دمج الحلول الأمنية في تصميم المدن الذكية

كيف نبني مدينة ذكية آمنة في عالم سيبراني متقلب

القمة العالمية للحكومات 2021

بالتعاون مع

EY

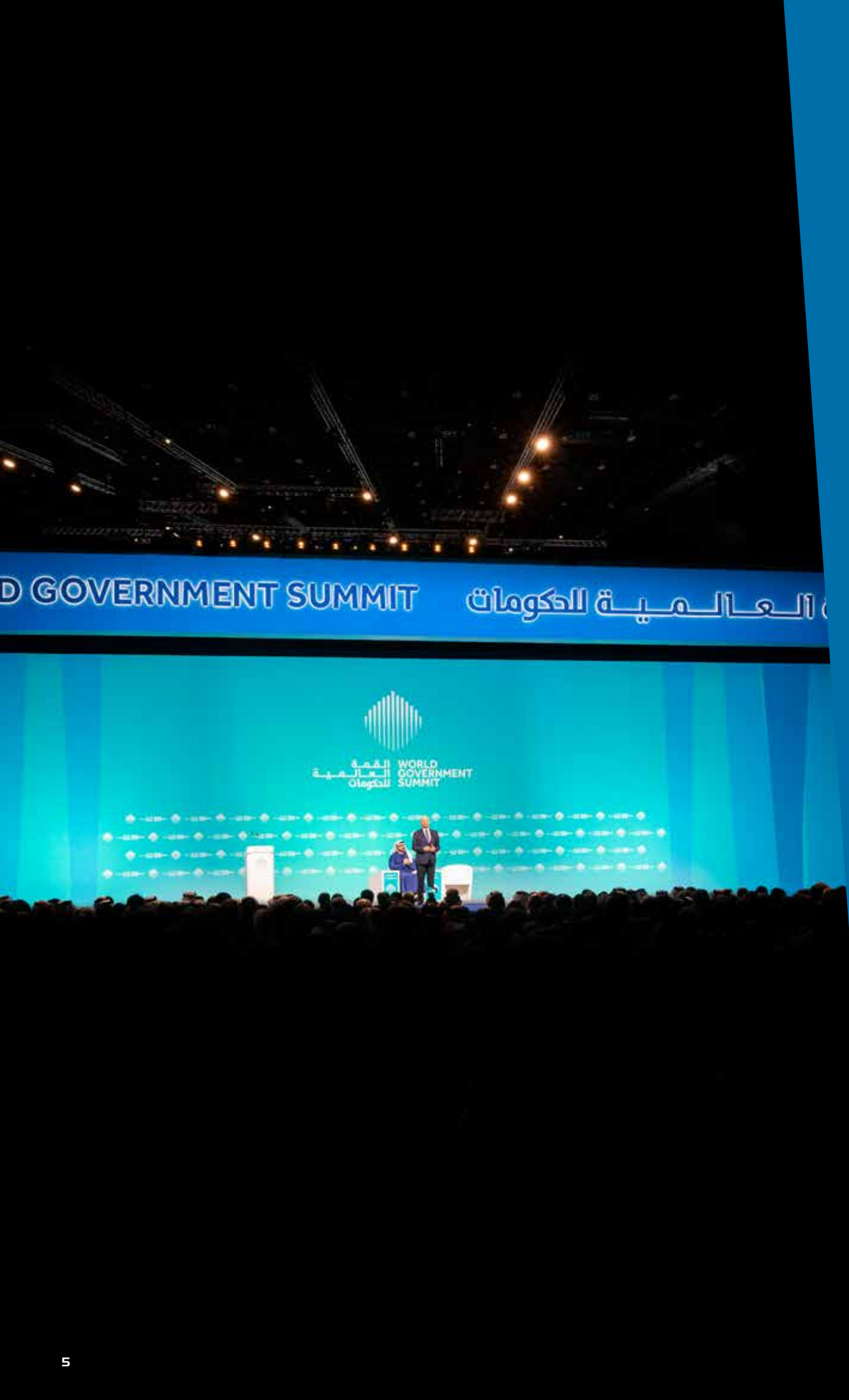
نبني عالماً أفضل للعمل

قائمة المحتويات

قائمة المحتويات

الإجابة على أسئلة الغد

القمة العالمية للحكومات منصّة عالمية تكرّس جهودها لاستشراف مستقبل الحكومات حول العالم، حيث ترسم القمة كلّ عام ملامح جدول الأعمال للجيل التالي من الحكومات، مع التركيز بشكل خاص على الاستفادة من الابتكار والتكنولوجيا في إيجاد حلول للتحديات العالمية التي تواجه البشرية. القمة العالمية للحكومات هي أيضاً مركز لتبادل المعرفة في مجالات العمل الحكومي واستشراف المستقبل والتكنولوجيا والابتكار، وهي منصّة تجمع بين قادة الفكرة وصناع السياسات والخبراء وروّاد الأعمال لتحقيق هدف مشترك واحد هو التنمية البشرية وتحسين حياة الشعوب. وتركّز القمّة العالمية للحكومات على دراسة وتحليل الاتجاهات المستقبلية والتحديات والفرص المتاحة عالمياً، إضافةً إلى عرض أحدث الابتكارات وأفضل الممارسات والحلول الذكية لتكون مصدر إلهام للإبداع في التصدّي للتحديات المستقبلية.


D GOVERNMENT SUMMIT
القمة العالمية للحكومات
WORLD GOVERNMENT SUMMIT

مقدمة

سيعيش 70٪ من سكان العالم في المناطق الحضرية بحلول عام2050، وسيفرض ذلك على الحكومات اتباع منهجيات مبتكرة واعتماد حلول رقمية متطورة لتلبية احتياجات هذا العدد المتزايد من السكان في المدن ومواجهة آثاره المترتبة على الأعمال.
وتتوقع الحكومات في شتى أنحاء العالم أن تعمل مدن المستقبل الذكية والمستدامة والمترابطة تكنولوجياً على توفير أسلوب حياة متطور وإنشاء أنظمة شاملة جديدة في جميع القطاعات، لا سيما الأغذية والمياه والطاقة.

وفيما تواصل المدن الذكية الاستثمار في التقنيات الناشئة والتقنيات الثورية لتحقيق النمو المستدام والتعامل مع عصر جديد من متطلبات السكان، حيث أن عملية التحول الرقمي السريع ستؤدي إلى ظهور عالم مجهول من التهديدات الإلكترونية التي قد تُحدث أضراراً جسيمة، مما يفرض على المدن الذكية والحكومات تحليل المتطلبات والاشتراطات الأمنية والاستثمار بقوة في تقنيات أمن المعلومات والاتصالات، والتي تشمل جميع الخدمات الرقمية،بالإضافة إلى تعزيز الوعي بالتقنيات الإلكترونية لدى جميع الجهات المعنية بما في ذلك السكان والموظفين الحكوميين.

تتناول هذه الورقة البحثية مجموعة من المواضيع الجوهرية للأمن السيبراني في المدن الذكية، والتي تشمل، على سبيل المثال لا الحصر، حوكمة الأمن السيبراني وحماية البنية التحتية الحسّاسة والتهديدات المتنامية التي يفرضها التحول الرقمي وخصوصية السكان والأساليب المبتكرة لتوفير الحماية المناسبة للجميع. كما تستعرض الورقة البحثية النتائج التجريبية والاستنتاجات العامة حول الاتجاهات العالمية فضلاً عن آراء الأشخاص المشاركين في الدراسة من أجل تناول هذه المواضيع من وجهات نظر مختلفة.

طرح الخبراء المتخصصون رؤاهم المكتسبة من مشاريع المدن الذكية وبرامج الأمن السيبراني العديدة التي يجري تنفيذها. وتوضح هذه الرؤى السبل التي يجب على المدن الذكية اتباعها من أجل دمج الحلول الأمنية خلال المراحل الأولى من التصميم، أي في مراحل صياغة الأفكار، وذلك بهدف التصدي للتهديدات السيبرانية التي تواصل مهاجمة الحكومات في أنحاء العالم.

7

لا شك أن فصل مفاهيم وتقنيات المدن الذكية عن البنية الحضرية للمدينة في المستقبل سيكون أمراً صعباً للغاية[1]. فمن أجل تطوير مدن ذكية مزودة بأعلى مستويات الأمن السيبراني، يجب أن نأخذ في الاعتبار التهديدات والمخاطر السيبرانية وأن نعمل على استكشاف النقاط المشتركة بين جائحة كوفيد-19 ومسارات القوى الأساسية الأخرى (كالتقنيات المبتكرة) وطرق تشكيلها للاتجاهات الحالية والجديدة في بناء المدن الذكية، بالإضافة إلى دمج الآليات الدفاعية وأساليب المراقبة السيبرانية في البنية التحتية للمدن من أجل الحد من الهجمات الإلكترونية والثغرات التي يمكن أن يستغلها المهاجمون.

ويترتب أيضاً على الحكومات تنفيذ مجموعة من الإجراءات لحماية أسس البنية التحتية الرقمية والحسّاسة للمدن من التهديدات والهجمات التي قد تطرأ في أي لحظة، مع مواصلة الابتكار لمواكبة التهديدات والجرائم السيبرانية مع تحديد الأولويات الأمنية وفهم المخاطر وتطبيق مستوى متطور من الضوابط الأمنية.

تناقش هذه الورقة البحثية هذا الجانب الذي يعتبر من العوامل الحاسمة في بناء المدن الذكية، وتستعرض بالتفصيل الحلول والممارسات التي ينبغي اعتمادها كي نتمكن من مواكبة عصر التحول الحضري والرقمي السريع من خلال دمج الحلول الأمنية في تصميم المدن الذكية.

تقدّر أحدث الدراسات أن الخسائر العالمية بسبب
الجرائم السيبرانية تجاوزت

1 تريليون دولار أمريكي[2]

1. إرنست ويونغ – كيف يبدو مستقبل المدن الذكية؟
2. تقرير McAfee و CSIS – التكاليف الخفية للجرائم السيبرانية التي تتخطى الاثار الاقتصادية

الملخص التنفيذي

أظهر الاستبيان العالمي لأمن المعلومات[3] الذي أجرته "إرنست ويونغ" في عام2020 أن 60٪ من المؤسسات والشركات واجهت حوادث جوهرية خلال الاثني عشر شهراً الماضية. وجاء حوالي خُمس هذه الهجمات من قِبل "النشطاء القراصنة" (أي النشطاء السياسيين والاجتماعيين الذين يقومون بهجمات إلكترونية لمناصرة قضاياهم)، لتحل في المركز الثاني بعد هجمات مجموعات الجريمة المنظمة والمسؤولة عن 23٪ من حوادث الأمن السيبراني. توضح هذه الإحصائية مدى التهديدات السيبرانية التي يجب على الحكومات في العالم الحذر منها. مع ذلك، يخلّف انتشار التقنيات الجديدة في بيئات المدن الذكية ثغرات إضافية يستغلها المهاجمون مما يؤدي إلى مخاطر يصعب الحد منها. لذلك يجب على الحكومات التي تتولى إدارة هذه المدن زيادة الوعي تجاه المخاطر عند البدء في تنفيذ أي مشروع تقني.

