الدفاع السيبراني في القطاع الصناعي

تقييم ثغرات الأمن السيبراني والاستعداد لمواجهتها في قطاع الطاقة والموارد الطبيعية

أكتوبر ٢٠٢١

كي بي إم جي في السعودية

فهرس المحتويات

تمهيد

تَطَوَّرت التهديدات المتعلقة بالأمن السيبراني للأنظمة الصناعية بشكل سريع خلال العام الماضي. وهناك مجموعة من العوامل التي أدت إلى زيادة هذه التهديدات، بما فيها تحول الأنشطة الهندسية وعمليات الصيانة للعمل عن بعد، إضافة إلى خطوط الإنتاج التي لا تزال تعمل عن بعد رغم عدم اكتمال التحول الرقمي بالشكل المتكامل والصحيح.

في المقابل، أصبح هناك تزايد مستمرّ في الوعي العام بالتهديدات السيبرانية في العالم. ومن الأمثلة على ذلك تعرض شركة" كولونيال بايب لاين" ، وهي أكبر مشغل لخطوط الأنابيب في الولايات المتحدة للتهديد في وقت سابق من هذا العام؛ مما أدى إلى إغلاق خطوط أنابيب البترول وانقطاع وصوله لمساحات كبيرة من الولايات المتحدة الأمريكية؛ مما أثر مباشرةً على المستهلكين، ولذا تعالت الأصوات المطالبة بضرورة اتخاذ الإجراءات اللازمة لحل المشكلة.
وعلى الرغم من التهديدات المتزايدة والضغط العام، ما زالت المنظمات والمنشآت غير جاهزة بعد، إذ يتضمن قطاع الأمن السيبراني خدمات لا تعد ولا تحصى، والعديد منها جديد نسبيًا حتى أنّ بعضها لم يخضع للاختبار بعد، ولأن هذه الخيارات المتعددة والمختلفة تُربك المنشآت وتؤخر قراراتها، فإنَّ الأمر يؤدي إلى بقائها دون حماية في النهاية.

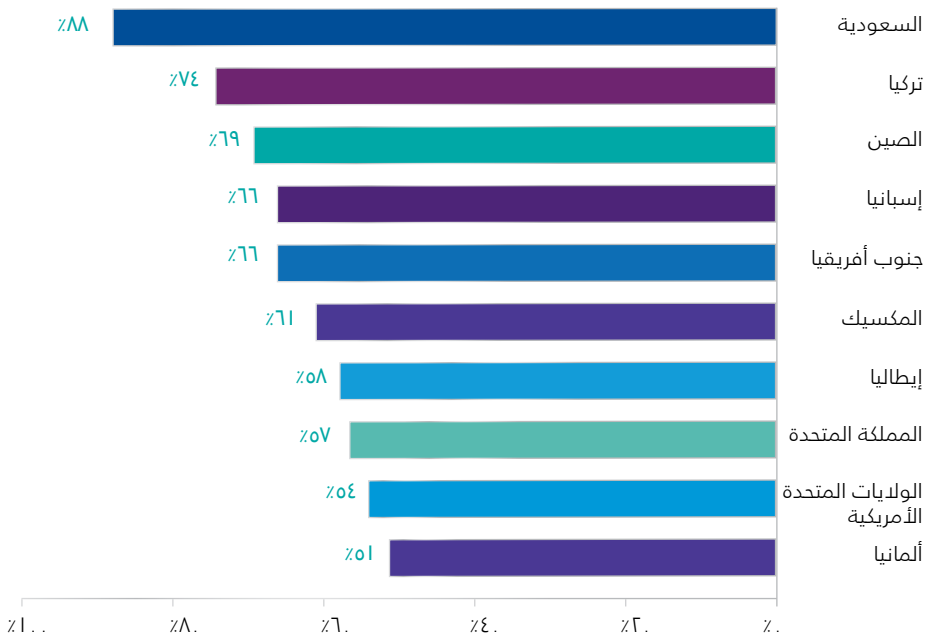
يستعرض هذا التقرير الوضع الحالي للتهديدات السيبرانية ويُقدم توجيهات للمنشآت لاتخاذ إجراءات يومية والاستعداد بطريقة أفضل للتهديدات المتطورة، ويوصي بتحليل وتقييم المخاطر المرتبطة بالإجراءات والعمليات السيبرانية (PHA) واستخدامه كأداة للتعامل مع المنظمات والمنشآت في القطاع الصناعي.

حسين الشدوخي
رئيس استشارات الأمن السيبراني
لقطاع الطاقة والموارد الطبيعية
كي بي إم جي في السعودية

الأهمية

تشير العديد من الدراسات إلى أنَّ قادة الأعمال والحكومات يدركون التهديدات السيبرانية في القطاع الصناعي، ولكنهم ليسوا مستعدين بعد لمواجهتها.
غالبًا ما تكون الهجمات السيبرانية عابرة للقارات ويتعرض الجميع لها دون استثناء ويعد التهديد للشركات الصناعية قائماً على مستوى العالم. ومع ذلك، بسبب العوامل الجيوسياسية وتركّز النشاط الصناعي في بعض البلدان؛ فإنَّ التهديدات تكون أكثر حدة فيها دونًا عن غيرها. وفي المملكة العربية السعودية، فإنَّ التهديدات تتسم بالحدة بشكل خاص.

