تحقيق التقارب بين تقنية المعلومات والتقنية التشغيلية

الكفاءة والأمن السيبراني في قطاع الطاقة والموارد الطبيعية

ديسمبر ٢٠٢١ م

كي بي إم جي في السعودية

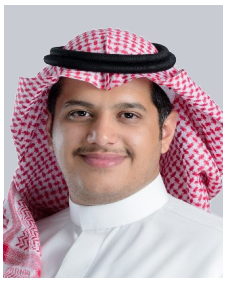
فهرس المحتويات

تمهيد

لطالما كان مفهوم تقنية المعلومات والتقنية التشغيلية مختلفين عن بعضهما البعض في المنشآت الصناعية، إذ تختلف كل منهما في الممارسات والأهداف والثقافة المتعلقة بهما والمعايير المتعلقة بين الأمن والكفاءة.

ومع ذلك، وفي ظل إدخال تقنيات جديدة إلى بيئة التقنية التشغيلية؛ أصبح من الضروري أن يتم تحقيق التقارب بين البيئتين، وخلافًا لذلك، ستكون الاستفادة من التقنيات الجديدة والبيانات المجموعة معدومة لدرجة كبيرة؛ مما يصعُب معه تبرير الاستثمارات اللازمة لتحديث بيئات التقنيات التشغيلية، فتحقيق التقارب يتطلّب من المنظمات تجسير الفجوات بين الأفراد والعمليات والأنظمة في بيئتي تقنية المعلومات والتقنية التشغيلية وبناء شبكة أكثر ذكاءً وأمانًا مع إمكانية وضع رؤية شاملة لمراقبة كلتا البيئتين والتحكم فيهما.

تون ديمونت
رئيس استشارات الأمن السيبراني
كي بي إم جي في السعودية



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

الانطلاق من الأساس

لا يدور التغيير حول التنفيذ أو المتابعة فحسب، بل يتعلّق بالتحضير له أيضاً، ويتطلب تحقيق التقارب بين تقنية المعلومات والتقنية التشغيلية أن تكون الشروط المسبقة –في بيئة المؤسسة وثقافتها– صحيحة وناجحة على الدوام.

وعلى الرغم من أنَّ بعض منشآت الطاقة والموارد الصناعية والطبيعية الأكثر نجاحًا في العالم تسير على طريق تحقيق التقارب بين تقنية المعلومات والتقنية التشغيلية، إلا أنَّ العديد من مثيلاتها الأصغرحجماً أوالأقل طموحًا لم تفعل ذلك حتى الآن، وفي هذا الإطار تُعيق الأنظمة والأشخاص والاستراتيجية هذه الشركات من البدء، أو تَحُد من تقدمها في عملية التقارب بين تقنية المعلومات والتقنية التشغيلية.

الأنظمة

عادة ما تكون أنظمة التقنية التشغيلية في أيّ منشأة أقدم قليلاً من أنظمة تقنية المعلومات نظرًا لطبيعتها التي تتطلب رؤوس أموال كبيرة وبروتوكولات السلامة التي تُفضل التناسق والثبات على التغيير. وتأتي البيئات الأحدث للتقنية التشغيلية، في معظمها -حسب التصميم- جاهزة بالفعل لتحقيق التقارب، ويمكن لهذه الأنظمة دعم التشغيل الآلي الكامل والرصد عن بُعد ويمكن بسهولة دمج أجهزة إنترنت الأشياء.

إنَّ عمر النظام وحده لا يعد بالضرورة عائقًا أمام تقارب تقنية المعلومات والتقنية التشغيلية. إذ يمكن تطوير بيئة التقنية التشغيلية لدعم الأجهزة الآلية والمراقبة وإنترنت الأشياء. ومع ذلك، لا تُعد أنظمة التقنية التشغيلية التي تستخدم معدات قديمة أو تُحدث فقط بالحد الأدنى من المستوى آمنة، ولا تهتم العديد من المنظمات بأمان هذه الأنظمة بسبب الرغبة في إبقائها منفصلة عن الإنترنت والشبكات الأخرى. وتجدر الإشارة إلى أن تحقيق أمان أنظمة التقنية التشغيلية هو شرط أساسي لتقارب تقنية المعلومات والتقنية التشغيلية، ولا بد من تطبيق إمكانيات الأمن السيبراني لتقييم الأنظمة القائمة ومعرفة التهديدات الحالية ومراقبتها باستمرار في المستقبل.

وثمة شرط أساسي آخر لتقارب تقنية المعلومات والتقنية التشغيلية، ألا وهو الفصل بين تقنية المعلومات والتقنية التشغيلية. قد يبدو هذا متناقضاً، ولكن إذا فُصلت بنية تقنية المعلومات عن بنية التقنية التشغيلية بوضوح قبل التقارب، فسيكون دمجهما في نهاية المطاف أسهل. ومن الأهمية بمكان إجراء ذلك في بداية دورة حياة تنفيذ مشروع التقارب بدلاً من إجراء ذلك في منتصف الطريق.

الأفراد

يُعد إعداد الأفراد والثقافة في المنشأة لتقارب تقنية المعلومات والتقنية التشغيلية أمرًا ضرورياً لتحقيق النجاح. وفي الواقع، غالبًا ما يكون الخطوة الأولى.

من المفترض بناء استراتيجية التقارب ابتداءً من القمة، ولسوء الحظ فإن مجرد طرح فكرة تقارب تقنية المعلومات والتقنية التشغيلية على مجلس الإدارة ينطوي على مشقة لبعض الشركات. وعندما لا تكون فوائد التقارب على المدى الطويل واضحة ومحددة ، فمن الصعب على مؤيديه التعبير عن الحاجة إلى التقارب أمام الإدارة أو مجلس الإدارة.