إضافةً إلى ذلك، يفرض التوسع الحضري ضغوطات كبيرة على المدن الذكية. فوفقاً للأمم المتحدة، يعيش نصف البشرية (3.5 مليار نسمة تقريباً) حالياً في المدن. وسيتحقق 95٪ من التوسع الحضري خلال العقود القادمة في دول العالم النامية، حيث من المتوقع أن يعيش 70٪ تقريباً من سكان العالم في المدن بحلول عام 2050، مما يفرض تحديات كبيرة على هذه المدن من حيث تلبية متطلبات سكانها. كما سيتسبب التحول الحضري السريع والبنى التحتية القديمة في ظهور تحديات بيئية واجتماعية واقتصادية كبيرة تحتاج إلى التصدي لها بأسرع وقت ممكن.

لذلك، يجب على المدن تطوير البنية التحتية القديمة لأنظمة وتقنية المعلومات فضلاً عن أساليب تقديم الخدمات التقليدية وأطر الحوكمة من أجل تحقيق النتائج المنشودة (وهي تقديم أحدث الخدمات لسكانها) والازدهار في المستقبل[4]. فإذا أرادت هذه المدن تطوير بنيتها التحتية بشكل كبير والاستفادة من التقنيات والحلول المبتكرة بأسلوب مستدام يحل مكان الأساليب التقليدية والنماذج التشغيلية لتقديم الخدمات، ينبغي عليها اتباع عمليات التحول الرقمي التي ستجعل منها مدناً ناجحة لها مكانتها في المستقبل.

تُعرّف "إرنست ويونغ" المدن "الذكية" بأنها المدن التي تواجه تحدياتها القائمة باستخدام الحلول الرقمية الشاملة لعدة قطاعات مع الاستفادة من تقنيات المعلومات والاتصالات لتحسين العمليات والخدمات الحضرية العامة والمستدامة[5]. ولمواجهة التحديات القائمة الناجمة عن التحول الحضري وإدارة البنى التحتية الحسّاسة بكفاءة، يجب على المدن الذكية تطبيق سلسلة من التقنيات الثورية التي غالباً ما تكون متداخلة في القطاعات والأنظمة والأجهزة المختلفة.

ولكي تتمكن المدن الذكية من إدارة عدد ضخم من الأجهزة المترابطة، يجب أن تتعاون المكونات الأساسية الثلاثة للبرنامج الرقمي فيما بينها، والتي يشار إليها بمصطلحات عامة هي الأشخاص وإجراءات العمل والتقنيات.

بالرغم من ذلك، فإن الربط بين الأشخاص وإجراءات العمل والتقنيات في بيئة المدينة الذكية مازال يتسبب في وجود ثغرات أمنية جديدة ونقاط وصول كثيراً ما يستغلها المجرمون في العالم الرقمي. وستضطر الحكومات إلى التركيز على المكونات الرئيسية التي تشكل أساس النظام الشامل مع فهم التهديدات المنتشرة التي ربما تؤدي إلى خسائر مالية للمدينة والإضرار بسمعتها، إضافة إلى تحديد دور هذه المكونات الأساسية في تعزيز الأمن السيبراني للسكان.

%60

من المؤسسات والشركات واجهت حوادث جوهرية أو كبيرة خلال الاثني عشر شهراً الماضية.

3.5 مليار

نسمة تقريباً يعيشون حالياً في المدن.

%95

من التوسع الحضري خلال العقود القادمة سيحدث في دول العالم النامية.

3. إرنست ويونغ – استبيان أمن المعلومات العالمية 2020
4. إرنست ويونغ – هل مدينتكم ذكية مثلما هم سكانها؟
5. إرنست ويونغ – كيف يبدو مستقبل المدن الذكية؟

كيف تصبح المدن "ذكية"؟

اعتُبر مفهوم المدينة الذكية اتجاهاً شائعاً على مستوى العالم لعدة سنوات بسبب ما شهدته هذه الفترة من تحول حضري ورقمي سريع، ويمكن أن ننسب نشأة هذا الاتجاه إلى تطور المدن على مستوى العالم.

المدن الذكية هي مجموعة من الأساليب المبتكرة والرائدة في تقديم الخدمات في جميع القطاعات باستخدام التقنيات الناشئة والثورية لابتكار مستقبل مستدام يعتمد على التقنيات الرقمية.

هناك أساليب متعارضة لتطبيق مفاهيم المدن الذكية وتختلف على مستوى المناطق والقطاعات، وقد ظهرت هذه الأساليب المتنوعة نتيجة للتحديات المختلفة التي يتم مواجهتها بالمفاهيم الذكية، مثل النمو السكاني داخل المدن والظروف الجغرافية والسياسية والتحولات الديمغرافية.

ولكي تحقق المدينة الذكية النجاح في تقديم خدمات مبتكرة و"ذكية" لسكانها، مع حماية أصولها الرقمية التي تستخدمها، يجب أن تضع في الحسبان المكونات الرئيسية الثلاثة للمدينة الذكية طوال مرحلة تنفيذ برنامج التحول الرقمي[6]:

1. الأشخاص

ترسيخ ثقافة إدراك المخاطر في المنظومة البشرية للمدينة الذكية

تعتبر المدن الذكية منصة فريدة بالنسبة إلى سكانها لتبادل أفكارهم والتعاون فيما بينهم والمساهمة في المبادرات "الذكية" كي يعيشوا حياة أكثر تطوراً تعتمد على التقنيات الرقمية.

تفضي العلاقات البشرية المتينة داخل المدينة الذكية، بما في ذلك القرارات والإجراءات المترتبة عليها، إلى نتائج قوية تفي بمتطلبات جميع الأفراد الذين يعيشون في هذه المدينة. كما يؤدي التعاون الوثيق إلى مجموعة من الآثار الإيجابية، على غرار الابتكار، مع عدم خلّوه من بعض الآثار السلبية كالجرائم السيبرانية.

يستهدف المجرمون السيبرانيون السكان أو الموظفين الذين يشغّلون البنى التحتية الحسّاسة على وجه التحديد، نظراً لافتقارهم للمعرفة الخاصة بالممارسات الجيدة للأمن السيبراني. فقد يستهدف المجرمون - مثلاً - الموظفين باستخدام رسائل التصيّد الاحتيالي الإلكترونية بجعلهم يضغطون على رابط ضار، أو يحتالون عليهم عبر المكالمات الهاتفية للحصول على البيانات الخاصة (التي تتضمن كلمات المرور الخاصة بالأنظمة الحسّاسة). ومن المعروف أن المدن الذكية هي ببساطة مجموعة من الأفراد يؤثرون بشكل منفصل أو جماعي على المدينة وكفاءة البنية التحتية. ولذلك يجب أن يكون كل فرد (حتى السكان) على دراية بالمخاطر والتهديدات الأمنية التي قد تؤثر على عمليات المدينة الذكية.

يُعتبر الوعي بالأمن السيبراني وأمن البنية التحتية لتقنية المعلومات أمراً في غاية الأهمية بالنسبة لجميع الأفراد بسبب المشاركة المتزايدة للسكان والأشخاص العاديين في عمل المدينة الذكية، كما يُعد أحد عوامل النجاح الرئيسية لأي مدينة ذكية. وينبغي وجود هيئة مركزية تدمج الأمن السيبراني في العمليات اليومية من خلال المعلومات الاستباقية وعمليات المراقبة والاستراتيجيات الأمنية وتعزيز الوعي الأمني. ويضمن وجود هذه الهيئة تلبية جزء كبير من متطلبات الأمن السيبراني في جميع المجالات والحد من مخاطر التهديدات التي تسعى لاختراق البنية التحتية للمدينة الذكية. كما يرسخ ذلك اتباع منهجية تنازلية للأمن السيبراني بدءاً من المستويات العليا وصولاً إلى مستوى السكان مع المنهجية التصاعدية من السكان إلى الإدارة العليا للمدينة، حيث يساهم السكان في تنفيذ الأفكار المبتكرة والضوابط الأمنية بشكل كبير.

يستهدف المجرمون السيبرانيون السكان أو الموظفين الذين يشغّلون البنى التحتية الحسّاسة على وجه التحديد، نظراً لافتقارهم للمعرفة الخاصة بالممارسات الجيدة للأمن السيبراني. فقد يستهدف المجرمون - مثلاً - الموظفين باستخدام رسائل التصيّد الاحتيالي الإلكترونية بجعلهم يضغطون على رابط ضار، أو يحتالون عليهم عبر المكالمات الهاتفية للحصول على البيانات الخاصة (التي تتضمن كلمات المرور الخاصة بالأنظمة الحسّاسة).

6. إرنست ويونغ – كيف يستطيع فكر الصمود تفكيك الطابع المعقد للمدن الحضرية

دراسة حالة: مدينة سنغافورة الافتراضية

تُعتبر "سنغافورة الافتراضية" مثالاً للمدن التي يجب أن تواكب النمو المتسارع خلال فترة زمنية وجيزة.

يسكن في هذه المدينة 5 ملايين نسمة تقريباً. ويعمل مشروع "سنغافورة الافتراضية" على تسجيل تحركات سكان المدينة ودراستها جيداً بهدف تعزيز خطط التطوير من خلال جمع البيانات الرقمية بمساعدة أجهزة الاستشعار والكاميرات.

يُعدّ هذا المشروع الأكبر من نوعه لجمع البيانات في مدينة بأكملها، إلا أنه لم يتضح حتى الآن الخدمات التي يجب استلهامها من هذه البيانات لتقديمها إلى سكان المدينة. إضافة إلى ذلك، يأخذ هذا المشروع في الحسبان الجوانب الاجتماعية الخاصة مثل رعاية كبار السن الذين يعيشون بمفردهم، وذلك بمساعدة عمليات الرصد بأجهزة الاستشعار مع تنظيم هيكل الإدارة العامة بكفاءة أكبر.