الشكل ١: نسبة المنظّمات التي أبلغت عن هجمات سيبرانية حسب البلدان

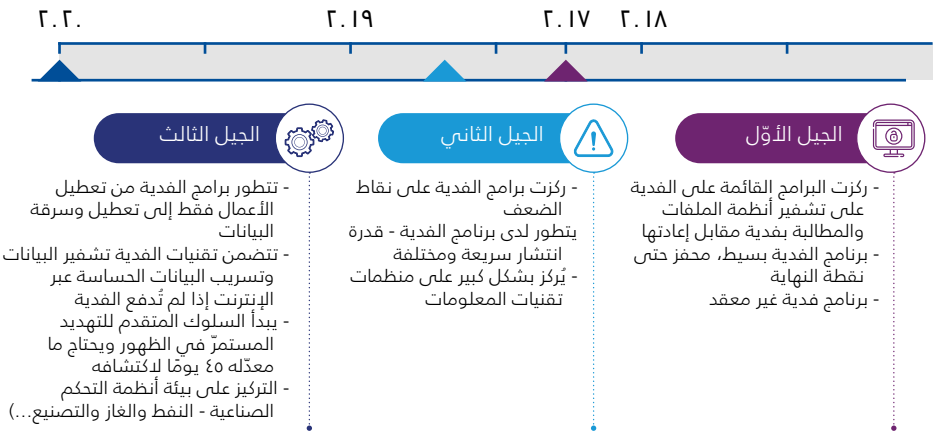


ارتفعت هجمات برامج الفدية؛ والتي تستهدف تشفير البيانات في شبكات الأنظمة الصناعية للشركات وتطالب بدفع مبالغ مالية لإعادتها بنسبة ٥٪ بين عامي ٢٠١٨ و ٢٠٢٠.
ومن بين هذه الهجمات، شكلت الجهات المصنعة أكثر من ثلث الهجمات المؤكدة على المنشآت الصناعية، تليها المرافق الخدمية، والتي شكلت ١٠٪. كما ارتفعت التكاليف المقدرة للهجمات إلى حدٍ كبير - حيث قفزت من ٨ مليارات دولار أمريكي في عام ٢٠١٨ إلى ١١,٥ مليار دولار أمريكي في عام ٢٠١٩ ووصلت إلى ٢٠ مليار دولار أمريكي في عام ٢٠٢٠؛ وقد أدى الاضطراب التشغيلي الناتج عن برامج الفديات في بيئات التقنيات التشغيلية إلى زيادة قدرها ٢٣ ضعفًا. وفي عام ٢٠٢٠، كانت هناك زيادة بنسبة ٣٢ بالمائة في هجمات برامج الفدية على مؤسسات الطاقة والمرافق[٢].

[١] Cybersecurity Magazine, Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031 (2021); 2021 Ransomware Statistics, Data & Trends, PurpleSec (2021)
[٢] Ibid

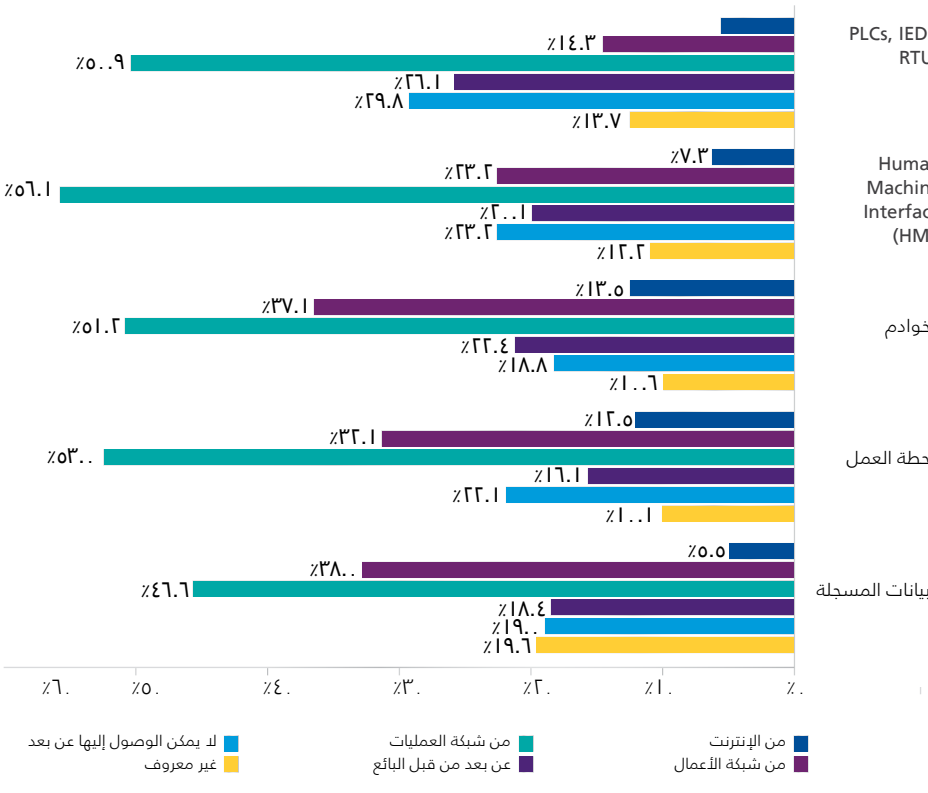
مع مرور الوقت، أصبحت هجمات برامج الفدية أكثر تعقيدًا وقامت بتغيير أنشطتها لتحقق أهدافها بطرق مختلفة، بالإضافة إلى ذلك، استهدفت هذه الأنواع من الهجمات بشكل متزايد بيئات أنظمة التحكم الصناعية ،مثل: النفط والغاز والتصنيع.

الشكل ٢: تزايد تهديدات برامج الفدية[٣]



أشارت دراسة أجرتها كل من الجمعية الدولية للأمن السيبراني لأنظمة التحكم وكي بي إم جي تحت عنوان "مسح الأمن السيبراني لأنظمة التحكم لعام ٢٠٢٠"، إلى وجود من ١٠ إلى ٢٠ في المائة من المستجيبين الذين لم يعرفوا ما إذا كان أي عنصر معين من الرسم البياني أدناه يمكن الوصول إليه عن بعد.

الشكل ٣: العناصر التي يمكن الوصول إليها عن بعد [٤]



[٣] KPMG - Securing a hyperconnected world_(2021)
[٤] Control System Cyber Security Survey 2019 2AI-KPMG(CS)

تطور مساحة التهديدات الأمنية

تطور الجهات المهددة

إنّ أساليب مجرمي الإنترنت مرنة ومتنوعة، ويسهل عليهم التكيف في مختلف الظروف، إذ يشكلون قوة بحد ذاتهم. وتتغيّر العمليات الإجرامية بشكل مستمرّ وتطور أساليبها وذلك لتقليل مخاطر اكتشافهم وتعطلهم. كما يحاولون تعظيم العائد على جهودهم بعدة طرق مثل: التحول من الشراكات إلى العمل داخل كيانات متماسكة؛ والاستفادة من فهم البيئة المحلية؛ ولزيادة دقة الاستهداف يقومون باستخدام وثائق قانونية تساعد على تحديد أفضل للضحايا المحتملين قبل إرسال البرامج الضارة لهم؛ أو يقومون ببيع وشراء الوصول المباشر إلى الشبكات المختلفة وذلك لسهولة إرسال برامج الفدية بدلاً من تنفيذ عمليات متقدمة وأكثر تعقيداً.