ويؤدي سوء الفهم إلى تقييمات غير دقيقة لعائد الاستثمارأيضاً، ولمعالجة هذه الصعوبات من المهم أن تحرص المنشآت على ضمّ مسؤولي تقنية المعلومات ومسؤولي التقنية التشغيلية في تقييم عرض\مقترح؟ تقارب تقنية المعلومات والتقنية التشغيلية، إذ في كثير من الأحيان، تستبعد المنشآت الصناعية مسؤولي تقنية المعلومات من هذه النقاشات.

وفي السياق نفسه، كثيراً ما تسمع المنظمات الصناعية آراء القادة التنفيذيين للعمليات قبل أن تسمع آراء القادة التنفيذيين لتقنية المعلومات، ومع ذلك يجب على القادة التنفيذيين للعمليات ولتقنية المعلومات تقديم مساهمات مهمة في التخطيط لاستراتيجية تقارب تقنية المعلومات والتقنية التشغيلي؛ وبالتالي فيما يتعلق بالمنظمات التي تأمل استكشاف تقارب تقنية المعلومات والتقنية التشغيلية، يجب تمكين الرؤساء التنفيذيين لتقنية المعلومات في فرق ومجالس الإدارة، وألا ينظر إليهم على أنّهم أدنى منزلة من الرؤساء التنفيذيين للعمليات.

ويجب أن يكون الأمن السيبراني جزءاً لا يتجزأ من مشروع تقارب تقنية المعلومات والتقنية التشغيلية منذ بدايته، وغالباً ما تقع مسؤولية تقارب تقنية المعلومات والتقنية التشغيلية على عاتق الرئيس التنفيذي لأمن المعلومات. وفي كثير من الحالات يدخل الرؤساء التنفيذيون لأمن المعلومات في مشروع التقارب في المراحل المتوسطة أو حتى المتأخرة؛ مما قد يعني أنَّ النظم والعمليات لا يتم دمجها بشكل آمن، ولذا يمكن للرؤساء التنفيذيين لأمن المعلومات، عندما يجري إدخالهم منذ مراحل التخطيط، تحديد المجالات الأكثر عرضة للتهديدات ووضع خطط لضمان أمانها في وقت مبكر.

الإستراتيجية

ومن الممارسات الجيدة التي يُمكن للمنشآت التي تدرس تقارب تقنية المعلومات والتقنية التشغيلية تطبيقها هي التحديد الواضح للحالات التي ترغب بحلها من خلال البيئات المتقاربة. هل ترغبون بأن تعمل أنظمتكم بكفاءة أكبر، وأن تُقدم رؤية أسرع حول بيانات الإنتاج والتحليل للقيادة، أم أنكم ترغبون في تحسين صيانة المعدات وخدمتها؟

وإذا فشلت المنشآت في تحديد أهداف واضحة لتحقيق تقارب تقنية المعلومات والتقنية التشغيلية، فقد تفشل في تنفيذ العمليات والأدوات المناسبة لبيئتها بالتحديد أيضاً، أو قد ينتهي بها المطاف بأهداف مبعثرة لا يمكن تحقيقها. وكلتا النتيجتين تقللان من فاعلية التقارب وتؤديان لانعدام الروح المعنوية والقبول للتقارب على المدى الطويل.

ومع ذلك، يجب على المنشآت، عند تحديد استراتيجية التقارب والمخرجات المطلوبة، أن توفر المرونة، سيما وأنَّ التهديدات والحماية وخاصة في مجال الأمن السيبراني تتطور بسرعة ؛ مما يحتم معالجة هذا الأمر من خلال تضمين المرونة في الإستراتيجية، وبالطبع، التطبيق صعب، ولكن لا بدّ من إيجاد حل وسط يسمح بالتكيف عند مواجهة الصعوبات الحتمية وبالوقت ذاته يحافظ على أهداف المشروع والجداول الزمنية بشكل واضح.

تقارب العمليات وسير الأعمال

تقارب العملية وسير العمل هو جزء لا يتجزأ من خطة التقارب الأوسع لتقنية المعلومات والتقنية التشغيلية، وإن إدخال التقنيات الجديدة إلى نظام متقارب دون تكييف العمليات وسير العمل مع النظام الجديد لن يحقق الفائدة التجارية المرجوة. وعليه وقبل أن تتمكن المنظمات من البدء في عمليات التقارب، من المهم التعرف على الأسباب التي تجعل عمليات تقنية المعلومات والتقنية التشغيلية مختلفة. وبمجرد تحديد «السبب»، يمكن للمنظمة النظر في كيفية تقارب العمليات دون المساس بفاعلية تقنية المعلومات الفردية أو عملية التقنيات التشغيلية أو سلامتها.

كانت ومازالت عمليات تقنية المعلومات والتقنية التشغيلية وسير العمل مختلفة دائماً - لسبب وجيه وتكمن السلامة في تحديد كل عملية من عمليات التقنية التشغيلية، والأفضل للسلامة هو الاتساق والاستمرارية، وبالتالي، تنحاز أنظمة التقنية التشغيلية للأنظمة والعمليات القديمة - فالتغيير نادر في تطبيقاتها وفي البُنى التحتية، ويجب أن يكون هناك سبب وجيه للقيام به. أما بالنسبة لعمليات تقنية المعلومات فهي عكس ذلك تماماً، ومن أجل تحقيق كفاءة أكبر في العمليات أو للتكيف مع المخاطر المتطورة، تُشجع عمليات تقنية المعلومات التحديثات المستمرة والتكيف مع التغييرات.

