلة الناجحة في قطاع الكهرباء ، مما يمهد الطريق لتعاون أعمق. وتشمل التالي:



أنشأ مشروع DEnSeK (المعرفة بأمن الطاقة الموزعة 2013-2015) المركز الأوروبي لتبادل معلومات الطاقة وتحليلها (EE-ISAC). وقد مكّن من تبادل المعرفة والمعلومات في الوقت الحقيقي بشكل تفاعلي وأنشأ شبكة توعية بالحالة للكشف عن التهديدات الناشئة.[46]

في أكتوبر 2019 ، دخلت الحكومة الأمريكية في اتفاقية مع منطقة البلطيق لحماية شبكات الطاقة من الهجمات الإلكترونية .[49] ويهدف التعاون إلى مشاركة أفضل الممارسات وزيادة الوعي التكنولوجي من أجل تشجيع استبدال البرامج والأجهزة القديمة والتحديث الأوسع. من قطاع الكهرباء.



يقوم المعهد الوطني الأمريكي للمعايير والتقنية (NIST) بتنفيذ إطار عمل بحثي تعاوني "للمنتجات والخبرات الفنية التي يمكنها تأمين أجهزة إنترنت الأشياء المتعلقة بالطاقة". [50] سيحقق الباحثون في تأثير الأجهزة المتصلة في الشبكات الكهربائية من أجل تحسين اكتشاف البرامج الضارة والتخفيف وإنشاء إرشادات أمنية لأفضل الممارسات للمالكين والمشغلين لاستخدامها في بيئاتهم.

يركز قانون الحماية الأمريكي (حماية الموارد على الشبكة الكهربائية باستخدام تقنية الأمن السيبراني) على تعزيز وضع الأمن السيبراني للشبكة الوطنية ويفوض وزارة الطاقة "لتحفيز هذه القطاعات على تكتيكات متقدمة في تقنية الأمن السيبراني".[46]

لم يعد التعاون في مجال الأمن السيبراني ومشاركة المعلومات في قطاع الكهرباء نوعًا من الترف وإنّما هو عنصر أساسي في استراتيجية الأمن السيبراني الناضجة. وعلى الرغم من التعقيدات والتحديات التي يواجهها بناء إطار التعاون الفعال، إلا أن الفوائد التي يوفرها ستحقق ميزة تنافسية ووعيًا سيبرانيًا متطوراً لتلك المنظمات المساهمة في ذلك.

الاتجاهات المستقبلية

سيتّسم مستقبل صناعة الكهرباء على المدى المتوسط والطويل بالابتكار التقني والاضطراب للمشاركين في السوق من جميع الأحجام ، وسيكون من الضروري مراعاة الأمن السيبراني عند تطوير وشراء ونشر هذه التقنيات الحديثة.

يمرّ قطاع الكهرباء حاليًا بمرحلة من التطور الهام، وثمّة عاملين رئيسيين على الأقل يتميز بها هذا التغيير وهما الجهات وأصحاب المصلحة الجدد في القطاع والابتكار التقني.

أصحاب المصلحة الجدد في القطاع، الأولويات الجديدة:منهجية تركز على المستهلكين

يتميز قطاع الكهرباء على المستوى الوطني بوجود مجموعة من أصحاب المصلحة الرئيسيين التقليدين الذين يديرون إنتاج وتوزيع الكهرباء إلى العملاء الذين تم وضعهم في نهاية هرم المنافع في سلسلة المستفيدين في القطاع.

ونشهد الان تحولاً متزايداً في هذه الآلية المتعارف عليها إلى وجود آليه وعلاقات أكثر تعقيدًا وديناميكية يقودها التفاعل المشترك، حيث يؤدّي عدد أكبر من أصحاب المصلحة أدواراً جوهرية في القطاع. وهناك عاملان رئيسيان يؤثران على هذه العلاقات االمتنامية.