5 ملايين نسمة

يقطنون هذه المدينة

٢٢ آراء المشاركين في الدراسة

ما هي أنواع آليات المرونة السيبرانية ومنهجياتها التي تتوقع وجودها في المدن الذكية؟

مسفر المسفر

مدير إدارة أمن المعلومات في المدينة المعرفية الذكية التي يجري بناؤها في منطقة الشرق الأوسط

- إنشاء أنظمة مستقلة ومترابطة وغير متصلة بالإنترنت للتحكم في البنية التحتية الحضرية الحسّاسة.
- إنشاء أنظمة كهربائية مستقلة للقواعد العسكرية والمنشآت الحسّاسة الأخرى.
- مراجعة وتعزيز أمن البنية التحتية الوطنية الحسّاسة.
- توفير تدريب أمني منتظم لجميع السكان والموظفين الرئيسيين المشاركين في إدارة الأنظمة والمعلومات السرية.
- تطوير الإجراءات واللوائح التنظيمية للكشف عن الهجمات السيبرانية والإبلاغ عنها والتصدي لها.
- تطبيق الهياكل والسياسات الشاملة لحوكمة حماية البيانات.

2. إجراءات العمل

تقليل الهجمات السيبرانية بالاعتماد على إجراءات الأمن السيبراني الفعّالة

لا يمكن لأي مدينة أن تصبح آمنة إلكترونياً بشكل كامل، ولذلك فإن اتباع سياسات وإجراءات الأمن السيبراني المناسبة يساعد في الحد من المخاطر المرتبطة بالهجمات الإلكترونية.

وقبل كل شيء، ينبغي على المدن الذكية وضع استراتيجية الأمن السيبراني التي تراعي متطلبات جميع القطاعات وتركز على البنى التحتية الحسّاسة بشكل كبير. كما يجب أن تضمن وثيقة استراتيجية لتحديد الإجراءات واتباعها بصورة ثابتة ومستمرة.

تُعتبر الإجراءات التالية أساسية بالنسبة إلى المدينة الذكية، نظراً لقيمتها الهائلة في الحد من التهديدات السيبرانية.

تعزيز المرونة والتدرب عليها

يجب على المدينة الذكية وضع خطة للتعامل مع الحوادث الأمنية تتضمن الإجراءات والسبل اللازمة لمواجهتها وإعادة تقديم الخدمات بكفاءة وسرعة كي تتمكن من التعامل مع هذه الحوادث أو الوقائع الأمنية، إضافة إلى التدريب على تنفيذ هذه الخطة من أجل ضمان نجاحها.

فهم المخاطر والتهديدات

يمثّل فهم المخاطر والتهديدات عنصراً مهماً من عناصر الأمن السيبراني في المدن الذكية ويجب أن يكون جانباً أساسياً منه. تستطيع المعلومات الاستخباراتية الكشف عن الهجمات التي يقوم بها المجرمون عن طريق استغلال الثغرات الأمنية، حيث تتيح هذه المعلومات لفرق الحماية الأمنية تطبيق إجراءات أمنية وقائية إضافية (كتغيير إعدادات النظام) بشكل استباقي. ولذلك يجب على الفرق الأمنية توثيق الإجراءات التفصيلية لجمع بيانات التهديدات من مختلف المصادر والتحقق من صحة المعلومات الواردة من مصادر متعددة وإطلاع الجهات المعنية عليها.

تحديد الأصول عالية القيمة

لا يمكن حماية كل الأصول في الوقت الحالي نظراً للطبيعة المركّبة للأصول المستخدمة في المدينة الذكية والحجم الهائل للأصول الرقمية. ولذلك يجب على المدن الذكية تحديد أولويات الإجراءات الوقائية بناءً على الأمور الأكثر أهمية للمدينة، مما يساعد في تركيز جهود الحماية والحد من أكبر عدد من المخاطر. وربما يتسبب عدم تحديد الأولويات في إنفاق أموال بلا داعٍ أو إنفاق الأموال على حماية البيانات أو الأنظمة أو الأفراد أو الإجراءات الأقل أهمية بالنسبة إلى المدينة. ويتطلب تحديد الأصول عالية القيمة إجراءات موثقة وشاملة ودقيقة، بحيث توفر إرشادات توجيهية واضحة لقطاعات المدينة الذكية خلال عملية التحديد.

3. التقنيات

اعتماد التقنيات الناشئة والثورية لتقديم أحدث الخدمات

تؤدي التقنية دوراً أساسياً في تمكين المدن الذكية من تحقيق النتائج المرجوة منها. وتعتمد المدن الذكية بشكل كبير على استخدام التقنيات الناشئة والثورية من أجل تقديم خدمات ذكية فريدة، مع التخلي عن نماذج الأعمال التقليدية واستخدام نماذج أعمال جديدة ومبتكرة.

يمكن أن تتخذ التقنية عدة أشكال، بدءاً من الشبكات التي تقدم خدمات النقل وحتى البرمجيات والأجهزة التقنية التي تتيح تكامل الأنظمة المتعددة المكوّنة للمدينة الذكية.

تستخدم المدن الذكية البيانات والتقنيات الرقمية لتقديم أفضل الخدمات والمساعدة في تسهيل العمليات والإجراءات وتوفير الفرص لاتخاذ أفضل القرارات وغيرها من المزايا، وذلك من خلال الاستعانة بالأفكار والرؤى الناتجة من البيانات التي تم جمعها من مختلف أجهزة الاستشعار والأجهزة الأخرى المدمجة في منظومة المدينة الذكية. ومع ذلك، تعتمد التحديات على تلبية متطلبات العدد المتزايد يومياً من السكان داخل المدينة الذكية بسبب التحول الحضري الكبير الذي يشهده العالم بأسره. ولتلبية متطلبات هذا العدد الهائل من السكان، تستعين الحكومات بأنظمة متطورة للغاية ومتصلة بالإنترنت لتقديم خدمات النقل والمواصلات والطاقة والمياه والاتصالات. وتحتاج هذه الأنظمة المتطورة إلى قواعد إدارة وحوكمة راسخة، لأنها تمثل هدفاً رئيسياً للمهاجمين السيبرانيين بشكل عام[7].

وسيكون ترسيخ الأمن داخل منظومة المدينة الذكية التحدي الأكبر بسبب الكم الهائل من الأضرار التي يمكن أن تسببها الهجمات على أنظمة أو شبكات المدينة الذكية. ففي السيناريو الذي يستطيع فيه المهاجمون السيطرة على أنظمة التحكم في الإشارات الضوئية المرورية وأنظمة إمدادات المياه وشبكات الطاقة والمرافق الخدمية، ستكون الآثار بعيدة المدى وضارة للغاية! ولذلك تحتاج الحكومات وهيئات المدن الذكية إلى دراسة متأنية لمستويات الربط بين هذه المكونات الثلاثة (الأشخاص وإجراءات العمل والتقنيات) من أجل بناء بيئة إلكترونية آمنة تخفّف من التهديدات الأمنية بأسلوب فعال.

---

7. إرنست ويونغ – كيف يستطيع فكر الصمود تفكيك الطابع المعقد للمدن الحضرية

اعتماد التقنيات الثورية

تأخذ الحكومات في حسبانها التطورات التقنية وانتشار الأنظمة والأجهزة الجديدة المتصلة، حيث توفر التقنيات مثل إنترنت الأشياء وغيرها من التقنيات الثورية للحكومات فرصة جني المزيد من الفوائد من الأنظمة الحالية باستخدام برامج التحليل وأجهزة الاستشعار التي أصبحت أقل تكلفةً وأكثر تطوراً في نفس الوقت.[8]

المبادرات على المستوى الوطني

تسخّر الحكومات أحدث التقنيات المتطورة وتوظفها في إطار مشاريع المدن الذكية من أجل تسريع التنمية المستدامة. فعلى سبيل المثال، تُستخدم روبوتات الدردشة المعتمدة على الذكاء الاصطناعي لتقديم الخدمات بصورة أفضل، فيما تستخدم البيانات الضخمة وتحليلها لتصميم وتنفيذ السياسات الحكومية مع استخدام إنترنت الأشياء وأجهزة الاستشعار المرتبطة بها لتحسين القدرة على اتخاذ القرار بفضل الأفكار والرؤى المستلهمة من أنظمة البنية التحتية الحسّاسة. ويبدو واضحاً أن استخدام مثل هذه التقنيات أدى إلى تحسين القدرة على اتخاذ القرار وتعزيز مستوى الكفاءة في عمليات المدينة، كما أدى إلى تقليل المشكلات والتحديات العالمية المشتركة.

الفوائد

من أهم فوائد التقنيات الثورية المدمجة بسلاسة في البنية التحتية الذكية أنها تمكّن الحكومات من الحصول على أفكار مناسبة وتوفير المعلومات وتحفيز الاستجابة للتهديدات أو الحوادث. كما يوفر تطور البنية التحتية الذكية بعض الإمكانات المدهشة، حيث تفتح هذه البنى التحتية الذكية الباب أمام فرص دمج التقنيات الحديثة والثورية وتشكيل الأساس للمبادرات الذكية.

في الوقت نفسه، يُتوقع أن توفر المقاييس المدعومة بالتقنيات المتطورة قدراً كبيراً من الآثار الإيجابية على المدن حول العالم، لا سيما في المناطق الحضرية بقارتي آسيا وأفريقيا، نظراً لأنها ستشهد أكبر نمو حضري خلال العقود القليلة المقبلة. وقد أصدرت الجمعية الدولية للهاتف المحمول (GSMA) تقريراً أشارت فيه إلى أن مدينة بانكوك عاصمة المملكة التايلاندية – المعروفة بالازدحام والاختناقات المرورية الشديدة – يمكنها توفير مليار دولار سنوياً من خلال استخدام أنظمة النقل الذكية لتحسين حركة المرور وخفض الانبعاثات وزيادة مستوى الإنتاجية.[9]

وسنتناول فيما يلي ثلاث تقنيات ثورية تؤثر على المدن الذكية على مستوى العالم ونقدم مقترحات لتحقيق الأمن أثناء وبعد تطبيق هذه التقنيات.