وتدعم هاتان النظريتان الأمن السيبراني بطريقتهما الخاصة، إذ يمكن أن تكون عمليات تقنية المعلومات آمنة بسبب تطويرها باستمرار لمعالجة نقاط الضعف عند ظهورها واستخدام دفاعات إلكترونية جديدة، ويمكن أن تكون عمليات التقنية التشغيلية آمنة بسبب التزامها الصارم بالإجراءات والتحكم الشديد في التغيير.

وقبل الدخول في بيئة التقارب، تحتاج عمليات الأمن السيبراني لتقنية المعلومات والتقنية التشغيلية وسيرالعمل إلى التكيف، ويمكن اكتساب معرفة كبيرة من إحداها وتسخيرها في خدمة الأخرى.

ويجب اعتماد مواقف أكثر صرامة تجاه العمليات وثقافة السلامة -وهي السمات المميزة لبيئة التقنية التشغيلية - داخل تقنية المعلومات أيضاً. والآن يحتاج مسؤولو تقنية المعلومات بعدما أصبح عملهم أكثر تكاملاً بطريقة مباشرة مع أنظمة التصنيع أو الإنتاج –والأشخاص الذين يُشغّلونها فعلياً- إلى الاعتراف بالمخاطر المرتفعة المرتبطة بالأمن السيبراني. ويجب أن يؤدي التغيير الثقافي الناتج في تقنية المعلومات إلى إعداد عمليات تقنية المعلومات وسير العمل على نحو أفضل للتقارب.

من ناحية أخرى، يجب تكييف عمليات التقنية التشغيلية وسير العمل لتناسب جدول تحديثات أكثر انتظامًا، وهذا النهج ضروري لدعم الأمن السيبراني في بيئة متقاربة تحتوي على أجهزة أكثر اتصالاً ونقاط ضعف محتملة. بالإضافة لذلك، يجري إطلاع مسؤولي تقنية المعلومات على هذا النهج، ويجب استخدام خبراتهم عند تصميم عمليات التقنيات التشغيلية الجديدة وأنظمتها وقدراتها لدعم التقارب.

يمكن لمركز أمن التقنية التشغيلية للتميز إعداد عمليات التقنية التشغيلية وسير العمل للتقارب ودعمها أثناء التقارب وبعده. ويُعتبر مركز التميز مهمّا لتدريب مسؤولي التقنية التشغيلية والمهندسين لحماية البنية التحتية الحيوية في ظل ظهور نقاط ضعف جديدة في تقارب تقنية المعلومات والتقنية التشغيلية. كما يمكن للمسؤولين التعلم من خلال التدريب العملي على تمارين الأمن السيبراني التي تحاكي المخاطر في العالم الحقيقي. وفي المقابل، يمكن لهؤلاء المهندسين تكييف سير عملهم حول الفهم الجديد للأمن السيبراني في بيئة متقاربة.

التفكير على مستوى الإدارة ومجلس الإدارة

قد يكون الأشخاص، وليست الأنظمة أو التقنيات - أهم عامل لنجاح تقارب تقنية المعلومات والتقنية التشغيلية، ومع ذلك، في حين يحظى الممارسون الفعليون لأنظمة تقنية المعلومات والتقنية التشغيلية – أي أولئك الذين يُشغلون الأنظمة – بكثير من الاهتمام، يضيع في الغالب من هم في قمة الهرم الإداري: أي الأشخاص على مستوى الإدارة ومجلس الإدارة.

بالإضافة إلى تحديد موازنة المنظمة أو أهدافها، يُحدد فريق الإدارة ومجلس الإدارة ثقافة المنظمة. وهناك جانبان رئيسيان للثقافة التي تدعم تقارب تقنية المعلومات والتقنية التشغيلية وهما الفهم والانفتاح، وعلى الرغم من أن الفهم والانفتاح قد يبدوان أكثر ملاءمة لتقديم المشورة الزوجية منها لعملية صناعية، إلا أنهما عمليان لكلا الأمرين.

ويُعد فهم كل فريق من فرق تقارب تقنية المعلومات والتقنية التشغيلية لأنظمة الفريق الآخر وعملياته بدرجة أفضل أمرًا في بالغ الأهمية لإعدادها، ومن شأن هذا الفهم أن يُحسن كفاءة العمليات المتقاربة حديثاً وسلامتها مثل نقل البيانات ورصد النظام.

وسيسهل الانفتاح –على النظراء في تقنية المعلومات أوالتقنية التشغيلية قبول البروتوكولات أو العمليات المشتركة الجديدة الناتجة عن تقارب تقنية المعلومات والتقنية التشغيلية. وإذا كان المسؤولون على دراية بالاحتياجات الفريدة لنظام تقنية المعلومات أو التقنية التشغيلية، فمن المرجح أن يقبلوا بالخطة وبالتنازلات حول اعتقاداتهم المتعلقة بتشغيل العمليات.

وهناك أيضاً المزيد من الخطوات العملية التي يمكن أن تتخذها المنظمات فيما يتعلق بفريق إدارتها ومجلس الإدارة لدعم تقارب تقنية المعلومات والتقنية التشغيلية.

وفي العديد من المنشآت الصناعية لا يكون الرئيس التنفيذي لتقنية المعلومات في مجلس الإدارة، وتأتي هذه الحقيقة بسبب طرق التفكير القديمة – ومفادها أنَّ العمليات أهم من أي شيء آخر، وخاصة تقنية المعلومات؛ وهذا الأمر يحتاج إلى تغيير على نطاق واسع تحديداً فيما يتعلق بالمنشآت التي تستعد لتقارب تقنيات المعلومات والتقنية التشغيلية؛ لذا لا بد لتقنية المعلومات من أن تحظى بمقعد في مجلس الإدارة من أجل تلبية احتياجاتها ورؤيتها وتضمينها في خطط التقارب.