برامج الفدية المستهدفة

يسبب اختلاف الدوافع مخاطراً جديدة في الدفاع ضد برامج الفدية والاستجابة لها. حيث يتفاقم تهديد برامج الفدية بشكل أكبر من خلال بيع الوصول إلى شبكات الشركات. وفي حين أن الدافع وراء مثل هذه الهجمات قد يبدو مالياً، إلا أن هجمات برامج الفدية المستهدفة قد تخدم في بعض الأحيان دوافع مختلفة، سواء كانت مالية أو أيديولوجية أو سياسية. وبغض النظر عن الدافع، يظل تهديد برامج الفدية قائمًا، ويجب على المؤسسات التأكد من أنها تتخذ التدابير المناسبة للتحضير لهجوم برامج الفدية على مستوى الشركة ومنعه واكتشافه والاستجابة له واحتوائه.

تهديدات سلاسل التوريد

يدفع تحسين وتصحيح النظام البيئي التهديدات لتتجه نحو سلاسل التوريد، مما يجعل الأصدقاء يصبحون أعداء في الوقت ذاته. ويبدو أن الترابط العالمي للأعمال، والاعتماد الأوسع للإجراءات المضادة للتهديدات السيبرانية في الصناعة التقليدية، والتحسينات التي أدخلت على النظام الأساسي للأمن السيبراني، يدفع الجهات الفاعلة في مجال التهديدات الإلكترونية إلى البحث عن سبل جديدة لإلحاق الضرر بالمنظمات، مثل استهداف سلاسل التوريد الخاصة بهم - بما في ذلك تلك المتعلقة بالبرامج والأجهزة والسحابة.

الحياة بعد الانهيار

تتطلب نقاط الضعف في البنية التحتية للتقنيات التشغيلية وأنظمة التحكم الصناعية حلولاً مكلفة. وقد شكل اكتشاف نقاط الضعف في وحدات التحكم المنطقية القابلة للبرمجة أو واجهة تفاعل الآلة مع البشر أو مسجل البيانات أو محطة العمل الهندسية في السنوات الأخيرة خطرًا كبيرًا على المنظمات مما قد يؤدي إلى خسائر في الأرواح في حال مهاجمتها.

الوصول إلى حلول للجغرافيا السياسية

مع ظهور التهديدات الجديدة وفي ظلّ المعلومات المضللة والتطور التكنولوجي السريع، تجد الشركات العالمية نفسها في وسط الكثير من التوترات الجيوسياسية المستمرة؛ ولذا تقوم الجهات الفاعلة في مجال الأمن السيبراني بالحفاظ على مستوى النشاط الحالي للمنظمة، وتستفيد من القدرات التقنية الجديدة والمختلفة لتقديم الاستراتيجيات والإجراءات والعمليات الأكثر تعقيداً أيضاً، وتركّز على التقنيات التشغيلية وأنظمة التحكم الصناعية [٥].

[٥] (2019) Security magazine, Five factors influencing the cybersecurity threat landscape

الصمود السيبراني

أعدت وزارة الداخلية الأمريكية تقريرًا عن تقنيات صمود الأمن السيبراني ومبادئ التصميم، حيث ركز التقرير بوجه خاص على القدرة على تحمل النشاط العدائي، نعرض مقتطفاً من هذا التقرير أدناه.[٣]

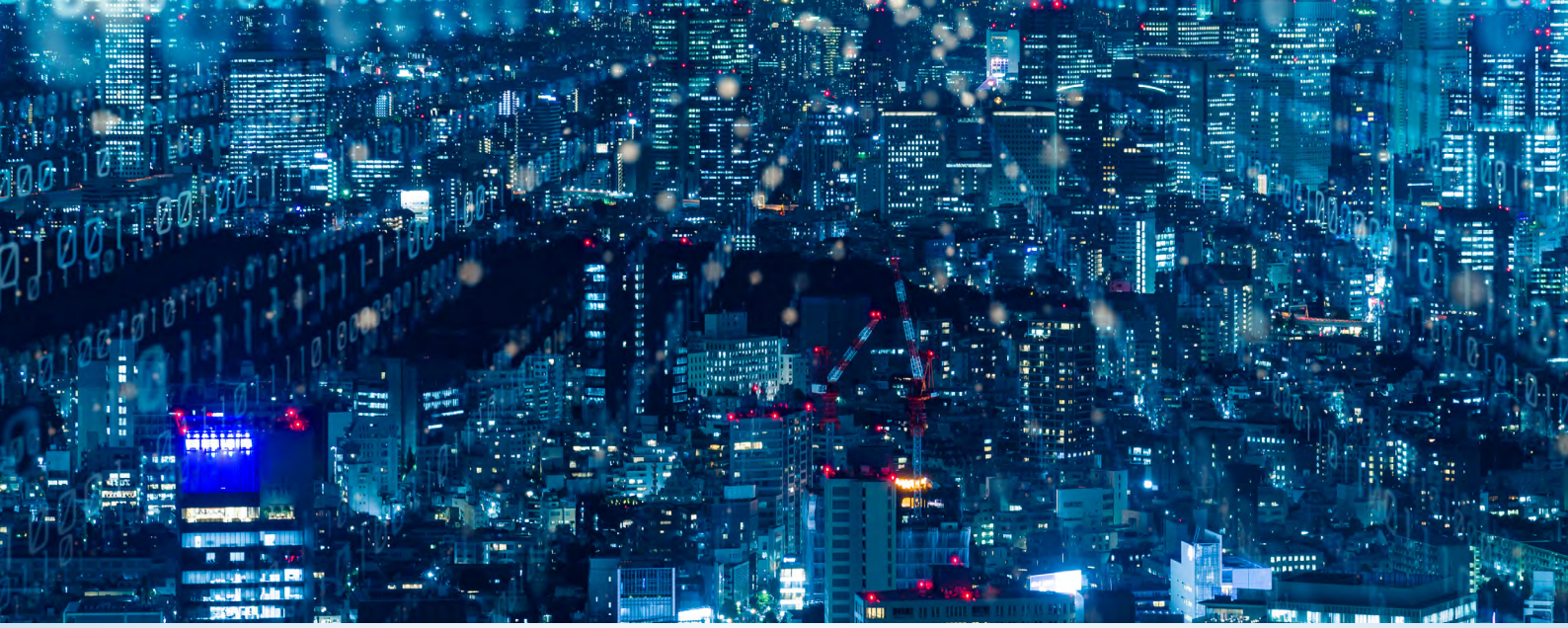
الصمود السيبراني هي سمة النظام التي تضمن استمراريته في أداء وظائفه الأساسية حتى في حالة تعرضه لهجوم سيبراني. يعد الصمود السيبراني مهم بوجه خاص لمجموعة فرعية من البنى التحتية الحيوية المعروفة باسم قطاعات شريان الحياة أو البنى التحتية الإستراتيجية.