8. إرنست ويونغ – هل مدينتكم ذكية مثلما هم سكانها؟
9. إرنست ويونغ – هل مدينتكم ذكية مثلما هم سكانها؟

دراسة حالة: برشلونة

كانت برشلونة كغيرها من المدن تبحث عن طرق لدرء الانكماش الاقتصادي والتنموي الذي حدث بعد الركود في العام 2008. قامت الحكومة المحلية باستخدام أحدث التقنيات الحاسوبية واعتماد مبادرات "المدينة الذكية" في 12 مجالاً، منها المياه والإنارة، للمساعدة في توفير الأموال وتحسين البنية التحتية الحضرية. وساهمت تلك الجهود على تقليل الازدحام وخفض الانبعاثات عبر أجهزة الاستشعار التي وجّهت السائقين إلى أماكن وقوف السيارات الخالية، كما ساعدت في إنشاء شبكة لأجهزة الاستشعار الخاصة بمراقبة هطول الأمطار والرطوبة، مما أتاح للمسؤولين التحكم في عمليات الري لتوفير المياه، إضافة إلى تركيب نحو 20,000 عداد ذكي لقياس استهلاك الطاقة وتحسين الكفاءة.

أدت جهود مدينة برشلونة إلى توفير 37 مليون دولار عبر أنظمة الإنارة الذكية و58 مليون دولار عبر عدادات المياه الذكية. كما زادت التدفقات النقدية المحصّلة من أماكن وقوف السيارات بواقع 50 مليون دولار بفضل اعتماد المدينة على تقنيات إنترنت الأشياء.

توفير

37 مليون دولار

عبر أنظمة الإنارة الذكية

58 مليون دولار

عبر عدادات المياه الذكية

زيادة التدفقات النقدية من أماكن وقوف السيارات بمبلغ

50 مليون دولار

1 إنترنت الأشياء وأجهزة الاستشعار

يمثل إنترنت الأشياء تحولاً هائلاً في العصر الرقمي، حيث بدأ تأثيرها في الظهور على جميع جوانب الأعمال والعمليات المرتبطة بها. وتستخدم معظم أجهزة إنترنت الأشياء تقنيات قائمة على أجهزة الاستشعار التي تحدد أو تقيس أي تغيير في المكان أو الموقع، أو ما إلى ذلك. وتُنقل البيانات التي جمعتها أجهزة الاستشعار إلى جهاز أو خادم مركزي، والذي يُستخدم بدوره لتحليل البيانات من أجل توفير معلومات مفيدة. واستخدمت المدن الذكية العديد من الأجهزة المترابطة وأجهزة الاستشعار القائمة على إنترنت الأشياء للحصول على مزايا التحول للعصر الرقمي، والتي تشمل أسلوب الحياة الذكي والتنقل الذكي والعدادات الذكية.

المخاطر والتحديات الحالية

أدى العدد الكبير من الأجهزة المتصلة والبنى التحتية للحوسبة السحابية التي تستخدمها المدن الذكية لتكون قادرة على تحقيق النتائج المرجوة منها، إلى مضاعفة تحديات الأمن السيبراني وتطورها باستمرار. وفي حال اختراق أحد هذه الأجهزة، يمكن أن يؤدي ذلك إلى اختراق جميع الأجهزة الأخرى المتصلة نظراً لعددها الكبير. ويوفر ذلك للمهاجمين نقاط دخول متعددة للوصول غير المصرح به إلى البنية التحتية للمدينة وأنظمتها الحسّاسة. بالإضافة إلى ذلك، كانت الحوسبة السحابية شرطاً أساسياً لظهور إنترنت الأشياء وتطورها. مع ذلك، أدى عدم وجود ضوابط أمنية في البيئات السحابية التي تمثل مركزاً لتخزين البيانات السرية، إلى العديد من الهجمات الإلكترونية التي هددت الأمن والخصوصية.

الإجراءات والحلول المقترحة للحكومات

ينبغي على الحكومات ترسيخ ثقافة دمج الحلول الأمنية والخصوصية في تصميم المدينة الذكية منذ البداية من أجل التصدي للتحديات الأمنية وتلبية متطلبات الأمن السيبراني. كما يجب على القائمين على المدينة الذكية تنفيذ العناصر التالية قبل اعتماد استخدام أجهزة الاستشعار القائمة على إنترنت الأشياء على نطاق واسع:

- يجب وضع سياسات حماية البيانات ومعايير أمن السحابة وتحديد الإرشادات التوجيهية واتباعها باستمرار في جميع البنى التحتية الحسّاسة التي تستخدم أجهزة الاستشعار لإجراء عملياتها.
- يجب اتباع منهجية حماية متعمقة ومتعدد الأوجه لضمان الأمن الشامل للأجهزة الذكية وأجهزة الاستشعار المستخدمة.
- يجب إعداد الحلول الأمنية لحماية النظام من الهجمات المعروفة وغير المعروفة (الهجمات الفورية)، والدخول غير المصرح به، والعبث بالمعلومات واختراقها، وتعطيل الخدمات، والتجسس والتهديدات الأخرى الناشئة من خلال المراقبة المستمرة وآليات الاستجابة التي تم اختبارها باستخدام تمارين المحاكاة والتدريبات التي تُجرى على أساس دوري.

2 السيارات المتصلة بالإنترنت [10]

انتقل مفهوم السيارات المتصلة بالإنترنت من مجرد كلمة غامضة إلى أحد مجالات التركيز في صناعة السيارات. وتوفر السيارات المتصلة بالإنترنت مزايا كبيرة مثل السلامة والأمن والكفاءة للعديد من الأطراف المعنية المشاركة في النظام الشامل لهذه السيارات، كما تقدم قيمة كبيرة للعملاء من خلال ربط أنظمة المعلومات والترفيه المختلفة معاً وإجراء تحديثات البرامج عبر الأثير والسيارات ذاتية القيادة.

المخاطر والتحديات الحالية

لم تُستكشَف مخاطر الأمن السيبراني المرتبطة بالتطورات وسُبل معالجتها المذكورة آنفاً بشكل كامل حتى الآن. ويمكن أن تتعرض السيارات ومركبات التنقل المتصلة بالإنترنت والتي تجمع قدراً كبيراً من البيانات، للعديد من محاولات الاختراق والقرصنة، مما يؤدي إلى تعطيل مزايا الأمان وانتهاك خصوصية العملاء. بالإضافة إلى ذلك، تواجه الشركات المصنعة للمعدات الأصلية (OEMs) وموردي السيارات تحديات ترتبط بالمنتجات المتطورة المعقدة، وإدارة الأنظمة المتكاملة التي تتكون من الشبكات والتطبيقات السحابية، والقرارات المتعلقة باستخدام تقنية الجيل الخامس أو اتصالات المركبة بجميع الأجهزة الأخرى المحيطة بها وسلسلة الإمداد المفتتة للغاية. إضافة إلى ذلك، يتعرض الطيف الترددي للاتصال والحوسبة السحابية للسيارات لهجمات ميدانية قريبة (على سبيل المثال، يكون المتسلل على مقربة من السيارة ويستخدم تقنية البلوتوث أو الاتصال اللاسلكي للوصول إلى البيانات السرية) أو الهجمات عن بُعد (أي يستهدف المتسللون الحوسبة السحابية للسيارات أو تطبيقات الهاتف المتحرك المرتبطة بها للوصول إلى البيانات أو التحكم في السيارات المتصلة بالإنترنت) مما يزيد من التحديات الأمنية المفروضة على هذه التقنية التي تفتقر في الأساس إلى التنظيم والمعايير القياسية الموحدة.

---

10. إرنست ويونغ – الأمن السيبراني وإنترنت الأشياء

الإجراءات والحلول المقترحة للحكومات

يمكن مواجهة التحديات المرتبطة بالسيارات المتصلة بالإنترنت باتباع منهجية السيارة المتصلة بالإنترنت مجرد حلقة واحدة في شبكة أوسع وأكثر تعقيداً. ولذلك يجب التركيز بدرجة أكبر على حماية الشبكة المعقدة (أي التفاعلات بين مستخدمي/مالكي السيارات والعديد من الأطراف المعنية الأخرى في المنظومة بأكملها). ويضمن اتباع هذه المنهجية أن يُنظر إلى الأمن بطريقة أكثر شمولاً مع الأخذ في الحسبان المنظومة بأكملها وما تتضمنه من أنظمة ومنصات وأطراف معنية، وعدم الاهتمام بأمن السيارات المتصلة بالإنترنت أو أجهزة الاستشعار أو أجهزة إنترنت الأشياء المرتبطة بها بصورة منفصلة.

ويتعين على إدارة المدن الذكية أن تأخذ في حسبانها أن نقاط الضعف غير المحددة والهجمات الفورية قد تؤدي إلى انعدام ثقة السكان، ولذلك ينبغي اعتماد منهجية دمج الحلول الأمنية في مرحلة التصميم. بحيث أن المدن الذكية ستحتاج إلى تحديد الحد الأدنى من المتطلبات الأمنية والأسس المرجعية للشركات المصنعة للمعدات الأصلية من أجل اعتمادها وتنفيذها. وتشمل القضايا الرئيسية التي يجب مناقشتها على مستوى المدينة الذكية في سياق الأمن السيبراني للسيارات المتصلة بالإنترنت أنظمة الاتصال المستخدمة في السيارات ومتطلبات التخزين السحابي للبيانات والبروتوكولات التي سيتم استخدامها للاتصال وتشفير البيانات والتحقق من هوية المستخدمين ونقاط الثقة الأمنية داخل شبكات المدينة (على أساس مستويات التأمين وضوابط التحكم في الدخول)، وآليات الحماية (مثل البوابات الأمنية والجدران النارية) والمراقبة الأمنية (مثل مراكز القيادة والتحكم التي تتيح التحكم عن بُعد في شبكات السيارات المتصلة بالإنترنت).

وبدأت هيئات المدن الذكية التعاون في هذا الصدد مع الشركات المصنعة للمعدات الأصلية وموردي السيارات من أجل دمج المستوى المطلوب من تجهيزات الأمن والسلامة في النظام الشامل للسيارات المتصلة بالإنترنت. إضافة إلى ذلك، ستواصل اللوائح التي حددها المنتدى العالمي لتنسيق اللوائح الخاصة بالمركبات، التابع للجنة الأمم المتحدة الاقتصادية لأوروبا (UNECE) فرض متطلبات الأمن السيبراني على السيارات المتصلة بالإنترنت في المستقبل.