المستهلكون المنتجون

أدّى التقارب بين تقنية المعلومات والتقنية التشغيلية دورًا رئيسيًا. ولأن هذا التقارب يحدث في الشبكات الذكية، فقد تم تحسين وظيفة الشبكة حيث أصبحت المنصة الضرورية التي تمكن هاتين التقنيّتين من التفاعل بالاعتماد عليها. ويتم تمكين ذلك من خلال ترقية البنية التحتية للاتصالات خاصة إلى تقنيات الجيل الخامس(5G)، مما يوفر إمكانية التقدم التجاري والتقني.

ستمكن هذه التطورات العملاء من لعب دور جديد يتمثل في مشاركة المعلومات عن الاستهلاك الفوري وبيانات توليد الكهرباء تدريجياً. وتهدف هذه العملية المستمرة والمتكررة إلى تحسين التوليد والتنبؤ بمقدار الاستهلاك وكفاءة الشبكة.[51]

كما ذكرنا أعلاه، هناك تحديات تتعلق بمعالجة هذه البيانات بشكل آمن في المصدر وأثناء نقلها وبعد وصولها إلى وجهاتها المختلفة. إن إعتماد شبكة الكهرباء بشكل متزايد على شبكة الاتصالات تضيف اعتماداً على عاملاً جديداً. كما تطرح المخاوف الأخيرة بشأن أمن مزودي معدات الجيل الخامس تساؤلات حول مدى ملاءمتها لدعم البنية التحتية الوطنية الحساسة.

لضمان السرية والتكامل فإنه يجب تشفير البيانات وتوقيعها رقمياً لدى المصدر وعند انتقالها من طرف إلى طرف اخر. ومع ذلك، فقد لا تمتلك الأجهزة منخفضة الطاقة مثل اجهزة الاستشعار والعدادات الذكية القدرة أو الطاقة الاحتياطية اللازمة لتحقيق ذلك. وعليه يجب على مشغلي الكهرباء النظر في كيفية دعم هذه الأصول الموزعة لتوفير القدرات اللازمة لتحقيق متطلبات الأمن السيبراني.

البنية التحتية المتجددة والمتوزعة

يتطلب التركيز المجتمعي المتزايد على التنمية المستدامة – بمعنى أشمل الانتقال إلى مستقبل منخفض الكربون – تغييراً ثقافياً والتحول إلى مصادر جديدة لتوليد الطاقة. وهذا ما يقود الابتكار والاستثمار في هذا القطاع وخاصة فيما يتعلق بتوليد الطاقة من الرياح والطاقة الشمسية، وتقنية المنازل الذكية، والمَرْكَبات الكهربائية.[51]

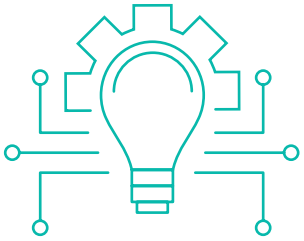
يقوم العملاء أيضًا بتركيب مولدات متجددة والتفاوض على أسعار الكهرباء وفواتيرها مباشرةً. أصبح هؤلاء (المستهلكون المنتجون) جزءًا لا يتجزأ من دورة الكهرباء - فهم المستهلكين والموردين في آن واحد -، حيث سيؤدي هذا في النهاية إلى تغيير متطلبات الطاقة من خلال التركيز بشكل أكبر على خيارات العملاء ومنحهم القدرة على أن يصبحوا جزءاً متأصلاً في الشبكة.

إن قدرة المستهلك (المنتج) على توفير البيانات العائدة إلى الشبكة تضيف مجالاً جديداً للهجمات السيبرانية والتي قد يتمّ استغلاله حيث يمكن أن تحتوي مجموعة متنوعة من أجهزة الاتصال التي تنقل البيانات بين معدات التوليد الخاصة بالمستهلك (المنتج) ومشغلي شبكات الكهرباء على نقاط ضعف يمكن استغلالها لتدمير أو إعادة تهيئة معدات التوليد بشكل خاطئ أو السماح للمهاجمين بالوصول إلى الأجهزة الشخصية (للمستهلكين المنتجين) على شبكتهم المنزلية.