ويمكن تطبيق هذا النهج على نطاق أوسع على الإدارة مع «تسوية» الآراء والمسؤوليات، ويجب ألا يكون رأي الرئيس التنفيذي للعمليات في منظمة صناعية بالضرورة أكثر أهمية من رأي الرئيس التنفيذي لتقنية المعلومات. ويجب أن يفهم المديرون الماليون تمامًا مخاطر وفوائد تقارب تقنية المعلومات والتقنية التشغيلية حتى يتم دعم عملية صنع القرار لهذه الجهود، فالقبول الكامل للإدارة ممكن فقط عندما يتم تقدير آراء الجميع وأخذها بالاعتبار.

توزيع المسؤوليات ما بين تقنية المعلومات والتقنية التشغيلية

على نقيض ما هو متوقع، من العوامل المهمة في نجاح تقارب تقنية المعلومات والتقنية التشغيلية هو معرفة أي العمليات يجب المحافظة عليها منفصلة، وبناء على ذلك، يُعد توزيع مسؤوليات الأمن السيبراني بين فرق تقنية المعلومات والتقنية التشغيلية أمرًا أساسياً لضمان ألا يجعل التقارب المنظمة أكثر عرضة للخطر مما سبق.

تتزايد أهمية وجود رؤساء أمن المعلومات التنفيذيين في المنشآت الصناعية، ومع ذلك، فإن المسؤوليات المختلفة للرئيس التنفيذي لأمن المعلومات داخل المنظمات الكبيرة والمتنوعة للأقسام المختلفة يُمكن أن تصبح مُرهقة وحتى خطيرة إذا كان الإضطلاع الشامل بها يمنع الفصل بين مسؤوليات الأمن السيبراني، وهناك طريقة لتجنب نقاط الضعف غير الضرورية الناجمة عن تحميل الرئيس التنفيذي لأمن المعلومات مسؤوليات إضافية تتمثل بتأدية دورين مشابهين لدوره – وهذان الدوران يتعلقان بتقنية المعلومات والتقنية التشغيلية - بالإضافة إلى دوره بصفته الرئيس التنفيذي لأمن المعلومات الذي يندرج تحت إشرافه على الدورين المذكورين. وتتمثل الفائدة من وجود رئيس تنفيذي لأمن المعلومات خاص بتقنية المعلومات وآخر خاص بالتقنية التشغيلية في دعم استراتيجية فصل مهام الأمن السيبراني من أجل منع أي هجوم سيبراني ينتقل من تقنية المعلومات إلى بيئة التقنية التشغيلية (أو العكس).

وتوضح إستراتيجية توفير رئيسين تنفيذيين لأمن المعلومات إستراتيجية أخرى أوسع نطاقًا لتوزيع مسؤوليات الأمن السيبراني بطريقة تمنع الهجمات من الانتقال من بيئة إلى أخرى. كما يجب ألا يكون المسؤولون عن جدار حماية تقنية المعلومات أيضا مسؤولين عن جدار حماية التقنية التشغيلية؛ وهذا الأمر منطقي على المستوى العملي – إذ يفصل الفريقان من المسؤولين بين الأنظمة والضوابط بإسلوب أفضل – وعلى المستوى الفلسفي – فإن استخدام أسلوب التفكير ذاته لإنشاء جداري حماية وصيانتهما يُخلف نظامًا أكثر «قابلية للاختراق» من استخدام أسلوبين مختلفين في التفكير.

ويُعد الوضوح الكامل للأصول من الشروط الأساسية للتوزيع الفاعل لمسؤوليات الأمن السيبراني؛ وتعني القدرة على رصد الأصول أولاً والحصول على رؤية للأصول الحساسة والحفاظ عليها، ثم استخدام أساليب قائمة على المخاطر عند تخطيط مراقبة الأمن الوقائي وتنفيذها.

تعزيز القدرات

يمكن للبُنيات المرجعية المختبرة على نطاق واسع وكذلك الحلول الأكثر تخصصاً والمتعلقة بإدارة البيانات وتخزينها تعزيز جهود تقارب تقنية المعلومات والتقنية التشغيلية للمنظمة.

هندسة مرجعية أمان الثقة الصفرية أو أمان انعدام الثقة

إن إنشاء بُنية مرجعية لأمن الشبكة أثناء تقارب تقنية المعلومات والتقنية التشغيلية سيحقق العديد من الفوائد، وتساعد البُنيات المرجعية جميع أصحاب المصلحة على التعاون والتواصل بفاعلية طوال العملية -وهي مهمة معروفة بصعوبتها بين فرق تقنية المعلومات والتقنية التشغيلية.

يمكن لمعايير (ISA/IEC 62443) أن تكون موردًا قيمًا للمنظمات التي تخضع لتقارب تقنية المعلومات والتقنية التشغيلية وتُعالج هذه المعايير المشكلات الأمنية المتفردة لأنظمة التقنية التشغيلية المتصلة.

من بين مهام التقارب المتعلقة بالأمن التي يعالجها المعيار (IEC 62443) هي ما يلي:

- تقييمات المخاطر السيبرانية للتقنيات التشغيلية
- بناء فرق إدارة الأمن السيبراني
- التحديث وغيرها من الضوابط الوقائية
- تقسيم مناطق الشبكة والقنوات وتأمينها
- إنشاء العمليات والحوكمة
- تحديد الأدوار والمسؤوليات المناسبة للمستخدمين أو الموارد

بالإضافة إلى ذلك، يُعد اختيار وإدارة الأجهزة المتصلة المناسبة لنظام فريد خاص بالتقنية التشغيلية أمرًا مهمًا لتأمين الشبكات من أجل تحقيق التقارب بين تقنية المعلومات والتقنية التشغيلية، ويعالج المعيار (IEC 62443) هذا الأمر ويُقدم التوجيه لتحسين العمليات القائمة لتحديد نطاق مشاريع التقنية واختيار البائعين والمشتريات. كما يحتوي هذا المعيار على مجموعة من المتطلبات والعمليات الإلزامية لدورات حياة تطوير المنتجات الآمنة المناسبة لبيئة التقنية التشغيلية المتصلة.