التمييز بين الصمود السيبراني والأمن السيبراني

النقطة الأساسية التي تميز الصمود السيبراني عن الأمن السيبراني هي أنَّ الصمود السيبراني يستمر في العمل حتى بعد أن يخترق المهاجم المحيط الأمني للشبكة ويعرض الأصول السيبرانية للخطر. حتى في المراحل اللاحقة من سلسلة الهجوم السيبراني، يمكن أن يساعد الصمود السيبراني في منع المهاجمين من جمع المعلومات الاستخبارية حول الأنظمة الأساسية لعمل المؤسسة أو تسريبها أو السيطرة عليها.

يمكن النظر إلى الوظائف العديدة التي يمكن أن يخدمها الصمود السيبراني بعد المساومة على أنها دليل لتحقيق نتائج الصمود السيبراني من منظور هندسة النظام في عمليات دورة حياة النظام. تضمن الطبيعة المخصصة للجهود الهندسية وعمليات دورة الحياة بأن الأنظمة الناتجة عن تطبيق مبادئ تصميم الصمود السيبراني كافية لحماية أصحاب المصلحة من المعاناة من الخسائر غير المقبولة لأصولهم الرئيسية وما يرتبط بها من عواقب اقتصادية وأمنية ووطنية.

٦ (2018) US Department of Homeland Security, Cyber Resilience and Response



تتضمن أنظمة الصمود السيبراني الهندسية الخصائص التالية والتي يجب أخذها في الاعتبار عند تصميم أنظمة جديدة أو تحسين الأنظمة الحالية.

التركيز على مهمة وأهداف العمل

ينطوي هذا على القدرة على دعم استمرارية الأعمال على الرغم من تعرضها للخطر. وفي بعض الحالات، قد يتم التضحية بعناصر النظام الأقل أهمية لتحقيق المهمة أو ضمان فاعلية الأعمال ولاحتواء الهجوم السيبراني وضمان سير العمل.

التركيز على تأثير التهديد المتقدم والمستمر

تُشكل موارد التهديد المتقدم والمستمر وسهولة قدرته على التكيف تهديدًا خطيرًا. ومن خلال التركيز على أنشطة التهديدات المستمر وتأثيراتها المحتملة، يمكن للمهندسين تصميم أنظمة تستطيع توقع مجموعة واسعة ومتنوعة من الظروف والضغوط المعاكسة وتتحملها وتتعافى منها وتتكيف معها.

افتراض أن الهجوم سينجح في تعريض النظام أو المنظمة للخطر أو الإختراق

يُعتبر هذا الاعتقاد أمرًا أساسيًا لتصميم الصمود السيبراني. كما يُقر هذا الافتراض بالضرورة أن الأنظمة الحديثة عبارة عن كيانات كبيرة ومعقدة تنطوي دائمًا على نقاط ضعف وعيوب سيتمكن المهاجمون من استهدافها واستغلالها.

افتراض أن الهجوم سيحافظ على وجوده الطويل في النظام أو المنظمة

قد يكون من الصعب على المنظمة أن تتأكد من أنه قد تم القضاء على التهديد الخفي تمامًا، إذ يمكن أن يتكيف التهديد المستمر المتقدم مع تكتيكات التخفيف أو محاولات الإزالة التي كانت فاعلة في السابق ضده. وفي بعض الحالات، قد تكون أفضل نتيجة هي احتواء التهديد بما يكفي لتحقيق أهداف المؤسسة الأساسية قبل فقدان الأنظمة الحرجة لقدرتها على العمل.

قيمة الصمود السيبراني على المستوى المؤسسي

يتطلب نشر الصمود السيبراني والحفاظ عليها جهداً أكثر من نشر تدابير الأمن السيبراني التقليدية والحفاظ عليه. ويرجع ذلك إلى التعقيد المتأصل والطبيعة الديناميكية لتقنيات الصمود السيبراني. وعلى الرغم من زيادة تكاليف النشر والصيانة، على أساس تكلفة دورة الحياة، فإن الصمود السيبراني يكلف المؤسسة أقل من تدابير الأمن السيبراني التقليدية.
ويرجع السبب الرئيسي لهذا الى قدرة الصمود السيبراني العالية على تحمل الهجمات السيبرانية وبالتالي تجنب تعطل المؤسسة وفقدان الإيرادات. إذ قد يؤدي هجوم سيبراني متطور إلى تعطيل بنية تحتية مهمة وإغلاق المؤسسة لعدة أسابيع، بدلاً من عدة أيام فقط، كما هو الحال عادةً مع الهجمات السيبرانية الأقل تعقيدًا.
إن احتساب تكلفة الإيرادات المفقودة جراء الانقطاع لعدة أسابيع، مقارنةً بتكلفة تنفيذ مبادئ وتقنيات تصميم الصمود السيبراني، هو ما يحدد ما إذا كان الصمود السيبراني مبرراً من حيث التكلفة بالنسبة للمؤسسة.