3 العدادات الذكية والشبكات الذكية [11]

توفر العدادات الذكية والبنية التحتية للشبكات الذكية فوائد كبيرة خلال دورة حياة الطاقة في المدن الذكية، بدءاً من توليد الطاقة ووصولاً إلى التوزيع والاستهلاك. ويتضمن ذلك القدرة على مواجهة التحديات الجديدة التي تواجه الاستجابة للطلب، وتحسين كفاءة الشبكة المحلية، والتنبؤ بحالات انقطاع التيار الكهربائي قبل حدوثها، واستعادة الخدمة بسرعة بعد انقطاعها، وتعزيز وعي المستهلكين بشكل أفضل من خلال توفير بيانات استهلاك الطاقة بصورة فورية.

11. إرنست ويونغ – الأمن السيبراني وإنترنت الأشياء

تبدو البنية التحتية لشبكة العدادات الذكية كشبكة تتكون من أربع طبقات أساسية وهي الطبقة المادية (تتضمن محطات الطاقة التي تعمل بالفحم والغاز الطبيعي ومصادر الطاقة المتجددة المرتبطة بالشبكة وتوربينات توليد الطاقة بالرياح ومحطات الطاقة النووية) وطبقة الاتصالات (تتضمن الشبكات المنزلية وشبكة المكاتب)، ومنصات دمج الأنظمة معاً (تتضمن البنية التحتية للحوسبة) وأنظمة البرمجيات التي تتيح تحليل البيانات، والتحكم عن بُعد في إدارة الأحمال، ودمج واجهات الأجهزة، وما إلى ذلك. وتُدار هذه الشبكات عبر الشراكات ومؤسسات السوق مع مساهمة كبيرة من الحكومة بفرض اللوائح التنظيمية. ومن أجل تقديم أفضل الخدمات وتمكين الشبكات الذكية والعدادات الذكية من تحقيق أهدافها المرجوة، تجمع هذه الشراكات كميات كبيرة من البيانات تشمل معلومات التعريف الشخصية، والتي تحتاج إلى الحماية باستخدام حلول أمنية وآليات حماية متطورة مهما كلف الأمر.

المخاطر والتحديات الحالية

على الرغم من الفوائد الكبيرة التي توفرها العدادات الذكية والشبكات الذكية، يمكن أن تسبب الهجمات الإلكترونية المرتبطة بهذه البنى التحتية كوارث كبيرة بسبب العدد الكبير للمستهلكين الذين يعتمدون على العدادات الذكية وخدماتها. ولذلك، إذا لم تأخذ عملية الانتقال إلى إدارة الطاقة الذكية والشبكات الذكية في اعتبارها مخاطر الأمن السيبراني بصورة كبيرة، ربما تعرض المدن الذكية نفسها لتهديدات كبيرة قد تسبب أضراراً مالية وتشغيلية كبيرة وتقوض سمعة المدينة نفسها.

الإجراءات والحلول المقترحة للحكومات

يجب اتباع نهج أمني وتعاوني شامل يدمج الحلول الأمنية والخصوصية في تصميم المدينة من أجل الحفاظ على أمن العدادات والشبكات الذكية، حيث يتم تنفيذ مجموعة من الضوابط الوقائية والرقابية والتصحيحية لضمان أمن نظام العدادات الذكية، والذي يشمل الأجهزة وأنظمة الإدارة والمراقبة والبنية التحتية للشبكة ووسائل سداد الرسوم. ومن الضروري أيضاً أن تراعي إدارة المدن الذكية وشركات المرافق الخدمية تكامل أنظمة التحكم الإشرافي وجمع البيانات (SCADA) مع الشبكات الذكية، ويتيح ذلك لشركات المرافق الخدمية مراقبة الأجهزة داخل البنية التحتية للشبكة والتحكم فيها عن بُعد لتحقيق أعلى مستويات الكفاءة وإدارة المخاطر.

هناك بعض الضوابط الرئيسية اللازمة لتلبية المتطلبات الأمنية للشبكات والعدادات الذكية، منها الفصل بين الشبكات (ويفضل التقسيم الجزئي مع مستويات ثقة قابلة للتعديل)، وتشفير البيانات (أثناء النقل والتخزين)، والمراقبة الدائمة باستخدام التكامل مع أنظمة التحكم الإشرافي وجمع البيانات داخل مركز القيادة والتحكم، وتطبيق حلول التحقق من هوية الجهاز/المستخدم، ونماذج انعدام الثقة وتسجيل الأجهزة وإلغاءها.

كما ينبغي على هيئات إدارة المدن الذكية وضع إطار الحوكمة الملائم وإعداد السياسات والإجراءات المناسبة والمراقبة المستمرة، وتحتاج أيضاً إلى تنفيذ نموذج النضج الذي يستخدم الهياكل الجديدة لتحديد الفجوات المحتملة في البنى التحتية للطاقة والمرافق الخدمية.

نظرة عامة على عوامل الأمن السيبراني المرتبطة بالتقنيات الثورية

توضح الأمثلة المذكورة سابقاً أن المزايا العديدة لتبني التقنيات الثورية يترتب عليها عدد كبير من التعقيدات المتعلقة بالأنظمة المترابطة والمتكاملة داخل المدن الذكية، مما يؤدي إلى نشأة ثغرات يمكن أن يستغلها المهاجمون السيبرانيون.

ترسيخ ثقافة دمج الحلول الأمنية في تصميم المدن الذكية

يتعين على الحكومات في جميع أنحاء العالم بذل جهود كبيرة لترسيخ ثقافة "دمج الحلول الأمنية في تصميم المدن الذكية"، حيث إن التركيز والإنفاق الإضافي على الأمن السيبراني مدفوع حالياً بالمخاوف المتعلقة بالمخاطر. وقد أظهر الاستبيان العالمي لأمن المعلومات[12] الذي أجرته "إرنست ويونغ" أن الإنفاق على العديد من وظائف الأمن السيبراني يتم توجيهه بشكل كبير نحو العمل بالطريقة المعتادة بدلاً من تنفيذ المبادرات الجديدة، حيث تنفق بعض المؤسسات 5٪ أو أقل من الميزانية المخصصة للأمن السيبراني على المبادرات الجديدة. يشير ذلك إلى انخفاض الوعي وعدم التركيز على التعامل مع التهديدات السيبرانية المتطورة من خلال الاستثمار في تقنيات الأمن السيبراني الجديدة والناشئة التي يمكنها الاستجابة للتهديدات والهجمات السيبرانية وتحديد نقاط الضعف والثغرات الأمنية بشكل استباقي من أجل تحسينها. وبالرغم من القلق المتزايد بشأن المخاطر التي يمكن أن تسببها الأجهزة المتصلة بالشبكة، فإن 2٪ فقط من الشركات ترى مبادرات إنترنت الأشياء عاملاً محفزاً لإنفاق المزيد على الأمن السيبراني.

الأمن السيبراني أحد المكونات الأساسية في استراتيجيات المدن الذكية

يمثل اتخاذ الأمن السيبراني أساساً لاستراتيجية المدينة الذكية فرصة مهمة لإعادة تركيز الإنفاق على الأمن السيبراني. فمن خلال مواجهة التحديات الأمنية التي تعاني منها المدن الذكية حالياً، يمكن للحكومات والبلديات مساعدة المدن في الحفاظ على ثقة السكان والجهات التنظيمية ووسائل الإعلام، وتعزيز هذه الثقة. ولم يعد بإمكان الحكومات افتراض أن الأمن السيبراني يتمثل فقط في تحمل مسؤولية أمن المعلومات أو مهام إدارة تقنية المعلومات، بل يجب على المدن أن تجعل الأمن السيبراني جزءاً أساسياً من الاستراتيجية والثقافة العامة، مما يمكّن المدينة بأكملها وسكانها من فهم المخاطر التي تحيط بهم، وتحفيز الابتكار اللازم لمواجهة هذه المخاطر، والتمتع بالمرونة الضرورية لاستعادة العمليات بسلاسة وكفاءة في أعقاب أي عملية اختراق.

٪5

أو أقل من الميزانية المخصصة للأمن السيبراني في بعض المؤسسات والشركات تُنفق على المبادرات الجديدة

٪2

فقط من الشركات ترى مبادرات إنترنت الأشياء عاملاً محفزاً لإنفاق المزيد على الأمن السيبراني

12. إرنست ويونغ – استبيان أمن المعلومات العالمية 2020

التحديات والحلول الأمنية

يشهد العالم اليوم مستوى غير مسبوق من التحول الحضري؛ حيث يُقدر أن يبلغ عدد سكان المدينة الواحدة ضمن مجموعة من 66 مدينة[13] من 5 إلى 10 ملايين نسمة بحلول العام 2030. ويوفر هذا الاتجاه فرصاً كبيرة للمدن، ولكنه يضع ضغوطات ضخمة على أنظمة البنية التحتية القديمة التي تم تصميمها لتلبية متطلبات عدد أصغر من السكان وأقل تقدماً على المستوى التقني. وربما ينتج عن ذلك منح الأولوية لتلبية متطلبات السكان المتزايدين باستمرار من خلال تنفيذ الحلول المبتكرة بدلاً من إصلاح نقاط الضعف والثغرات الأمنية داخل البنية التحتية الحالية لتقنية المعلومات والتقنيات التشغيلية.

يفرض التحول الحضري السريع مع البنية التحتية القديمة تحديات ضخمة ربما يترتب عليها عواقب وخيمة. ففي حين أن التحول الحضري يدفع المدن إلى إعادة التفكير في استراتيجياتها والوصول إلى أفكار "ذكية" ومبتكرة باستمرار، فإن المدن لا تقوم بتحديث البنية التحتية التي تستضيف هذه التقنيات من أجل دعم مجموعة واسعة من الأنظمة المختلفة والمترابطة.