تعتمد النُهج التقليدية لتأمين شبكات التقنية التشغيلية منذ فترة طويلة على الحفاظ على فصل التطبيقات الصناعية عن شبكات تقنية المعلومات، ومع ذلك، فيما يتعلق بالمنظمات التي تخضع لتقارب تقنية المعلومات والتقنية التشغيلية، فإن طرق الفصل التقليدية غير كافية.

تأخذ الثقة الصفرية طرق الفصل التقليدية إلى مستوى أكثر دقة، وبدلاً من أن تبني جدارًا حول شبكة التقنية التشغيلية، فإنها تفترض بأن كل مستخدم أو جهاز أو نظام أو اتصال مُعرض للخطر بالفعل (افتراضياً) سواء كان داخل الشبكة أو خارجها. والهدف من الثقة الصفرية هو تقليل السطح المعرض للهجوم ومنع الحركة الجانبية مع التقسيم أو التقسيم الجزئي. وإذا حدث خرق، فلا يمكن للمتسلل الوصول بسهولة إلى أنظمة أخرى أو بيانات حساسة عن طريق التحرك أفقيًا.

إدارة البيانات

واحدة من أكبر فوائد تقارب تقنية المعلومات والتقنية التشغيلية هي توليد البيانات التي لم يستفد منها سابقًا. ويمكن استخدام هذه البيانات لتعزيز كفاءة عملية ما، أو تعزيز الأمن، أو إجراء الصيانة التنبؤية -على سبيل المثال لا الحصر. ومع ذلك، بدون ممارسات فاعلة لإدارة البيانات، فإن الكثير من قيمة هذه البيانات لا يتم إدراكها

في حين أن العديد من المنشآت تدير بياناتها عن طريق إرسالها إلى السحابة للتخزين أو المعالجة، فإن هذه الطريقة لا تسمح للمنظمات بالاستفادة من الإمكانات الكاملة لقدرات التقنية التشغيلية. ويمكن أن تتطلب معالجة كمية كبيرة من البيانات مباشرة أوقات استجابة كبيرة وكمية كبيرة من عرض النطاق الترددي. والحل البديل هو حوسبة الحافة.

تُقرب حوسبة الحافة تخزين البيانات ومعالجتها من مصادر البيانات. تحدث عمليات حوسبة الحافة على أرضية منشأة صناعية ما، مما يعني أن بعض البيانات فقط تحتاج للإرسال إلى السحابة للتخزين، أو التوزيع على المدى الطويل إلى شبكة مختلفة. يؤدي تقريب التحليل إلى تحسين وقت الاستجابة واستهلاك عرض النطاق. كما أنه يقلل من توزيع البيانات والمخاطر الكامنة في سرقة تلك البيانات أو تلفها أثناء نقل البيانات.

ويجب أن تشمل إدارة البيانات أيضًا جانب الأمان. بالإضافة إلى تخزين البيانات وطرق المعالجة مثل: حوسبة الحافة، تضمن ممارسة المشاركة الانتقائية الوصول إلى البيانات بالطرق المناسبة فقط. قد تتدفق بيانات محددة في اتجاه واحد، ذهابًا وإيابًا، أو لا تتدفق على الإطلاق، والحد من تدفق البيانات يجعلها أقل عرضة للتهديدات.

العوامل المتطورة لمخاطر الأمن السيبراني

مفارقة أمن التقنية التشغيلية

عادة ما تُنفذ أنظمة التقنية التشغيلية – وليس أنظمة تقنية المعلومات - العمليات التجارية الأكثر أهمية للمنظمة. وبالتالي، يمكن أن يكون وقت تعطل نظام التقنية التشغيلية أكثر تكلفة للمنظمة من وقت تعطل نظام تقنية المعلومات؛ ولذلك يفترض المنطق أن أمن نظام التقنية التشغيلية يجب أن يكون أكثر أهمية للأعمال التجارية من أمن نظام تقنية المعلومات.

ومع ذلك، فإن المفارقة هي أن معظم الشركات تستثمر الكثير من المال في تأمين أنظمة تقنية المعلومات الخاصة بها بدرجة أكبر من الاستثمار في تأمين أنظمة التقنية التشغيلية الخاصة بها. وفي هذا الصدد، لا يحتاج هذا النموذج الاستثماري بالضرورة إلى التعديل بشكل كامل، ولكن يجب اتباع نهج أكثر توازناً لتخطيط الأمن السيبراني والاستثمار خلال تقارب تقنية المعلومات والتقنية التشغيلية.

تقارب تقنية المعلومات والتقنية التشغيلية يُحسن من الأمن السيبراني

يتيح تقارب تقنية المعلومات والتقنية التشغيلية إمكانية رصد التهديدات وكشفها على نطاق أوسع. وقبل التقارب، من المرجح أن يكون للمنظمات رؤية محدودة للبنية والخدمات التي تعمل على النظام والتقنية التشغيلية الخاص بها. كما يتيح التقارب مع تقنية المعلومات إمكانية الرصد وجمع البيانات على نطاق واسع. عند تحليل هذه البيانات، يمكن استخدام تقنيات تحديد السمات لمعرفة المزيد عن اتجاهات النظام. وبمجرد فهم سمات وأنماط البيانات فهمًا أفضل، يمكن اكتشاف السلوكيات غير الطبيعية بسرعة دون انقطاع في العملية الصناعية.