قيمة الصمود السيبراني على المستوى المجتمعي

قد لا ينتج عن الاستثمار الخاص بالصمود السيبراني فائدة اقتصادية على مستوى المؤسسة، إلا أنه سيحقق فائدة اقتصادية على المستوى المجتمعي. ويجب أن تكون مؤسسات البنية التحتية الحيوية، والتي تدرك أن إغلاق مؤسساتها له آثار مضاعفة في جميع أنحاء المنطقة التي توجد فيها، قادرة على عرض هذه القضية على حكوماتها. وقد تجد المؤسسات ذات الموقع الاستراتيجي والمتعلّق بالبنى التحتية أنها غير قادرة على تطبيق الصمود السيبراني لنفسها فقط دون أن تدرك مدى اعتماد الشركات الأخرى عليها، بالتالي يجب أن تقدم التقييم والحالة على المستوى المجتمعي الإقليمي.

أمثلة توضح الطبيعة المتغيرة للهجمات السيبرانية في القطاع الصناعي

الهجوم على خط أنابيب الوقود في الولايات المتحدة

في مايو ٢٠٢١، شهدت الولايات المتحدة أحد أكبر انتهاكات الأمن السيبراني عندما أُجبر أحد أكبر خطوط أنابيب الوقود في البلاد على الإغلاق بسبب هجوم باستخدام برنامج الفدية. كان على خط أنابيب الوقود الأمريكي هذا أن يدفع للمبتزين ٥ ملايين دولار كفدية لإعادة التشغيل. وتعتبر هذه الحادثة واحدة من أكبر عمليات الفدية الرقمية وأكثرها تخريبًا، حيث لفتت الانتباه إلى ضعف البنية التحتية في قطاع الطاقة في الولايات المتحدة.

تسرب البيانات في كبرى شركات الطاقة العالمية

في منتصف عام ٢٠٢١، واجهت شركة طاقة عالمية تسريباً للبيانات من أحد المتعاقدين معها، حيث احتجز المبتزون واحد تيرابايت من البيانات في محاولة لابتزاز الأموال من الشركة.
تسلط مثل هذه الحوادث الضوء على أهمية الاستثمار في الأمن السيبراني واتخاذ تدابير ضد الهجمات السيبرانية، إذ أصبحت هذه الهجمات شائعة.

طريقة تحليل مخاطر العمليات

تسهيل تحليل مخاطر العمليات السيبرانية

تحليل مخاطر العمليات السيبرانية هو منهجية موجهة نحو السلامة، وتقوم بإجراء تقييم لمخاطر الأمن السيبراني لنظام التحكم الصناعي أو نظام الأمان الآلي.
وفي العادة يتم تنفيذ تحليل مخاطر العمليات السيبرانية على مراحل، وهذا التحليل قابل للتطوير، ويمكن تطبيقه على أنظمة فردية أو مرافق أو مؤسسات كاملة.
وهناك ست مراحل لتحليل مخاطر العمليات السيبرانية:

١. الموظفين في موقع العمل ومقيِّمي التهديدات - يجب على فريق المخاطر والتشغيل إيجاد التوافق بينهم والاتفاق على المجال الذي سيتم التركيز عليه لتقييمه.

٢. جمع معلومات حول عناصر التقنيات التشغيلية مع شبكة التقنيات التشغيلية وأنظمة أدوات السلامة واتصالاتها لتحديد نقاط الضعف.

٣. يسمح تحليل البيانات للفريق بتوثيق نقاط الضعف الأمنية المحتملة التي قد تُستغل أثناء الهجوم السيبراني.

٤. عقد ورشة عمل حول تحليل مخاطر العمليات السيبرانية حيث يتم جمع جميع المعلومات وتحليلها ودمجها مع سيناريوهات التهديد لتطوير صورة كاملة للمخاطر.

٥. بمجرد اكتمال تحليل مخاطر العمليات السيبرانية، يتم إعداد تقرير شامل يوضح المخاطر التي تتعرض لها المؤسسة وخطة التخفيف من المخاطر إلى المستوى المقبول للمؤسسة.

٦. تتضمن خطة العلاج الفاعلة قائمة من الإجراءات ذات الأولوية وتقديرات الموازنة ومتطلبات الجدول الزمني والموارد، والتي توفر مستويات من المرونة وسهولة التكيف.

التوسع في الأتمتة الصناعية

لا ينبغي النظر إلى تدابير الأمن السيبراني على أنها مجرد حماية للأصول القديمة أو الضعيفة. قد يكون من الصعب جدًا تعديل الأمن السيبراني لأنظمة كبيرة مثل شبكات الطاقة، إلا أننا قد نكون قادرين على توفير منهجية مراقبة وتجزئة مناسبة – ولكن غالباً لن تكون هذه الأنظمة قابلة للترقية أو التطوير أو حتى الصيانة. أمّا الأنظمة الصناعية الأحدث والتي تستخدم التشغيل الآلي، فإن بروتوكولات الأمن السيبراني مهمة فيها بالقدر ذاته، إن لم تكن أكثر أهمية.

مع ترقية أنظمة التصنيع المؤتمتة، يجب على المؤسسات تضمين الأمن السيبراني ضمن الوظائف الأساسية.

يجري تطوير نماذج النضج للتطورات المستقبلية لأنظمة التحكم الصناعي المؤتمتة بوظائف تقنية المعلومات. حدد نموذج واحد فاعل -جرى تطويره في ألمانيا- الخطوات الخمس نحو جيل جديد من الأنظمة ذاتية التشغيل وذاتية التحسين، والتي تتطلب درجة كبيرة من الاستقلالية [٧]. وتتضمن الخطوات الثلاث الأولى شراء البيانات وتحليلها بشكل منهجي.

١. تكون أنظمة التصنيع المؤتمتة "متصلة"، أي تقوم على شبكات يمكنها تبادل البيانات مع بعضها البعض.
٢. تستخدم أجهزة الاستشعار لجمع البيانات.
٣. تقوم بتحقيق شفافية في عمليات التصنيع من خلال وظائف التحليل والتحديد.
٤. يتم تقييم البيانات باتباع مفاهيم الذكاء الاصطناعي. ويمكن تفسير البيانات والتعرف عليها بمستويات مختلفة من التعقيد. على سبيل المثال، يمكن استخدام محاكاة تنبؤية لتوقع سيناريوهات متعددة في المستقبل.
٥. إنشاء نظام تصنيع قابل للتكيف بالكامل. يمكن أن تكون أنظمة المستقبل هذه ذاتية التحسين أو حتى ذاتية التصرف. ويُعد جانب التكيف الذاتي أو حتى الوظائف المستقلة موضوعًا مهمًا في البحث، على الرغم من أن فكرة وجود نظام مستقل بالكامل يتحكم في أنشطته الخاصة قد تبدو غير ممكنة التصديق.