كما يمكن للمهاجمين استخدام أجهزة الاتصال لإرسال أوامر ضارة إلى شبكة الكهرباء، وعليه يجب أن تسعى الجهات إلى فرض ضوابط أمن سيبراني لحماية البرامج والمعدات و الأجهزة التي تسهل الاتصالات ثنائية الاتجاه مع شبكة الكهرباء، كما هو مطبق في بريطانيا من قبل مركز الأمن الالكتروني UK NCSC من خلال شهادة ضمان المنتج التجاري (CPA) الذي يضمن التوافق مع متطلبات الأمن السيبراني لنظام القياس الذكي (SMETS2) .

سيؤدي هذان التغيران دورًا أساسيًا في تطوّر قطاع الكهرباء، حيث إنهما يخلقان "فرصة للوصول إلى ذكاء المستهلك في شبكة الطاقة الكهربائية، مما يمكن الوكلاء الموزعين والأفراد من التعاون وتنسيق خططهم وإجراءاتهم".[52]

سيتعين على شركات المرافق والمؤسسات الوطنية تحديث نماذج أعمالها واستراتيجيات الصمود السيبراني لدمج توليد الطاقة الموزعة وتطوير مرونة الشبكة ضد انقطاع التيار الكهربائي وحماية البيانات التي يتم إنشاؤها ومشاركتها من قبل أصحاب المصلحة الجدد.



الابتكار التقني

تَعِدُ التقنيات الجديدة بتعزيز دورة توليد الكهرباء واستهلاكها وتحسين السوق، وسيستمر التحول الرقمي عبر القطاع في ربط الأنظمة والمؤسسات، مما يؤدي إلى فرص وتحديات جديدة وأكثر تعقيداً للأمن السيبراني. وتشمل هذه الابتكارات:

معايير انترنت الأشياء (IOT)

تهدف معايير توحيد البنية التحتية وشكل البيانات وواجهات البرمجة المتقدمة (APIs) التي تستخدمها أجهزة إنترنت الأشياء (IoT) إلى التغلب على تحديات التوافقية (interoperability) و التي تحد من إمكانيات الأتمتة والكفاءة في هذا القطاع. يمكن للاستشعار والمراقبة عن بعد واكتشاف الأعطال في الأسلاك والإصلاح المؤتمت للأعطال ومعدات المنزل الذكي الاستفادة من درجة جديدة من التوافقية.[53] ستكون الأجهزة الذكية في المنزل والصناعة قادرة على الاستجابة بشكل مستقل لتقلبات أسعار السوق، وبالتالي تمكين مستويات كفاءة أعلى في السوق والتي كانت مستحيلة سابقًا.

الثغرات في البرمجيات مفتوحة المصدر

إتباع وتوحيد المعايير سيدعم رفع مستوى الأمن السيبراني حيث سيمكن مطوري البرمجيات من استخدام مكتبات البرمجيات المشتركة بدلاً من محاولة تطوير واجهات مخصصة جديدة. كما يمكن أن تؤدي الثغرات السيبرانية في مكتبات البرمجيات المشتركة المستخدمة على نطاق واسع إلى تعريض عدد كبير من الأنظمة للتهديدات السيبرانية. يجب على المطورين اعتماد دورة حياة آمنة لتطوير البرامج وإجراء تقييم أمني شامل للكشف عن الثغرات السيبرانية المحتملة ومعالجتها.

الهجمات المعتمدة على الذكاء الاصطناعي

الذكاء الاصطناعي وتعلم الآلة سيتم استخدامه في الشبكات المحلية الدقيقة لتحسين الكفاءة التشغيلية وضمان الاتصال المرن بالشبكات التقليدية الأكبر وتعظيم القدرات الذاتية المحدودة حالياً.[54] وهذا يشمل الشبكات الصغيرة في المناطق الريفية والنائية أو في الأماكن الحساسة مثل المستشفيات. ومع ذلك، فمن الممكن أن يستخدم المهاجمون البيانات المنمذجة الخاصة بتعلّم الآلة لإجراء هجوم بطيء ومتطور تدخل فيه الشبكة في حالة حرجة. وسيكون وقتها من الصعب للغاية الكشف عن مثل هذا الهجوم السيبراني المتقدم.