ولجمع البيانات على نطاق أوسع فوائد تتجاوز الكشف عن التهديدات. بالإضافة لذلك، يمكن دمج مجموعات البيانات الجديدة مع مجموعات البيانات من أنظمة أخرى عبر نظام التقنية التشغيلية - وأنظمة المراقبة بالفيديو، مثل: الدوائر التلفزيونية المغلقة أو أنظمة إدارة المباني - للسماح بمراقبة أكثر شمولية واستخدام أفضل للبيانات.

ويمكن أيضاً تحسين صيانة المصنع من خلال تقارب تقنية المعلومات والتقنية التشغيلية. وتعتمد معظم المنظمات على الصيانة الوقائية لتقليل احتمال تعطل النظام والإصلاحات المكلفة. يتيح تقارب تقنية المعلومات والتقنية التشغيلية للمنظمات التحول من الصيانة الوقائية إلى الصيانة التنبؤية، وتجمع تقنيات الصيانة التنبؤية بيانات في الوقت الفعلي من أنظمة التقنية التشغيلية ويمكن أن تكتشف الحالات التي قد تؤدي إلى فشل المعدات. وعند القيام بذلك، يمكن إجراء إصلاحات محددة الأهداف قبل حدوث الأعطال -وهي طريقة غالباً ما تكون أقل تكلفة من الصيانة الوقائية، التي تتخذ نهجاً أوسع للإصلاحات.

ويجب على المنظمات أن تضع في اعتبارها أن مزايا الأمن السيبراني لتقارب تقنية المعلومات والتقنية التشغيلية محدودة بنوع وعمر نظام التقنية التشغيلية الخاص بالمنظمة. وغالباً لا تسمح أنظمة التحكم الإشرافي وتحصيل البيانات (SCADA) القديمة برصد التهديدات أو كشفها أو جمع البيانات على نطاق أوسع وهو أمر ضروري لبناء نظام بيئي أكثر أماناً، وتمتلك أنظمة التقنية التشغيلية التي تستخدم المزيد من أجهزة التقنية التشغيلية والأجهزة المتصلة نقاط الوصول للرصد وجمع البيانات وبالتالي فهي أكثر ملاءمة لفوائد الأمن السيبراني لتقارب تقنية المعلومات والتقنية التشغيلية.

يمكن أن يؤدي تقارب تقنية المعلومات والتقنية التشغيلية إلى خلق نقاط ضعف في مجال الأمن السيبراني

في حين أن تقارب تقنية المعلومات والتقنية التشغيلية يمكن أن يسمح بأمن سيبراني أكثر قوة، فإنه يُعرِّض أيضا أنظمة التحكم الصناعية وأنظمة التحكم في العمليات وغيرها من التقنيات التشغيلية لهجمات البرامج الضارة، والقرصنة، والتخريب على الموظفين وإلى المخاطر الأمنية الأخرى التي أثرت في السابق على أنظمة تقنية المعلومات للشركات فقط.

يتضمن تقارب تقنية المعلومات والتقنية التشغيلية دمج الأجهزة المتصلة ببروتوكول الإنترنت في نظام التقنية التشغيلية. وتجعل نقاط الوصول الإضافية هذه نظام التقنية التشغيلية أكثرعرضة للتهديدات القائمة على الإنترنت، ويستخدم العديد من هذه الأجهزة المتصلة تقنية من الدرجة الاستهلاكية وهي من بائعين متعددين - وكلتا الصفتين تجعلهما عرضة للهجمات السيبرانية.

في كثير من الأحيان، يُعد التغيير التنظيمي أصعب جانب من جوانب إدارة تقارب تقنية المعلومات والتقنية التشغيلية. ليس لدى الأنظمة أي آراء — بينما الإنسان لديه. يمكن أن تؤدي الاختلافات المعرفية والثقافية بين موظفي تقنية المعلومات والتقنية التشغيلية إلى نقاط ضعف يمكن لمهاجمي الإنترنت استغلالها. أحد الاختلافات الرئيسية بين عقلية تقنية المعلومات وعقلية التقنية التشغيلية هو التردد في تطويرات النظام أو قبولها في حين أن مسؤولي تقنية المعلومات يقومون بتحديث أنظمتهم باستمرار بهدف التحسين والأمان، فمن المرجح أن يلتزم مسؤولو التقنية التشغيلية بالأنظمة القديمة بسبب موثوقيتها.

يمكن أن يؤدي الإختلاف في الفكر ما بين مسؤولي تقنية المعلومات والتقنية التشغيلية إلى ضعف تكامل النظام؛ وهذا لا يؤدي فقط إلى نتائج دون المستوى لتقارب تقنية المعلومات والتقنية التشغيلية، ولكن أيضاً الى نقاط ضعف في النظام.

نقاط الضعف التي تم إنشاؤها بواسطة استضافة الشركات المصنعة للمعدات الأصلية المختلفة في بيئة واحدة

إن إدارة العديد من الشركات المصنعة للمعدات الأصلية في بيئة واحدة أمر صعب من منظور تشغيلي؛ لأن معظم أنظمة الشركات المصنعة للمعدات الأصلية لم تكن مصممة للعمل على النحو الأمثل مع أنظمة من بائعين مختلفين. ويمكن أن تؤثر خصوصيات النظام هذه أيضًا في سلامة البيئة. يحتاج مسؤولو النظام إلى تحديد نقاط الضعف والتحديث عند الضرورة.

في ضوء وجود نظام يحتوي على أجهزة وأنظمة فرعية من العديد من الشركات المصنعة للمعدات الأصلية، من المهم للمنظمة تعريف مسارات نقل البيانات وتحديدها، ويُعد نقل البيانات أمر بالغ الأهمية لنجاح تقارب تقنية المعلومات والتقنية التشغيلية، وبدون ذلك، فإن النظم تكون متكاملة بشكل سيء ولن يُسفر التقارب عن تحسين النظام المطلوب، ومع ذلك، يجب أن يقتصر نقل البيانات على الجهات التي يمكن أن يكون مفيدًا لها—خاصة من الشركات المصنعة للمعدات الأصلية المختلفة.