توضح هذه الخطوات حاجة الأعمال للوصول في الوقت الفعلي وبشكل مباشر للبيانات التشغيلية، مما يعني أن الأنظمة الصناعية - التي كانت معزولة وآمنة – قد أصبحت متكاملة بأسلوب متزايد مع شبكات الشركات، وأحيانًا على منصات تجارية جاهزة. بالإضافة الى ذلك، يمكن أن يخلق هذا الاتصال مزايا مثل التحليلات الذكية والصيانة التنبؤية والمراقبة عن بُعد. لكنه يعرض أيضًا أنظمة التحكم الصناعية وأنظمة التحكم في العمليات وغيرها من التقنيات التشغيلية لهجمات البرمجيات الخبيثة والقرصنة وتعطيل الموظفين والمخاطر الأمنية الأخرى التي أثرت سابقًا على معلومات الشركة فقط.

نظرًا لأن الخطوط غير واضحة بين تقنية المعلومات والتقنيات التشغيلية، فإن تحليل مخاطر العملية السيبرانية يمكن أن يساعد في توفير الوصول المناسب إلى بيانات التحكم والإنتاج مع منع أحداث الأمن السيبراني والتي قد تتسبب في عمليات الإغلاق وتهديدات السلامة وتعطل العمليات.

[٧] (2018) Micheal Weyrich, Towards future Automation Systems – Cyber physical, intelligent, flexible and efficient

الإطار التنظيمي

مع زيادة تطبيق الأنظمة السيبرانية عبر القطاعات والصناعات المختلفة، أصبح من المهم وضع معايير أمان وتدابير تنظيمية لضمان حماية البيانات والأنظمة جميعها.
في عام ١٩٩٢ تم تحديد طريقة لإدارة سلامة العمليات وهي عبارة عن برنامج شامل يمنع إطلاق المواد الخطرة، وعادة ما يتطلب التزام الإدارات لدعمه، ويتضمن ١٤ عنصرًا مترابطًا مثل: مشاركة الموظفين، والتدريب، وتحليل مخاطر العملية، ومعلومات سلامة العملية.
وقد بدأت المنظمات باتخاذ تدابير تنظيمية للحماية من الهجمات المختلفة. وعلى سبيل المثال، يتطلب معيار السلامة الوظيفية الصادر عن اللجنة الكهروتقنية الدولية١ ٦١٥١ (IEC) تقييم المخاطر الأمنية لنظام أدوات السلامة. كما يلخص التقرير المحدّث أداة تقييم المخاطر المسماة بتحليل مخاطر العمليات السيبرانية. ويُعد الارتباط بتحليل مخاطر العمليات هنا خطوة في تقييم المخاطر أولاً، لمراجعة مخرجات تحليل مخاطر العمليات ولتحديد أسوأ حالة للصحة والسلامة والأمن والآثار البيئية للأصول وثانيًا، لتحديد أي سيناريوهات للمخاطر المتوقعة.

وهناك مثال آخر يأتي من الجمعية الدولية نامور، التي نشرت ورقة عمل (NA163) بعنوان "التقييم الأمني لنظام أدوات السلامة".
وهنا، يمكننا استخدام منهجية تحليل مخاطر العمليات السيبرانية لتقييم المخاطر المرتبطة بعوامل تصعيد الأمن السيبراني المحددة وإجراءات التخفيف الموصى بها لتقليل المخاطر إلى مستوى معين.
ومن خلال التجسير والربط بين طرق تحليل مخاطر العملية وطرق تقييم مخاطر الأمن السيبراني، تصبح أنظمة السلامة أكثر قوة في مواجهة هجمات الأمن السيبراني.

لطالما طبقت بعض شركات الطاقة العالمية طرقًا لتقييم المخاطر ورفع السلامة. وتتضمن هذه الجهود استخدام مصفوفات تقييم المخاطر التي تأخذ في الاعتبار عواقب وتأثيرات المخاطر على الأفراد والأصول والمجتمعات والبيئة، واستخدمت نماذج الربط المتصلة لتصوّر العناصر المختلفة لسيناريوهات المخاطر المتوقعة.

الشكل ٥: رسم توضيحي لمواقف الصحة والسلامة المهنية [٨]

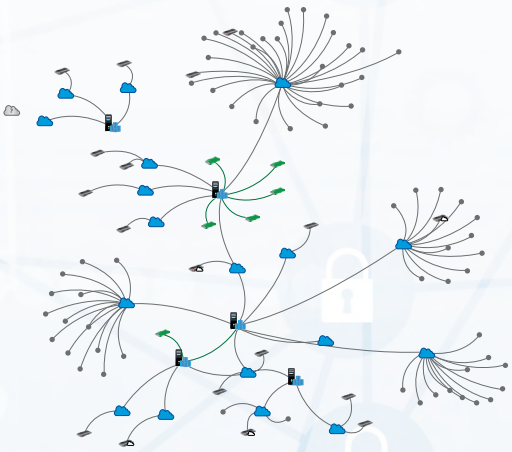
Process safety management of highly - 1910.119 ,US Department of Labor, Occupational Safety and Health Administration hazardous chemicals

يمكن أن تساعد أداة تحليل مخاطر العمليات السيبرانية على تسهيل عمل تمرين يشمل التأثيرات المضرة. ويتضمن ذلك مراجعة الوثائق الحالية، ووضع قائمة بجميع الأصول السيبرانية، وتفاصيل الموقع، وتحليلات مخاطر العمليات السابقة، وبعد ذلك إعداد قائمة بجميع أنواع الأصول السيبرانية المستخدمة في كل عملية محددة أو وحدة مرافق، حيث توجد مخاطر مختلفة متعلقة بسلامة العمليات أو المخاطر البيئية أو المالية المتعلقة بها.