تقنية سلسلة الكتل (BLOCKCHAIN)

تتم تجربة تقنية سلسلة الكتل Blockchain في قطاع الكهرباء لتمكين التعاون بين مختلف الجهات لتنفيذ العمليات التجارية ودعم منصات التداول بحيث يمكن للعملاء والموردين التعامل بثقة في القطاع. فثمّة إمكانية لهذا التداول لتحسين كفاءة السوق، بالنظر إلى أن الأسعار المحلية لشركات المرافق التجارية يمكن أن تكون أعلى من البدائل التي توفرها المصادر المتجددة.[55]

قد تمكّن التطورات المستقبلية في الحوسبة الكمية المهاجمين من تطوير وسائل قادرة على تزوير التوقيع الرقمي للمستخدمين. وذلك من شأنه أن يتيح للمهاجمين القدرة على انتهاك سلامة تقنية سلسلة الكتل (blockchain) عن طريق تعديل تاريخ المعاملات والحصول على ملكية الأصول الرقمية الخاصة بالآخرين. وهذا من شانه أن يحدّ من إمكانية الحصول على رؤية حقيقية للسوق. فيجب على مطوري تقنية سلسلة الكتل Blockchain النظر في تطبيق خوارزميات مقاومة للتشفير الكمي لحماية أسواق المستقبل ضد هذا النوع من الهجمات السيبرانية.

يتميز المستقبل القريب والطويل الأمد لصناعة الكهرباء بالابتكار التقني والقدرة على إعادة ترتيب مجالات التعاون بين أصحاب المصلحة في القطاع، وسيكون من الضروري الالتزام بمتطلبات الأمن السيبراني عند تطوير هذه التقنيات الجديدة وشرائها وتطبيقها.

الخاتمة

يهدف هذا التقرير إلى مساعدة قطاع الكهرباء على تعزيز الدفاعات السيبرانية وإدارة المخاطر الإلكترونية بشكل أكثر فاعلية - في الحاضر وفي المستقبل.

كتب المؤلف الإنجليزي ل.ب هارتلي ذات مرة أن "الماضي هو بلد آخر، إنهم يفعلون الأشياء بطريقة مختلفة هناك." وهذا يصح في قطاع الكهرباء حيث شهد القطاع تغيرًا ونموًا هائلين خلال العقود الأخيرة.

سيتمكن العديد من قراء هذه الدراسة من التعرف على الاختلافات بين الماضي والحاضر، على سبيل المثال، الكهرباء التي تمتد إلى أبعد بقاع العالم وكذلك نمو مصادر الطاقة البديلة والاعتماد الكامل للعالم الجديد على الكهرباء، بما في ذلك الكهرباء التي تعمل على تشغيل الكمبيوتر المحمول أو الهاتف الذكي الذي تستخدمه لقراءة هذه الدراسة.

إلى جانب هذه التغيرات تأتي مخاطر جديدة، وخاصةً المخاطر السيبرانية التي تؤثر على قطاع الكهرباء. تتعلق بعض هذه المخاطر بجهات التهديد السيبراني والبرمجيات الضارة الخبيثة، بينما تتعلق المخاطر الأخرى بالبنية التحتية القديمة أو سلاسل التوريد المعقدة أو الحوكمة أو تحقيق متطلبات الأمن السيبراني المتباينة للبنى التحتية لتقنية المعلومات والتقنية التشغيلية. في حين أنّ الآثار المترتبة على بعض هذه المخاطر واضحة، إلا أنّه من الصعب تحديد البعض الآخر، التي قد تؤدي الى حدوث هجمات سيبرانية كارثية.

تتوفر العديد من الأدوات لإدارة هذه المخاطرالسيبرانية، ويمكن تحقيق الكثير من خلال تطبيق ضوابط الأمن السيبراني على قطاع الكهرباء، إلى جانب تطوير أنظمة أمن سيبراني واضحة ومتسقة لتكون الأساس للنمو في المستقبل.

من نواح عدة، هذا المستقبل هو أيضًا بلد آخر مليء بالفرص والتطلعات ولكنّه غامض ومتغيّر أيضًا ولم يتمّ تحديده بوضوح بعد. ويحدونا الأمل في أن تساعد وجهات النظر والتوصيات الواردة في هذا التقرير قطاع الكهرباء على تعزيز قدراته السيبرانية وإدارة المخاطر السيبرانية بشكل أكثر فعالية، في الحاضر والمستقبل.