ومع ذلك، هناك اختلافات في الرأي حول سلامة استضافة العديد من الشركات المصنعة للمعدات الأصلية في بيئة واحدة، ويرى بعض المسؤولين أن وجود العديد من الشركات المصنعة للمعدات الأصلية يوفر حماية من المهاجمين الذين ينتقلون بسهولة من نظام إلى آخر. وفي رأيهم، إن وجود شركة واحدة مصنعة للمعدات الأصلية يُعرض المنظمة للخطر في كامل بيئتها .

التخفيف من مخاطر الهجوم أثناء تقارب تقنية المعلومات والتقنية التشغيلية وبعده

من المستحيل التنبؤ بهجمات اليوم الصفري بحكم تعريفها، ومع ذلك، فمن الممكن خلق دفاع ضدها، وفي ظل تقارب أنظمة تقنية المعلومات والتقنية التشغيلية، تحول المنظمة البيئة المغلقة إلى بيئة مفتوحة؛ مما يخلق نقاط ضعف جديدة لهجمات اليوم الصفري التي تحتاج إلى معالجة.

يمثل التقسيم الجزئي إحدى الممارسات التي تستخدمها المنظمات للتخفيف من أثر هجوم ناجح لمدة يوم واحد، وفي بيئة تقارب تقنية المعلومات والتقنية التشغيلية، تكون عناصر التحكم الأمنية التقليدية، مثل: أنظمة الشبكة المحلية الظاهرية غير كافية للحماية من هجوم اليوم الصفري. كما يوفر التقسيم الجزئي تحكمًا أكثر في حركة مرور الشبكة من خلال تقسيم الشبكة المحلية الظاهرية وإضافة نقاط أمن لكل قسم.*

وعلاوة على ذلك، يمكن تكييف التقسيم الجزئي مع بيئة تشغيل محددة ولأنواع محددة من حركة مرور الشبكة؛ وهذا يسمح للحد من حركة مرور معينة دون التقليل إلى أدنى حد من الفوائد المثلى لتقارب تقنية المعلومات والتقنية التشغيلية.

وعلى المستوى الأساسي، يمكن للمنشآت التخفيف من مخاطر الهجوم لمدة يوم واحد من خلال تنفيذ مبادئ «المرونة حسب التصميم» قبل تقارب تقنية المعلومات والتقنية التشغيلية. كما أن ترسيخ المرونة لدى الأشخاص والعمليات والأنظمة في منشأتك قبل التقارب سيقلل أيضا من تأثير هجوم اليوم الصفري في حالة حدوثه.

* https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-securing-ot-networks-with-microsegmentation.pdf

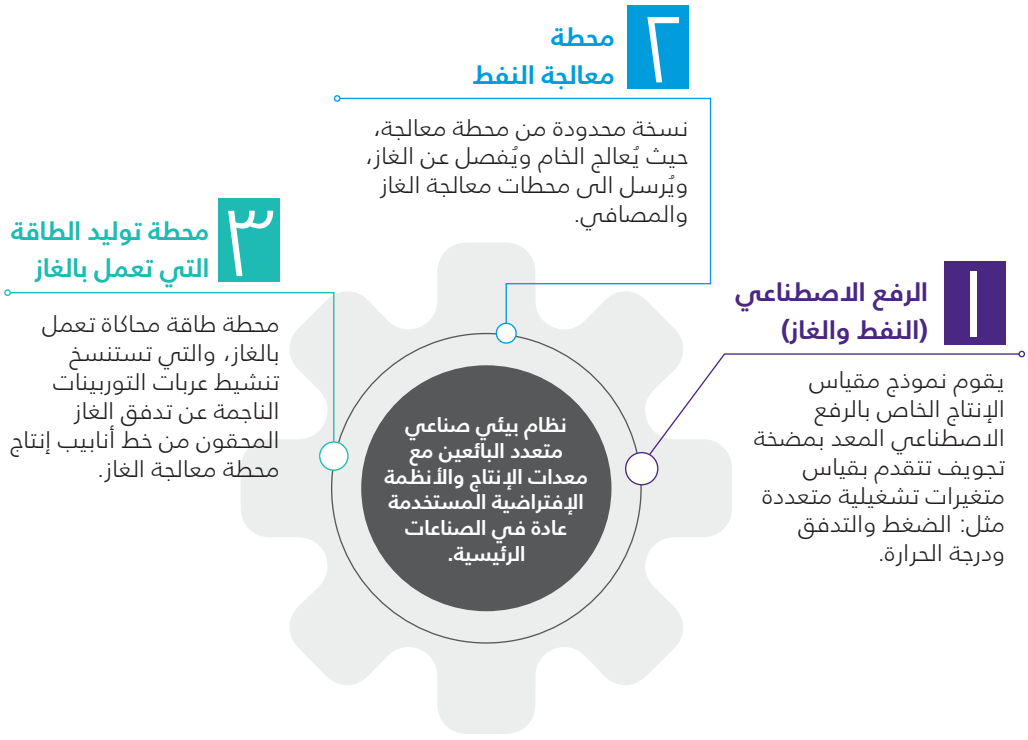
مختبرات النطاق السيبراني للتقنية التشغيلية / نظام التحكم الصناعي

تُعتبر محاكاة الهجوم السيبراني في بيئة التقنية التشغيلية عملية صعبة. في حين أن العديد من المتخصصين في مجال الأمن السيبراني في مجال تقنية المعلومات على دراية جيدة بطرق مختلفة مثل اختبار الاختراق والاختبارات الأخلاقية واختبار قوة دفاعاتهم السيبرانية، يكافح متخصصو الأمن السيبراني في التقنية التشغيلية للعثور على ممارسات مستخدمة على نطاق واسع لمحاكاة الهجمات السيبرانية للتقنية التشغيلية.