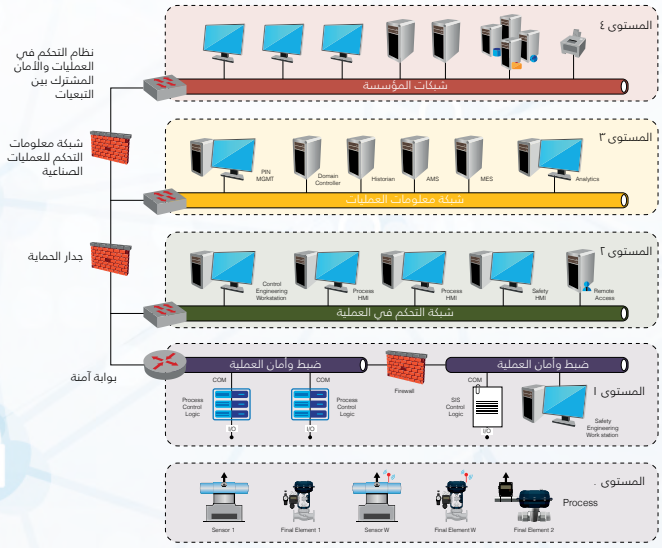
من أجل حدوث هجوم سيبراني، يجب أن يكون كل من عمليات البدء بتشغيل الأعمال وحمايتها قابلين للاختراق. إذا ما جعلنا أحدهما غير قابل للاختراق، سيتم تقليل المخاطر، ولكن إذا أصبح كلاهما غير قابل للاختراق، سيتم القضاء على المخاطر تمامًا.
وعلى الرغم من أن تقييم نقاط الضعف يُعتبر في غاية الأهمية، إلا أنه لا يكفي للحماية من الهجمات السيبرانية. كما أن هناك عامل أساسي آخر يجب مراعاته وهو فهم الأنواع المختلفة للتهديدات السيبرانية المحتملة، وعندها فقط يمكن اتخاذ الخطوات اللازمة ضد هذه الهجمات وتطوير وسائل فاعلة لتخفيف الآثار. ويُعد تدريب الموظفين على الوعي بالأمن السيبراني جزءاً أساسياً من العملية لأنه يرتقي بالفهم فيما يتعلق بالتهديدات السيبرانية وطرق الحماية منها.

من الأهمية بمكان إجراء تحليل مسار الشبكة والتحقق من صحة تجزئة الشبكة والعزل الوظيفي. كما يجب دائمًا التحقق من بنية نظام الاتصال مقابل مستوى الأمان المطلوب للمنطقة التي يتفاعل معها.

الشكل ٦: بنيات السطر الواحد -مثال



الشكل ٧: ناتج بنية الشبكة التي توضح الترابط وتحليل المسار - مثال



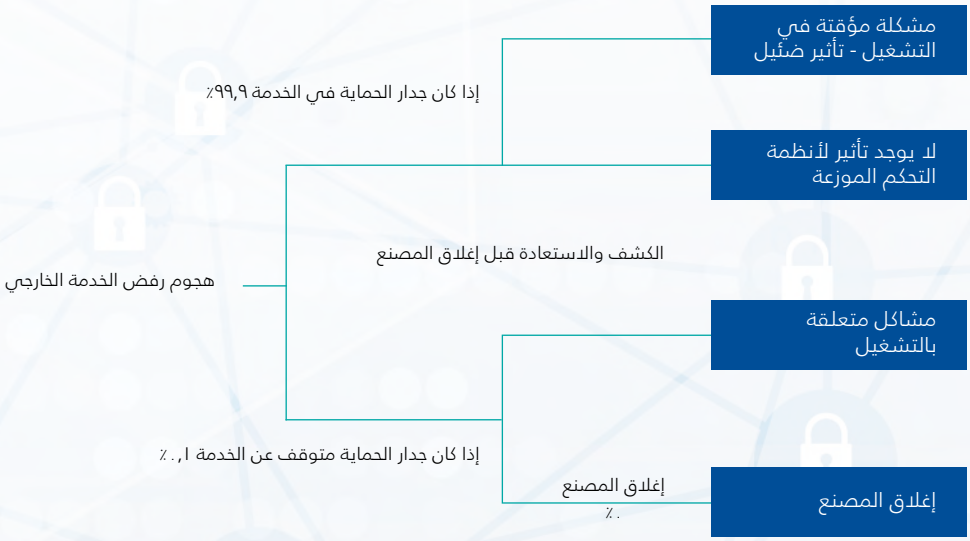
نتائج تحليل مخاطر العمليات السيبرانية

يجب أن تحدد نتيجة تحليل المخاطر والتهديدات نقاط الضعف والمخاطر المحتملة وتوفر مناهج قابلة للتنفيذ من شأنها تسهيل تنفيذ التوصيات العملية. وعلى الرغم من أن وضع تهديدات الأمن السيبراني متغير باستمرار، إلا أن هناك تصنيفات عامة لعوامل أو مصادر التهديدات المحتملة والتي يجب على المؤسسة وضعها في الاعتبار:

١. الهجمات الخارجية – فنية
٢. الهجمات الداخلية - غير فنية
٣. سوء الاستخدام الداخلي وسوء المعاملة
٤. الوصول غير المصرح به
٥. تسوية المعلومات (تعديل المنطق)
٦. أعطال في النظام
٧. انقطاع العمليات
٨. انقطاع نظام السلامة
٩. الأخطاء البشرية
١٠. التأثير غير المتوقع للتغييرات

يوضح الشكل ٨ كيف يكون هذا في التطبيق العملي، مع الأخذ في الاعتبار المخاطر المتبقية لأنظمة التحكم الموزعة ونشر التدابير المضادة.

الشكل ٨: المخاطر المتبقية لأنظمة التحكم الموزعة ونشر التدابير المضادة



فوائد تحليل مخاطر العمليات السيبرانية

بالنظر إلى المخاطر السيبرانية القائمة، والتي تتزايد بشكل واضح فيما يتعلق بالشركات الصناعية؛ فإنَّ الفوائد المترتبة على تحليل مخاطر العمليات السيبرانية عديدة، وأهمها بالتحديد هو تقييم أمن النظام. وعندما تُطبق منهجية تحليل مخاطر العمليات السيبرانية بالأسلوب الصحيح؛ فإنها تغرس الممارسات السليمة في جميع أنحاء النظام والتي من شأنها منع معظم الهجمات السيبرانية.