المراجع

المساهمون

المؤلف الرئيسي

الهيئة الوطنية للأمن السيبراني	المملكة العربية السعودية

تتوجه الهيئة الوطنية للأمن السيبراني بالشكر إلى الأشخاص التالية أسماؤهم لمشاركتهم الغنية في المناقشات والمقابلات والاستبيانات التي ساهمت في إعداد هذا التقرير.

المساهمون الأفراد

إيفان دراجنيف	القائد التقني الرئيسي للأمن السيبراني أوروبا، معهد أبحاث الطاقة الكهربائية EPRI، إسبانيا
لوران هاوزرمان	شريك مؤسس، سنتريو، فرنسا
ساندیب باتانيا	خبير التقنيّة التشغيليّة للأمن السيبراني، فرنسا
إيان سبيلر	مدير الأمن، SmartDCC، المملكة المتحدة
جوناثان توب	رائد تطوير الأعمال الإلكترونية، سيمنز، الولايات المتحدة الأمريكية

المساهمون في الصناعة

هيئة تنظيم الكهرباء والإنتاج المزدوج (ECRA)	المملكة العربية السعودية
مرافق	المملكة العربية السعودية
الشركة السعودية للكهرباء	المملكة العربية السعودية
الشركة السعودية لتقنية المعلومات (SITE)	المملكة العربية السعودية
ديلويت	قدمت ديلويت المساعدة في إعداد هذا التقرير عبر المساهمة في البحوث الرئيسية والثانوية

[1] - ليفينغستون، س.، سانبورن س.، سلوتر، أ. ، زونيفيلد بي (2019) "إدارة المخاطر السيبرانية في قطاع الطاقة الكهربائية"، ديلويت إنسايتس
https://www2.deloitte.com/insights/us/en/industry/power-and-utilities/cyber-risk-electric-powersector.html

[2] - 2019) BP)"مراجعة إحصائية للطاقة العالمية 2019 | الطبعة 68"،
https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/energy-economics/statistical-review/bp-stats-review-2019-full-report.pdf

[3] - (2018) Export.gov"دليل المملكة العربية السعودية التجاري القطري – الطاقة"،
https://www.export.gov/article?id=Saudi-Arabia-Power

[4] المنتدى الاقتصادي العالمي (2019) "المرونة السيبرانية في النظام البيئي للكهرباء: مبادئ وإرشادات للمجالس"، مركز الأمن السيبراني ومجتمع صناعة الكهرباء .http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf

[5] مدينة الملك عبد الله للطاقة الذرية والمتجددة (2020) "المشروع القومي للطاقة الذرية"،
https://www.energy.gov.sa/ar/snaep/Pages/ov.aspx

[6] توماس، ب. (2019) "الهجوم الإلكتروني على محطة الطاقة النووية الهندية يكشف عن خطر "التطفل" الخبيثة "، BitSight،
https://www.bitsight.com/blog/cyber-attack-on-indian-nuclear-power-plant-exposes-threat-of-snooping-malware

[7] دراغوس (2017) "Crashoverride: تحليل التهديد لعمليات الشبكة الكهربائية"،
https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf

[8] US CERT (2016) "الهجوم الإلكتروني ضد البنية التحتية الحيوية الأوكرانية"، .https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01

[9] - "البرلمان الأوروبي مركز أبحاث (2016) "منتجوا الكهرباء"، البرلمان الأوروبي مركز الفكر
http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)593518

[10] المكرمي، هـ (2016) "نظام الكشف عن التسلل للأمتار الذكية"، الشبكة الذكية السعودية.
https://ieeexplore.ieee.org/document/7849674

[11] ساردانا الخامس، شهي هـ. ل. أ. (2017) "تأمين شبكة الكهرباء في أبوظبي من الهجمات السيبرانية: نهج فعال من حيث التكلفة لتجميد أنظمة المراقبة والمراقبة الفرعية"، المؤتمر الدولي لتقنيات وتطبيقات الكهرباء والحوسبة
https://ieeexplore.ieee.org/document/8251926