تُستخدم تقنيات المعلومات والاتصالات لتحسين العمليات والخدمات الحضرية، لا سيما الخدمات العامة وتنفيذ إجراءات الاستدامة البيئية والاجتماعية والمؤسسية من أجل ضمان التنمية المستدامة. ونقدم فيما يلي قائمة بالتحديات الأمنية الرئيسية التي تواجهها المدن الذكية بناءً على تجاربنا مع المدن الذكية في أفريقيا والشرق الأوسط من أجل دراستها أثناء تنفيذ البنية التحتية للمدن الذكية وترقيتها[14]:

يشهد العالم اليوم مستوى غير مسبوق من التحول الحضري؛ حيث يُقدر أن يبلغ عدد سكان المدينة الواحدة ضمن مجموعة من

66 مدينة

من 5 إلى 10 ملايين

نسمة بحلول العام 2030

---

13. الأمم المتحدة – مدن العالم في

14. إرنست ويونغ / مؤتمر الأمن الهندي / اتحاد الغرف التجارية والصناعية "اسوكام" الهند – الأمن السيبراني، ركيزة ضرورية للمدن الذكية

التحديات الأمنية

1. الأجهزة غير الآمنة
2. ربط الرؤية بالاستراتيجية والسياسات
3. تنفيذ البرامج المتعددة في نفس الوقت
4. مساحة الهجوم الكبيرة
5. عدم كفاية التمويل
6. غياب الهيكل الأمني الموحد
7. الضوابط الأمنية الخاصة بالبنية التحتية للتقنيات التشغيلية
8. نشر التقنيات الثورية

١١ آراء المشاركين في الدراسة

ما هي المخاطر والتهديدات السيبرانية الرئيسية التي قد تواجهها المدن الذكية بسبب تطبيق التقنيات الجديدة (مثل الذكاء الاصطناعي والجيل الخامس وإنترنت الأشياء)؟

مسفر المسفر

مدير إدارة أمن المعلومات في المدينة المعرفية الذكية التي يجري بناؤها في منطقة الشرق الأوسط

أعتقد أننا نمر حالياً بمرحلة فاصلة فيما يتعلق باستخدام التقنيات الجديدة. ويدرك البشر أهمية التقنيات الثورية، ولكنهم يحجمون عن منح السيطرة للآلات بغض النظر عما قد تشير إليه البيانات الإحصائية. يعود جزء من هذا القلق إلى الخوف الطبيعي من منح الآلات السيطرة، بينما تأتي البقية من إدراك أن الآلات يمكن اختراقها من قبل المجرمين الإلكترونيين والإرهابيين التقنيين، مما قد يسبب أعمالاً تخريبية واسعة النطاق إذا كان هؤلاء المجرمون قادرين على إعادة برمجة الآلات التي تسيطر على الأنظمة الأساسية. وتأتي التهديدات الرئيسية للمدن الذكية من المصادر التالية:

النشطاء القراصنة/المجرمون الذي يخترقون الأنظمة بغرض التلاعب بالحسابات أو سرقة البيانات أو تعديلها أو إتلافها.

الجماعات الإرهابية التي تخترق الأنظمة بهدف التخريب وإحداث الأضرار.

الدول التي تخترق الأنظمة بغرض التجسس.

التحدي الأول

الأجهزة غير الآمنة

المشكلة

تتمثل أحد أكبر المشكلات المتعلقة بالمدن الذكية في استخدام أجهزة الاستشعار بدون ضوابط أمنية ولا اختبارات شاملة. ونظراً لعدم وجود معايير قياسية موحدة لأجهزة إنترنت الأشياء، فيصبح من السهل قرصنة أجهزة الاستشعار. ويمكن للمجرمين اختراق أجهزة الاستشعار وإضافة بيانات مزيفة، مما يتسبب في توقف العمل وإغلاق النظام.

الحلول المقترحة

ينبغي على المدن الذكية تبني منهجية تدريجية في تحديث البنية التحتية واعتماد التقنيات الناشئة والثورية، مما يحد من أي تأثيرات سلبية على البنية التحتية لتقنية المعلومات ويضمن مراقبة نقاط الضعف والبحث عن الثغرات ومعالجتها. وتساعد هذه التحديثات التدريجية المدن الذكية في مواجهة التحديات الأمنية في البنية التحتية لتقنية المعلومات مع ضمان اختبار مكونات الأجهزة بدقة قبل اعتماد التقنيات على نطاق واسع. بالإضافة إلى ذلك، يمكن للحكومات وضع معايير موحدة للاختبارات وإنشاء معامل ومختبرات أمنية معتمدة لإجراء التقييمات الأمنية قبل تطبيق التقنية الجديدة وضمان مطابقتها للمعايير الأمنية المقررة.

التحدي الثاني

ربط الرؤية بالاستراتيجية والسياسات

المشكلة

تواجه المدن مشكلة ربط رؤية التحول الحضري بالاستراتيجية والسياسات الأمنية. وربما لا تتوافق الاستراتيجية والسياسات واللوائح الحالية مع رؤية المدينة الذكية الجديدة التي تم وضعها لتنفيذ برامج المدينة المستقبلية التي تشمل الاعتماد السريع للتقنيات الناشئة والثورية.

الحلول المقترحة

يمكن للمدن الذكية إنشاء مجموعة عمل أو لجنة تكون مسؤولة عن مواءمة الرؤية الشاملة مع استراتيجية الأمن وتنسيق أنشطة الأمن السيبراني. تم إنشاء هذه اللجان في جنوب أفريقيا تحت مسمى "مركز الأمن السيبراني"، وفي المملكة المتحدة، "المركز الوطني للأمن السيبراني" التابع لمكتب الأمن السيبراني وتأمين المعلومات (**OCSIA**). كما تشمل مسؤوليات هذه اللجان، على سبيل المثال لا الحصر، تقديم الدعم المستمر لتحقيق أهداف المدينة الذكية، وضمان تحقيق العائد على الاستثمار المخطط له، واعتماد التعديلات التي يتم إدخالها على استراتيجية الأمن السيبراني، مما يساعد في الوفاء بمتطلبات جميع القطاعات داخل المدينة ووضع استراتيجية ترتبط ببرامج المدينة المستقبلية.

التحدي الثالث

تنفيذ البرامج المتعددة في نفس الوقت

المشكلة

تحول المدينة إلى مدينة ذكية يتطلب العديد من المبادرات بالتوازي لتحقيق النتائج المخطط لها. ويمكن أن تواجه المدن الذكية تحديات متداخلة مثل التمويل والموافقات التنظيمية ومتطلبات البنية التحتية لتقنية المعلومات. ولكن بسبب تعدد المبادرات التي يجري تنفيذها بالتوازي، غالباً ما يتم تهميش الأمن ولا يحصل على القدر المناسب من الأهمية لدى الأطراف المعنية الرئيسية المشاركة في برنامج التحول. وتؤدي هذه التحديات إلى نشأة ثغرات أمنية محتملة في البنية التحتية وعادة ما يستغلها النشطاء القراصنة والدول الداعمة للهجمات الإلكترونية.

الحلول المقترحة

يجب دمج الأمن في المبادرات التي تتضمن استخدام التقنية في المدن الذكية باتباع منهجية دمج الحلول الأمنية في تصميم المدن الذكية. كما ينبغي أن تخضع عمليات استخدام التقنيات لتقييم المتطلبات الأمنية المرتبطة بالتنفيذ على يد فريق أمني متخصص. ويجب أن يكون هذا الفريق الأمني مؤهلاً وماهراً في إجراء عمليات تقييم الأمن السيبراني، وأن يتضمن عدداً كافياً من المتخصصين والخبراء القادرين على إدارة عدد كبير من المشاريع في نفس الوقت للحد من التحديات التي تنشأ نتيجة تعدد المبادرات.

التحدي الرابع

مساحة الهجوم الكبيرة

المشكلة

تستخدم عمليات المدينة الذكية بنية تحتية متشابكة لتقنية المعلومات من أجل تقديم الخدمات لسكانها. ويتصل عدد كبير من الأجهزة بشبكة المدينة الذكية، مما يزيد من مخاطر تعرضها للاختراق، وبذلك يتضاعف عدد نقاط الخطر التي يستخدمها المخترقون لمهاجمتها. وفي حال اختراق جهاز واحد، تصبح مُهاجَمة النظام بأكمله أو الشبكة بأكملها سهلة.

الحلول المقترحة

تحتاج الجهات التي تدير المدن الذكية إلى اعتماد منهجية دفاعية متعمقة ومتعدد المجالات تتماشى مع نموذج "كسر تسلسل الهجمات السيبرانية" **(kill chain model)** الذي يحمي الأجهزة المتصلة بالإنترنت من مجموعة متنوعة من التهديدات. إضافة إلى ذلك، من الضروري أن تتبنى البنى التحتية الحسّاسة تقنية الخداع (مثل المصائد الأمنية التي تسمى مصائد العسل "**Honeypots**" وفخاخ المحاكاة) من خلال إنشاء مصائد أو فخاخ لتحديد هوية المهاجم الذي حاول التسلل إلى البنية التحتية ومنعه من التسبب في مزيد من الضرر. وكذلك تعتبر مراقبة البنية التحتية على مدار الساعة من قبل الفرق المخصصة وآليات الاستجابة الإلكترونية (مثل الكتيبات الإرشادية لتفعيل الأتمتة والتدابير الأمنية لحماية المعلومات "**SOAR**") عنصراً مهماً آخر لمواجهة الهجمات السيبرانية التي تستغل العدد الكبير للأجهزة المتصلة بالشبكة

التحدي الخامس

عدم كفاية التمويل

المشكلة

تكافح المدن من أجل توفير التمويل اللازم لجهود التحول الشاملة. وتفتقر المدن إلى الأموال اللازمة للتحول إلى مدن ذكية بسبب انخفاض الميزانيات وتضارب الأولويات والعزوف عن الاستثمار في التقنيات والبنية التحتية الذكية. وتؤدي المشكلات المتعلقة بتمويل التحول إلى مدن ذكية إلى قيام الحكومات بتعويض التكاليف عن طريق تقليل حجم الاستثمار في الأمن السيبراني.

الحلول المقترحة

يجب على الحكومات مراعاة المتطلبات الأمنية والتكاليف المرتبطة بها من بداية برنامج التحول. ولا ينبغي أن تبدأ عملية التحول إلا بعد تحديد متطلبات الأمن السيبراني وتقييمها ومناقشتها على نطاق واسع على مستوى جميع القطاعات والأطراف المعنية الرئيسية. وبدلاً من تجنب المخاطر تماماً، يجب على المدن الذكية تعزيز الثقة في الأنظمة والتصاميم والبيانات لتتمكن من تحمل المزيد من المخاطر وتحفيز التغيير والابتكار. يتطلب هذا النهج إجراء تقييم المخاطر قبل نشر التقنية الجديدة وتنفيذ التقنيات الثورية، مع تقييم تأثيرها العام على البنية التحتية. كما يجب توفير ميزانية مخصصة للأمن السيبراني، بدلاً من الاعتماد على التمويل المقدم إلى الدوائر أو القطاعات الأخرى مثل تقنيات المعلومات والاتصالات.