وفي محاولة لجعل جهود محاكاة التقنية التشغيلية تصل إلى مستوى تقنية المعلومات، أنشأت كي بي إم جي مختبرات النطاق السيبراني للتقنية التشغيلية / نظام التحكم الصناعي باستخدام معدات درجة الإنتاج لمحاكاة إصدارات نموذج النطاق من العمليات الصناعية، ويمكن استخدام المختبرات لإنشاء اتصالات آمنة عن بُعد من خلال البنية التحتية لشركة كي بي إم جي لأداء:

- دورات التدريب العملي
- محاكاة الهجوم السيبراني
- إثبات المفاهيم
- أبحاث قطاع الصناعة المتعلقة بالأمن السيبراني

أمثلة المحاكاة المخبرية:



ولا توجد بيئتان صناعيتان متشابهتان تماماً؛ ونتيجة لذلك غالباً ما ينطوي التدريب على التخصص المفرط لمجموعة محددة من بيئات التقنية التشغيلية وأنظمتها الخاصة بالمنظمة. وفي البيئة الافتراضية، يمكن تصميم مختبرات التقنية التشغيلية / نظام التحكم الصناعي التابعة لشركة كي بي إم جي لتتناسب مع الاحتياجات التدريبية المحددة للعملية الصناعية، حيث استثمرت كي بي إم جي على مستوى العالم وبنت مختبرات مختلفة في الولايات المتحدة الأميركية والاتحاد الأوروبي وسنغافورة والمملكة العربية السعودية، حيث صُمم كل منها لاستهداف عملية صناعية محددة.

يمكن بناء مختبرات كي بي إم جي الافتراضية لتكرار بيئات تقنية المعلومات والتقنية التشغيلية الخاصة بالمنظمة من خلال ربط الأجهزة المملوكة والمكونات الافتراضية للتقنية التشغيلية. وهذا يُمكّن المتخصصين في تقنية المعلومات والتقنية التشغيلية من التدريب عبر استراتيجيات الاستجابة للحوادث حتى الإتقان.

حالات الاستخدام المخبري:

١. دورات التدريب العملي على الأمن السيبراني للتقنية التشغيلية:

يمكن استخدام المختبرات لأداء دورات تدريبية عبر الإنترنت مع معدات مشابهة لمحطات الإنتاج لتعلم مفاهيم الأمن السيبراني للتقنية التشغيلية /نظام التحكم الصناعي. سوف يتعرف المتدربون على أداء مهامهم اليومية بطريقة آمنة عبر الإنترنت.

٢. عروض أداة الأمن السيبراني للتقنية التشغيلية

تساعد العروض العملية لأدوات الأمن السيبراني موظفي التقنية التشغيلية على فهم القدرات التقنية للأدوات فهمًا أفضل وتقييم استخدامها في سيناريوهات متعددة.

٣. عروض الهجوم السيبراني للتقنية التشغيلية

في المختبرات، يمكن تطبيق سيناريوهات متعددة لهجوم سيبراني على البيئة الصناعية لإظهار كيفية عمل أصول التقنية التشغيلية عندما تكون معطلة، تساعد السيناريوهات في إظهار نقاط الضعف والمعدات التي قد تتعرض للخطر في الهجوم.

٤. اختبار إصلاح الأمن السيبراني للتقنية التشغيلية

قبل تنفيذ خطة إصلاح الأمن السيبراني، يمكن استخدام المختبرات لإنجاز إجراءات الاختبار ومراجعة فاعلية الحل البديل والاعتماد عليه في بنية مماثلة.

تواصل معنا:

تون ديمونت
رئيس استشارات الأمن السيبراني
كي بي إم جي في السعودية
البريد الإلكتروني: antondiemont@kpmg.com
هاتف: ٨٣٩٣ ٨٦ ٥٦ ٩٦٦+

حسين الشدوخي
رئيس استشارات الأمن السيبراني لقطاع الطاقة والموارد الطبيعية
كي بي إم جي في السعودية
البريد الإلكتروني: halshedoki@kpmg.com
هاتف: ٧٨٧٩ ١٤ ٥٠ ٩٦٦+

ساهم في إعداد التقرير :

ديفيد فيربراش، رئيس استشارات مستقبل الأمن السيبراني، كي بي إم جي العالمية.
ديمتريوس بتروبولوس، رئيس استشارات الأمن السيبراني وخصوصية البيانات ، كي بي إم جي لورجالف.
رونالد هيل، الرئيس العالمي لاستشارات الأمن السيبراني، والشريك المسؤول عن قطاع الطاقة، كي بي إم جي في هولندا
داني ميتشو، القائد العالمي السيبراني لبنية إدارة المشروع، كي بي إم جي في أيرلندا
والتر أرييل ريسي، الرئيس العالمي لاستشارات الأمن السيبراني، والشريك المسؤول عن الأمن السيبراني لإنترنت الأشياء/التقنية التشغيلية، كي بي إم جي في الأرجنتين
جيسون هاوارد-غراو، المدير الإداري، خدمات الأمن السيبراني، كي بي إم جي في الولايات المتحدة
بابلو ألمادا، الشريك المسؤول عن الأمن السيبراني لإنترنت الأشياء/التقنية التشغيلية، كي بي إم جي في الأرجنتين
بيتر بانينك، مدير الدراسات والبحوث، كي بي إم جي في السعودية
مؤيد العليوي التسويق والاتصالات، كي بي إم جي في السعودية

KPMG.com/sa