[12] ليو.، ج.، شياو، ليانغ و.، تشين، س ل ب. (2012) "الأمن السيبراني وقضايا الخصوصية في الشبكات الذكية"، معهد مهندسي الكهرباء والإلكترونيات، 14:4.
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.462.4054&rep=rep1&type=pdf

[13] بورسكي س.، أندرياديس س.، كيندريك جـ. سي.، بيترسون بي. اف. (2017) "الأمن السيبراني في محطات الطاقة النووية: رؤى للتقنيات النووية المتقدمة"، مركز الأمن السيبراني طويل الأجل جامعة كاليفورنيا بيركلي
http://fhr.nuc.berkeley.edu/wp-content/uploads/2017/09/TH-Report-UCBTH-17-004.pdf

[14] مكتب مساءلة الحكومة الأمريكية (2019) "حماية البنية التحتية الحيوية: الإجراءات اللازمة لمعالجة المخاطر الكبيرة للأمن السيبراني التي تواجه الشبكة الكهربائية"، يسلط الضوء على مكتب المحاسبة العام
https://www.gao.gov/assets/710/701079.pdf

[15] سيمنز، معهد بونمون (2019) "واقعة في مرمى: هل المرافق مواكبة التهديد السيبراني الصناعي؟" ، سيمنز.
https://assets.new.siemens.com/siemens/assets/api/uuid:35089d45-e1c2-4b8b-b4e9-7ce8cae81eaa/version:1572434569/siemens-cybersecurity.pdf

[16] ديلويت (2018) "تحليل البيانات الداخلية".

[17] ديلويت (2019) "إدارة المخاطر السيبرانية في قطاع الطاقة الكهربائية"، ديلويت
https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/cyber-risk-electric-power-sector.html

[18] US-CERT (2018) "Alert (TA18-149A)", US CERT.
https://www.us-cert.gov/ncas/alerts/TA18-149A

[19] كاسبيرسكي لاب (2018) "من شامون إلى ستوندريل"، كاسبيرسكي https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf

[20] F-Secure (2020) الباب الخلفي : "W32/Havex"
https://www.f-secure.com/v-descs/backdoor_w32_havex.shtml

[21] تريند مكرو (2014) "HAVEX(يستهدف أنظمة التحكم الصناعي"، تريند مايكرو
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/139/havex-targets-industrial-control-systems

[22] كاسبيرسكي (2019) "مشهد التهديد لأنظمة التشغيل الآلي الصناعي H1 2019"، كاسبيرسكي.
https://ics-cert.kaspersky.com/media/H1_2019_kaspersky_ICS_REPORT_EN.pdf

[23] ليدن، ج. (2016) "مصنع معالجة المياه اخترق، تغير المزيج الكيميائي لإمدادات الصنبور"، السجل.
https://www.theregister.co.uk/2016/03/24/water_utility_hacked/

[24] او دونيل، ل. (2019) "طلب الفدية وراء هجوم نورسك هيدرو يستحوذ على مقدرات وايبر-لايك"، ThreatPost.
https://threatpost.com/lockergoga-ransomware-norsk-hydro-wiper/143181

[25] فيندلاي، اس.، وايت، اي (2019) "الهند تؤكد الهجوم الإلكتروني على محطة الطاقة النووية"، فاينانشانشال تايمز.
https://www.ft.com/content/e43a5084-fbbb-11e9-a354-36acbbb0d9b6

[26] أمبروسي، ج. (2020)، "تبقى الأضواء على الرغم من الهجوم السيبراني على النظام الكهربائي في المملكة المتحدة"، The Guardian.
https://www.theguardian.com/business/2020/may/14/lights-stay-on-despite-cyber-attack-on-uks-electricity-system

[27] كلاوس، نسخة (2020)، "مخترقون يهاجمون الشبكة تضرب Elexon بملفات الشبكة المظلمة"، The Telegraph.
https://www.telegraph.co.uk/business/2020/06/07/hackers-hit-grid-taunt-elexon-dark-web-files/