التحدي السادس

غياب الهيكل الأمني الموحد

المشكلة

تفتقر المدن إلى وجود الاستراتيجية الشاملة والهيكل الأمني والأدوات اللازمة لإدارة برامج التحول. كما تعمل أنظمة المدينة "منفصلة" بعضها عن بعض. وهناك مشاكل مرتبطة بمشاركة البيانات والتعاون بين الأنظمة وتضارب الأولويات. وأدى ذلك الافتقار إلى الترابط بين أنظمة المدينة واتباع ضوابط أمنية غير متسقة عبر الأنظمة المستخدمة لإدارة البنية التحتية الحسّاسة إلى نجاح العديد من هجمات النشطاء القراصنة.

الحلول المقترحة

يجب على الجهات الحكومية التي تتحمل مسؤولية الأمن السيبراني تحديد الهيكل الأمني والمبادئ والضوابط والمعايير الأمنية الخاصة بعمليات استخدام التقنيات الجديدة. وينبغي أن يتضمن الهيكل الأمني التصاميم والسياسات والإجراءات والمعايير التي تساعد المسؤولين عن تشغيل البنية التحتية الحسّاسة على فهم متطلبات الأمن السيبراني وتصميم نماذج التقنيات الجديدة وتقنية المعلومات على النحو المطلوب. وكذلك يجب على الحكومة المركزية تحديد متطلبات الضوابط الأمنية لضمان عدم وجود نقاط ضعف ظاهرة في البنية التحتية.

التحدي السابع

الضوابط الأمنية الخاصة بالبنية التحتية للتقنيات التشغيلية

المشكلة

غالباً ما تتم إدارة البنية التحتية للتقنيات التشغيلية من خلال البنية التحتية العامة لتقنيات المعلومات، مما يعني أن جودة أنظمة التقنيات التشغيلية تتحدد وفق جودة البنية التحتية لتقنيات المعلومات. ويتم التحكم في الدخول إلى أنظمة التقنيات التشغيلية في كثير من الحالات عن طريق خدمة دليل المستخدمين في البنية التحتية المؤسسية لتقنية المعلومات. ولذلك ربما يؤدي اختراق البنية التحتية لتقنيات المعلومات إلى اختراق البنية التحتية للتقنيات التشغيلية المستخدمة في إدارة البنية التحتية الحسّاسة في المدينة.

الحلول المقترحة

تماشياً مع توصيات المركز الوطني للأمن السيبراني بالمملكة المتحدة، يجب على المدن الذكية عدم إدارة التقنيات التشغيلية من خلال البنية التحتية المؤسسية لتقنية المعلومات، وذلك لضمان عدم اعتماد أنظمة التقنيات التشغيلية على أنظمة المصادقة والترخيص الأقل مصداقية وحدها. إضافة إلى ذلك، يجب على المدن الذكية إنشاء هيكل موحد لمساعدة موظفي الأمن السيبراني على الالتزام بالضوابط الصارمة لإدارة المخاطر والامتثال لها، والتي يجب أن تكون موحدة في جميع القطاعات وتساعد على تتبع أي انتهاك لها.

التحدي الثامن

نشر التقنيات الثورية

المشكلة

تعتمد المدن الذكية التقنيات الثورية على نطاق واسع، على غرار الطائرات بدون طيار وإنترنت الأشياء وتقنية "بلوك تشين" وتعلم الآلة والتعلم الإدراكي. ومع ذلك، غالباً ما يكون الدافع وراء اعتمادها هو الحماس دون اتباع نهج عملي يتضمن تحليل تكلفة اعتمادها والعائد الناتج عنها. ورغم أن بعض الحكومات ربما تولي أهمية لإجراء تحليل التكلفة والعائد قبل اعتماد التقنية الثورية على نطاق واسع، فإن التحليل يفتقر إلى دراسة النفقات المرتبطة بالضوابط الأمنية التي سيتم تنفيذها من أجل حماية الأنظمة.

الحلول المقترحة

يجب على إدارة المدينة الذكية إجراء تحليل التكلفة والعائد بكفاءة، بحيث يتضمن المتطلبات الأمنية للتقنيات الثورية والناشئة. كما يجب دعم هذا التحليل بإجراء أبحاث مكثفة فيما يخص الضوابط الأمنية المرتبطة بالتقنيات الرائدة التي ربما ليس لها معايير أمنية محددة مسبقاً (مثل الهيدروجين الأخضر، والسيارات الطائرة، والتوصيل بدون تلامس من خلال الطائرات بدون طيار).

عادة ما يتم تنفيذ برامج التحول للمدينة الذكية باستخدام موارد محدودة مع تمويل منخفض وبدون وجود هدف عام. وغالباً ما تكون مشاركة الجهات والفرق المتخصصة في الأمن السيبراني في تنفيذ هذه البرامج المفككة محدودة للغاية. ويمكن أن يتسبب غياب منهجية دمج الحلول الأمنية في تصميم المدن الذكية في عواقب سلبية كبيرة تخلف آثاراً طويلة الأمد على البنية التحتية لتقنية المعلومات في المدينة الذكية. ولذلك يجب على الحكومات أن تؤدي دوراً نشطاً في برامج التحول وتنفيذها واستخدام التقنيات الجديدة ودمج الحلول الأمنية في عملياتها من خلال التوجيهات والإرشادات المحددة بدقة والتأكد من اتباع الهيكل الأمني الموضوع باستمرار في جميع القطاعات.

المدن الذكية المستدامة والآمنة على المستوى السيبراني في العصر الرقمي

من أجل تطوير المدن الذكية بشكل مستدام، يجب أن تأخذ الحكومات في اعتبارها التحديات وأن تبتكر الحلول الأمنية المخصصة لمواجهة هذه التحديات. ويؤدي عدم النجاح في اعتماد الحلول الأمنية المناسبة للمدينة الذكية إلى ضعف آليات الحماية، مما يمكّن القراصنة الإلكترونيين المدربين بشكل جيداً على يد الجماعات الإرهابية والدول الداعمة لها من استغلالها.

١١ آراء المشاركين في الدراسة

ما هي المخاطر التي تتعرض لها المدن الذكية عند اعتماد التقنيات الثورية والناشئة؟

الدكتور طه خدرو

شريك في قسم الاستشارات التقنية في شركة "إرنست ويونغ"

رئيس قسم الوجهات والمدن الذكية في شركة "إرنست ويونغ" في منطقة الشرق الأوسط وشمال أفريقيا ومشارك في برنامج "المدن المستقبلية العالمية" التابع لشركة "إرنست ويونغ".

يبدو أن ظهور إنترنت الأشياء أنشأ مزيداً من نقاط الضعف وفرض العديد من التحديات على المدن الذكية، حيث تتطلب أجهزة إنترنت الأشياء والأنظمة المرتبطة بها مستوى عالٍ من الحماية. ويمكن أن يؤدي اختراق جهاز واحد إلى أضرار كارثية على الأنظمة الحسّاسة التي تؤدي عدداً من العمليات الأساسية داخل المدينة الذكية. إضافة إلى ذلك، أدى الافتقار إلى التخطيط السليم ومراعاة حماية البنية التحتية للمدن الذكية إلى نجاح الهجمات الإلكترونية على الأنظمة الحسّاسة للمدن الذكية. ولذلك لم يعد إنشاء مركز عام للعمليات الأمنية كافياً في هذا العصر الذي تطوّر فيه المجرمون كثيراً، وتحتاج المدن الذكية إلى إنشاء مركز عام للقيادة والتحكم يكون بمثابة هيئة مركزية لعمليات المدينة الذكية.

اتجاهات الأمن السيبراني

وفقاً للأبحاث التي أجرتها "إرنست ويونغ" وبناءً على مشاركاتها في العديد من مشاريع المدن الذكية، هناك اتجاهات مختلفة تؤثر على المدن الذكية، ولها آثار مباشرة على عمليات المدن الذكية، كما تفرض تحديات على البنية التحتية فيها.

	اتجاهات الأمن السيبراني	الوصف
1.	**تحسين البنية التحتية**	يحظى تحسين البنية التحتية لتقنية المعلومات بأهمية كبيرة بسبب الاعتماد السريع للتقنيات الرقمية والحلول المبتكرة في إدارة البنى التحتية الحسّاسة بشكل أفضل، مع الحاجة إلى تقديم خدمات ذكية تلبي متطلبات السكان، مما يخلف تأثيراً كبيراً على البنية التحتية لتقنية المعلومات في المدينة.
2.	**زيادة عدد المدن الكبرى**	من المتوقع زيادة عدد المدن الكبرى (أي المدن التي يزيد عدد سكانها عن 10 ملايين نسمة)، من 33 مدينة في العام 2018 إلى 43 مدينة[15] في العام 2030. وسيفرض ذلك مزيداً من الضغوط على الحكومات من أجل تحقيق النتائج المرجوة منها من خلال الاستفادة من الحلول الرقمية الرائدة والمبتكرة التي ليس لها منهجية موحّدة للتنفيذ والإدارة.
3.	**الطفرة السكانية الكبيرة**	من المتوقع حدوث طفرة سكانية كبيرة وسريعة بارتفاع عدد السكان الذين تبلغ أعمارهم عن 60 سنة إلى 2,1 مليار نسمة[16] بحلول عام 2050، مما سيُحدث تأثيراً كبيراً على أنظمة الرعاية الصحية والبنى التحتية لتقنية المعلومات المرتبطة بها. وسيتعين على الحكومات الاستثمار بقوة في الأساليب المبتكرة لتوفير بيئة صحية لجميع السكان، لا سيما كبار السن.
4.	**تطبيق التكنولوجيا**	من المرجح أن يصبح استخدام التقنية لتقليل التكاليف طويلة الأجل للبنية التحتية ظاهرة بارزة في غضون السنوات القادمة. ويمكن للمدن الكبرى توفير التكاليف في الحاضر والاستثمار في المستقبل من خلال تبني استراتيجيات ربط البنية التحتية الحالية بالشبكات الرقمية التي يمكن أن تحقق أقصى استفادة منها.
5.	**إنترنت الأشياء**	يفضي دمج إنترنت الأشياء في الأنظمة الرقمية على نطاق واسع إلى تعزيز أسلوب الحياة، وستصبح هذه التقنية في غضون فترة قصيرة للغاية عنصراً ضرورياً في تقنيات وأنظمة المؤسسات. ومن المحتمل أن يؤدي استخدام أجهزة الاستشعار وأنظمة إنترنت الأشياء إلى آثار إيجابية بعيدة المدى، وتقوم الحكومات في جميع أنحاء العالم باعتماد تقنيات إنترنت الأشياء، إلى جانب البنية التحتية الذكية والشبكات المترابطة، كما بدأت في تقديم حلول مثل الشبكات الذكية وإدارة النفايات الذكية والتحكم الذكي في حركة المرور والمرافق الذكية، وما إلى ذلك.