بالإضافة إلى الفائدة الواضحة للأمن السيبراني، يفيد تحليل مخاطر العمليات السيبرانية في الممارسات التجارية الأوسع للمؤسسة أيضاً. كما يوثق تطبيق منهجية تحليل مخاطر العمليات السيبرانية العمليات التجارية للمؤسسة ويتطلب إنشاء سياسات وإجراءات ومعايير وضوابط أمن المعلومات المتكاملة المستخدمة داخل المنشأة:

- تحديد وتوضيح استراتيجية أمن المعلومات المبينة على أهداف المؤسسة ووحدة العمل.
- تحديد المعرفة الهندسية ومحاذاة الضوابط الأمنية على أساس المخاطر وأهداف العمل.
- فريق عمل واثق وفاعل جراء وضوح الأدوار والمسؤوليات الخاصة بهم.
- تسهيل عملية تحديد أسباب وتأثيرات النظام المترابط وإدارة نقاط الضعف والمخاطر.
- إدارة الحوادث والاستجابة السيبرانية المحددة ذات الأولوية.
- وضع معايير للعمليات الأمنية المحددة، وإعداد التقارير، وتحديد متطلبات التكنولوجيا لتلبية أهداف العمل.

الشكل ٩: تحسين الإنترنت ومستوى السلامة والتكاليف من خلال العمليات الأمنية

دراسة حالة: تطبيق تحليل وتقييم المخاطرالمرتبطة بالإجراءات والعمليات السيبرانية (PHA)

التحديات في المنشأة

لقد كان العميل بحاجة إلى توحيد عملياته عبر بيئة متنوعة من الأنظمة تضمّ موردين ومتعاقدين متعددين؛ مما يجعل الجميع في نفس مستوى الأمان التشغيلي.

عدم وجود نظام لإدارة الأمن السيبراني

عدم وجود نظام لإدارة الأمن السيبراني محدد ومناسب لبيئة وطبيعة التصنيع

إجراءات غير متصلة بالعمليات

وجود كيانات متعددة يديرها العديد من أصحاب المصلحة المختلفين بعمليات وأنظمة منفصلة عن بعضها

عدم وجود شبكة مرجعية نموذجية

عدم وجود مخطط شبكة مرجعي قياسي ونموذجي وفقًا لنموذج بوردو وإرشادات معيار (الأيزا ISA ٦٢٤٤٣) لمصانعها المختلفة

تقرير ومقابلات لتقييم الفجوة

تعدّ هذه النشاطات ضرورية لفهم الوضع الأمني الحالي وفقًا لإرشادات الجمعية الدولية للأتمتة. ثم يتمّ لاحقاً إنشاء إطار عمل أمني موحد ومشترك وبرنامج نظام إدارة قياسي للمؤسسة بأكملها.

تصميم لوحات للمراقبة

تقوم الإدارة العليا بتمثيل الحالة الأمنية الحالية مقابل الحالة المستهدفة لبيئة أنظمة التحكم الصناعية لفهم مستوى التعرض للتهديدات.

تصميم خطة أساسية لتنفيذ المبادرات الأمنية المحددة

السماح للعميل بالتتبع وتنفيذ الخطط المطلوبة عبر بيئة أنظمة التحكم الصناعية وذلك حسب الأولوية.

التقييم الأمني التقني لتطبيقات وحدات التحكم المنطقية والقابلة للبرمجة ونظام التحكم الإشرافي وتحصيل البيانات (SCADA)

تقييم الوضع الأمنيالتقني العام للأجهزة المدمجة ووحدات التحكم المنطقية القابلة للبرمجة في المصنع. ثم تصميم ووضع سيناريوهات لحالات التهديد الخاصة بسير العمليات واستمرارية الأعمال وذلك لإجراء التقييم بشرط عرض العميل لمستوى الهجوم المحتمل ومناطق التسوية المحتملة في حالة وقوع هجوم فعلي.

تحليل مخاطر العمليات بناءً على تحليل مخاطر العمليات السيبرانية

مراجعة ثغرات الأمن السيبراني في بيئة العمل بناء على إجراء دراسة المخاطر وقابلية التشغيل و تحليل طبقة الحماية ورسم التقييم لفئات المخاطر المحددة عبر الصحة والسلامة والمالية والعمليات؛ وبالتالي ربط المخاطر الشاملة مع الثغرات.

تقرير تقييم مستوى أمن النظام

تقييم مستويات الأمن لكل نظام في كل منطقة في شبكة أنظمة التحكم الصناعية.

تطوير تقرير حول بنية الشبكة

تصميم مناطق وقنوات لكيانين مختلفين وبنوعين مختلفين من شبكات أنظمة التحكم الصناعية ثم تقديم الثغرات التي حُددت إلى المتعاقدين مع المصنع لتحسين تصميم بنية الأمن الشاملة للمصنع.

للتواصل :

تون ديمونت
رئيس استشارات الأمن السيبراني
كي بي إم جي في السعودية
E: antondiemont@kpmg.com
هاتف: +966 56 860 8393

حسين الشدوخي
رئيس استشارات الأمن السيبراني
لقطاع الطاقة والموارد الطبيعية
كي بي إم جي في السعودية
E: halshedoki@kpmg.com
هاتف: +966 50 014 7879

kpmg.com/sa

المعلومات الواردة هنا ذات طبيعة عامة ولا تهدف إلى معالجة أحوال أي فرد أو كيان معين. على الرغم من أننا نسعى لتقديم معلومات دقيقة وفي الوقت المناسب، غير أنه لا يمكن أن يكون هناك ضمان على أن هذه المعلومات دقيقة اعتبارا من تاريخ استلامها أو أنها ستظل دقيقة في المستقبل.لا ينبغي لأحد أن يتصرف بناء على هذه المعلومات دون مشورة مهنية مناسبة بعد إجراء فحص شامل للحالة المعينة.

إخلاء مسؤولية

أعُد هذا التقرير لأغراض معرفية فقط.
ووفقًا لذلك، لا تتحمل كي بي إم جي ولن تتحمل أي مسؤولية عن المعلومات المقدمة هنا أو طبيعة ومدى استخدام هذا التقرير.