[28] هايدين، اي. (2019) "تاريخ مختصر لنظام الأتمتة والضوابط الصناعية والأمن السيبراني"، معهد SANS.
https://www.sans.org/reading-room/whitepapers/physical/abbreviated-history-automation-industrial-controls-system-cybersecurity-35697

[29] رأفت ر.، ماكلورن و. ج.، ترال تي.، حسن أ.، شيخ أ. (2016) "معالجة الأمن السيبراني لقطاع النفط والغاز والطاقة"، 2016 مؤتمر المملكة العربية السعودية للشبكة الذكية (SASG)
https://ieeexplore.ieee.org/document/7849685

[30] بارتز، هـ. (2018) "إغلاق مزرعة التشفير مع 6000 من عمال المناجم في روسيا بسبب فاتورة الكهرباء المتأخرة"، كوين تلغراف.
https://cointelegraph.com/news/crypto-farm-with-6000-miners-shut-down-in-russia-for-overdue-electricity-bill

[31] سلويك، جو (2019)، "CRASHOVERRIDE: إعادة تقييم حدث الطاقة الكهربائية الأوكرانية لعام 2016 كهجوم يركز على الحماية"، دراغوس.
https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

[32] أسود الكربون (2019) "كيفية مكافحة التنقل بين الجزر"، الكربون الأسود
https://www.carbonblack.com/resource/how-to-combat-island-hopping-ebook/

[33] يان واي.، تشيان واي.، شريف هـ.، تيبر د. (2013) "دراسة استقصائية عن البنى التحتية للاتصالات الشبكية الذكية: الدوافع والمتطلبات والتحديات"، معهد مهندسي الكهرباء والإلكترونيات، 15(1):20-5
https://ieeexplore.ieee.org/document/6157575

[34] مجلس منظمي الطاقة الأوروبيين (2018) "تقرير CEER للأمن السيبراني حول قطاعي الكهرباء والغاز في أوروبا"، مجلس منظمي الطاقة الأوروبيين.
https://www.ceer.eu/documents/104400/-/-/684d4504-b53e-aa46-c7ca-949a3d296124

[35] 2(ISC)2، (ISC) (2019)، دراسة القوى العاملة في مجال الأمن السيبراني - استراتيجيات لبناء وتنامي فرق الأمن السيبراني القوية"،
https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482

[36] نودار، تي. (2019) "مايكل تشيرتوف على الأمن السيبراني OT في صناعة المرافق العامة"، Cyberwire.
https://thecyberwire.com/events/Michael-Chertoff-on-OT-cybersecurity-in-the-utilities-industry.html

[37] ساردانا الخامس.، الشحي هـ. أ. (2017) "تأمين شبكة الكهرباء في أبوظبي من الهجمات السيبرانية: نهج فعال من حيث التكلفة لتجميد أنظمة التحكم والمراقبة في المحطات الفرعية"، المؤتمر الدولي لتقنيات وتطبيقات الكهرباء والحوسبة، 1-5.
https://ieeexplore.ieee.org/document/8251926

[38] المركز الوطني البريطاني للأمن السيبراني (2019) "ضمان المنتجات التجارية (CPA)"، المركز الوطني للأمن السيبراني.
https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa

[39] مايمكاست (2020) "استخبارات التهديد: التدريب الواعي يقلل من النقرات غير الآمنة وسط التهديدات الإلكترونية فيروس كورونا"،
https://www.mimecast.com/blog/2020/04/threat-intelligence-briefing-security-awareness-training-reduces-unsafe-clicks-amid-surging-coronavirus-cyber-threats/

[40] (The CyberWire 2019) "مقابلة مع روبرت م. لي، الرئيس التنفيذي في دراغوس".

[41] الجماعة إي آي (2019) "المرونة السيبرانية في النظام البيئي للكهرباء: مبادئ وإرشادات للمجالس بالتعاون مع مجموعة بوسطن الاستشارية"، المنتدى الاقتصادي العالمي
http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf

[42] MITRE (2019)، "ATT/CK للمؤسسات"، MITRE.
https://attack.mitre.org/resources/enterprise-introduction

[43] - هاتشينز، إم. إي.، كلوبيرت جاي. إم.، أمين ن. ر. (2011) "الاستخبارات - مدفوعة شبكة الكمبيوتر الدفاع المستنير من خلال تحليل الحملات العدائية وسلاسل قتل التسلل"، شركة لوكهيد مارتن
https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

[44] ووغان، د.، برادان س.، الباردي، س. (2017) "نظرة عامة على نظام الطاقة في دول مجلس التعاون الخليجي"، مركز الملك عبد الله للدراسات والبحوث البترولية. https://www.kapsarc.org/research/publications/gcc-energy-system-overview-2017/

[45] ليزسينا، ر.، روبيل، ر. م. (2014) "تبادل المعلومات الأمنية للشبكات الذكية"، المؤتمر الدولي التاسع لتقنية الإنترنت والمعاملات المضمونة.
https://www.researchgate.net/publication/282255776_Security_information_sharing_for_smart_grids_Developing_the_right_data_model

[46] ماجواير وودز ذمم (2019) "قانون الحماية يسعى إلى تعزيز الأمن السيبراني للشبكة الكهربائية المحلية"، Lexology.
https://www.lexology.com/library/detail.aspx?g=1a655017-2599-436e-80a2-29aabc9bee5d

[47] بيكر، س.، شنيك ب. (2011) "في الظلام: الصناعات الحرجة مواجهة الهجمات الإلكترونية"، CSIS.
https://csrc.nist.gov/CSRC/media/Events/ISPAB-JULY-2011-MEETING/documents/Jul14_CIP-CSIS-2011-ISPAB.pdf

[48] لام، جاي. (2016) "IIET - الأمن السيبراني في أنظمة الطاقة الحديثة - حماية الشبكات الكبيرة والمعقدة"، مؤسسة الهندسة والتقنية
https://ieeexplore.ieee.org/document/7835821

[49] يوراكتيف مع وكالة فرانس برس، (2019) "الولايات المتحدة للمساعدة في تأمين شبكة الطاقة البلطيق ضد الهجمات السيبرانية"، Euractiv.
https://www.euractiv.com/section/energy/news/us-to-help-secure-baltic-energy-grid-against-cyber-attacks/

[50] جونسون، ب. د. (2019) "NIST تبحث عن شركاء لتأمين الطاقة"، FWC - أسبوع الكمبيوتر الاتحادية
https://fcw.com/articles/2019/10/07/nist-energy-cyber-johnson.aspx

[51] جمعية شبكات الطاقة (2018)، "استراتيجية الابتكار في شبكة الكهرباء"، جمعية شبكات الطاقة.
http://www.energynetworks.org/assets/files/electricity/futures/network_innovation/electricity_network_innovation_strategy/Energy%20Networks%20Association%20-%20Electricity%20Network%20Innovation%20Strategy-March%202018.pdf

[52] كيزلينغ، ل. (2010) "تشجيع الابتكار في صناعة الكهرباء" في الشؤون الاقتصادية، 30(2):12-6
https://www.researchgate.net/publication/227670308_Promoting_innovation_in_the_electricity_industry

[53] ENISA (2016) "دليل NCSS للممارسات الجيدة: تصميم وتنفيذ الاستراتيجيات الوطنية للأمن السيبراني"، وكالة الاتحاد الأوروبي للأمن السيبراني. https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[54] إلسمور، جاي. (2018) "ستة اتجاهات للطاقة المتجددة للمشاهدة في 2019"، فوربس.
http://www.forbes.com/sites/jamesellsmoor/2018/12/30/6-renewable-energy-trends-to-watch-in-2019/#7e04f5454a1f

[55] منظمة التعاون والتنمية في الاقتصاد (2018) "سلسلة من ردود الفعل: الابتكار التخريبي في قطاع الكهرباء"، منظمة التعاون والتنمية في الاقتصاد.
https://www.oecd.org/competition/A-chain-reaction-disruptive-innovation-in-the-electricity-sector.pdf

[56] الهيئة الوطنية للأمن السيبراني www.nca.gov.sa

© 2020. الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية. مركز الدراسات الاستراتيجية للأمن السيبراني.