	اتجاهات الأمن السيبراني	الوصف
6.	**حلول إزالة الكربون**	تتوفر الآن حلول جديدة لإزالة الكربون من أجل نماذج العمل الخاصة بمحايدة الكربون، مما يضيف قيمة طويلة المدى ويبرز ريادة المدينة الذكية في الحفاظ على المناخ[17]. وتؤثر حلول إزالة الكربون بشكل واضح على نماذج الأعمال وتفرض مجموعة واسعة من التحديات التقنية بسبب تحويل العمليات التشغيلية إلى الطاقة الكهربائية، بما في ذلك النقل والمواصلات، وعمليات التدفئة والتسخين والعمليات الصناعية التي تتسم بأصولها الكبيرة.
7.	**خبرات الأمن السيبراني**	تستثمر الحكومات بقوة في بناء الخبرات المحلية المتعلقة بالأمن السيبراني للحد من التهديدات المتزايدة. وتشير التقارير الصادرة مؤخراً إلى نقص كبير في مهارات الأمن السيبراني، والسبيل الوحيد لمواجهة هذا التحدي هو اعتماد برامج التدريب على الأمن السيبراني بدءاً من السكان العاديين. كما تشارك الجهات المسؤولة عن الأمن السيبراني في وضع المقررات التعليمية، فيما يشير إلى زيادة الوعي بأهمية الأمن السيبراني في القطاعات المهنية والصناعية.
8.	**التنسيق**	يتم اتباع منهجية متطورة في إدارة المخاطر السيبرانية والمشكلات المهمة من خلال التنسيق وتبادل المعلومات بين الأطراف المعنية المسؤولة عن البنية التحتية الحسّاسة والمؤسسات الحكومية والقطاع الخاص.
9.	**تحديد الأصول عالية القيمة**	نفذّت المدن الذكية الكثير من المشاريع والمبادرات لتحديد الأصول عالية القيمة المستخدمة في المدينة الذكية وفرض الضوابط الأمنية اللازمة لحمايتها من الاستغلال والاختراق والدخول غير المصرح به.
10.	**تحديث برنامج الأمن السيبراني**	يؤدي تطور المدن الذكية إلى تحديث برامج الأمن السيبراني فيها، مدعوماً بالاستراتيجية الانتقالية وخارطة الطريق، مما يساعد في التخلي عن البرامج الحالية المعرضة للخطر والتي ربما يستغلها المهاجمون ذوي القدرات العالية.
11.	**فرق الاستجابة لحالات الطوارئ الحاسوبية**	تتزايد أعداد فرق الاستجابة للطوارئ الحاسوبية (وحدات الاستجابة للحوادث الأمنية الحاسوبية) كلما تعرّض مزيد من المدن لحوادث الأمن السيبراني.
12.	**القوانين واللوائح**	سنّت الحكومات الكثير من القوانين لتطبيق أنظمة ولوائح الأمن السيبراني وحماية مواطنيها من الجرائم الإلكترونية. وتشمل هذه القوانين مجموعة كبيرة من الأنشطة الإلكترونية والوحدات المتخصّصة في الجرائم الإلكترونية التي تتعامل مع النشاط الإجرامي على الإنترنت وتتصدى له.
13.	**نموذج التشغيل المرن**	ما زالت جهود التحول إلى النماذج التشغيلية المرنة تتواصل بالتزامن مع التغييرات الجذرية التي تحدث في هذا العصر الرقمي. ويجب على الجهات المسؤولة عن الأمن السيبراني في المدن الذكية أن تطور نطاق اختصاصاتها ومجموعة مواردها وإمكاناتها وشراكاتها باستمرار. فسيكون إلزامياً على هذه الهيئات أن تتسم بالمرونة في أعمالها من أجل تلبية متطلبات واتجاهات المستقبل، فضلاً عن توفير أسس راسخة من خلال تجديد هيكلها الأساسي.

---

15. الأمم المتحدة – مدن العالم في 2018
16. مدونات البنك الدولي – هل المدن جاهزة لمواجهة تزايد عدد سكانها كبار السن؟
17. تقرير إرنست ويونغ للاتجاهات الكبرى في العام 2020

اتجاهات منذرة بالخطر

يعتبر معدل اعتماد الحكومات والمدن الذكية في جميع أنحاء العالم للرقمنة بسرعة لا تعادل الاهتمام بالأمن السيبراني وتنفيذه من الاتجاهات الأكثر إثارة للقلق. وأوضحت المقارنة بين تقرير مؤشر الأمن السيبراني العالمي (GCI) للعام 2018 ومؤشر الأمم المتحدة لتطور الحكومة الإلكترونية إلى أن البلدان التي تعتلي مؤشر تطور الحكومة الإلكترونية لا تستثمر بالضرورة في الأمن السيبراني بنفس مستوى الالتزام والعكس صحيح. إضافة إلى ذلك، أشارت دراسة مفصلة لتقرير المعهد الدولي للتطوير الإداري حول مؤشر المدن الذكية للعام 2020 إلى أن الأمن لا يعتبر أمراً مُلحاً أو ذا أولوية بالنسبة لغالبية المدن الذكية التي تتصدر التصنيف. ويعتبر ذلك أحد الأسباب المهمة التي تثير القلق، حيث يدل على أن المدن الذكية وحكوماتها ما زالت لم تمنح جهود الأمن السيبراني الأولوية، رغم أنه يجب أن يواكب رحلة التحول الرقمي والرقمنة الشاملة.

وضع التهديدات السيبرانية

مع استمرار ية تطور التهديدات وتوسعها، تواصل الجهات والمؤسسات الخاصة والحكومات في جميع أنحاء العالم مواجهة تحديات الأمن السيبراني. وأصبحت الهجمات الإلكترونية، على غرار هجمات تعطيل الخدمات والهجوم الوسيط والتصيّد والبرمجيات الخبيثة، شائعة في العالم الذي يعتمد على الحلول الرقمية بمعدل غير مسبوق، وهو ما تؤكده جميع نتاج الأبحاث الحالية. أظهر الاستبيان العالمي لأمن المعلومات الذي أجرته "إرنست ويونغ" أن ما يقرب من نصف مجالس إدارة الشركات (48٪) يعتقدون أن شركاتهم ستتعرض إلى حد ما للخسائر الناجمة عن الهجمات الإلكترونية أو عمليات انتهاك البيانات خلال الاثني عشر شهراً القادمة، ويعتقدون أيضاً أن 40٪ من تلك الهجمات ستأتي من المجموعات الإجرامية المنظمة أو "النشطاء الاجتماعيين القراصنة"[18].

تعزز هذه البيئة من صعوبة سعي المدن الذكية والحكومات في جميع أنحاء العالم وراء الفرص الرقمية وتطوير نماذج أعمالها لزيادة الكفاءة التشغيلية. ففي هذه الحالة تحتاج المدن الذكية التي تسعى إلى تعزيز قدرات الأمن السيبراني لديها إلى تطوير فهم أفضل لطبيعة التهديدات والمخاطر التي قد تؤثر عليها. ويمكن للمدن الذكية تمكين بيئة آمنة ومرنة من خلال تحديد طبيعة التهديدات والمخاطر التي تؤثر عليها ودراسة سُبل ظهور هذه التهديدات. وينبغي على الهيئات المسؤولة عن المدينة الذكية طرح الأسئلة المهمة المرتبطة بالأطراف المعنية الرئيسية وتنظيم منتديات للمناقشة تضم هذه الأطراف وممثلين عن جميع القطاعات لتعزيز معرفتهم بالتهديدات السيبرانية.

وينبغي على الجهات المسؤولة عن المدينة الذكية مناقشة ودراسة أنواع التهديدات والآثار المحتملة التي قد تنتج عنها قبل اختيار وتنفيذ آليات دفاعية متطورة تحمي أصولها الرقمية. وتزداد ثقة المدن الذكية في قدرتها على الحد من أنواع معينة من الهجمات المختلفة التي أصبحت مألوفة في السنوات الأخيرة (مثل برامج الفدية والهجوم الوسيط)، ولكن التحدي يكمن في مواجهة التهديدات دائمة التطور، حيث يزداد المهاجمون ذكاءً ويستخدمون تقنيات جديدة ومتطورة للتغلب على أنظمة المدن الذكية واختراق المعلومات السرية. ولكن المدن الذكية ما زالت تفتقر إلى القدرات اللازمة لمواجهة الهجمات المتطورة محددة الأهداف، لا سيما تلك التي تستهدف التقنيات الناشئة المستخدمة في البنى التحتية الحسّاسة. ويُعزى ذلك بشكل أساسي إلى افتقار المدن لأنشطة البحث والتطوير التي تركز على التهديدات السيبرانية بشكل استباقي خلال مرحلة تصميم خطة تنفيذ هذه التقنيات الناشئة.

ولكي تكون المدن الذكية قادرة على صد التهديدات السيبرانية، يجب أن تتناقش باستمرار مع الأطراف المعنية فيما يتعلق بالهجمات الإلكترونية التي قد تؤثر على القطاعات المختلفة ودراسة المخاطر والتهديدات الأمنية طوال فترة تطبيق التقنية. ويوضح الجدول التالي[19] ثلاث فئات أساسية من الهجمات السيبرانية التي تتعرض لها المؤسسات والشركات والحكومات وتفرض تحديات أمنية متزايدة باستمرار وبشكل يومي.

%48

من مجالس إدارة الشركات يعتقدون أن شركاتهم ستتعرض إلى حد ما للخسائر الناجمة عن الهجمات الإلكترونية أو عمليات انتهاك البيانات خلال الاثني عشر شهراً القادمة.

%40

من تلك الهجمات ستأتي من المجموعات الإجرامية المنظمة أو " نشطاء القرصنة ".

---

18. إرنست ويونغ – استبيان أمن المعلومات العالمية 2020

19. إرنست ويونغ – الأمن السيبراني المستعاد: الاستعداد لمواجهة الهجمات السيبرانية [استبيان أمن المعلومات العالمية 2018 – 2017]

أنواع الهجمات السيبرانية

	الهجمات الشائعة	الهجمات المتقدمة	الهجمات الناشئة
طبيعة الهجمات	هي الهجمات التي تستغل الثغرات الأمنية المعروفة باستخدام أدوات القرصنة المتاحة مجاناً، ولا تحتاج سوى القليل من الخبرة لتحقيق أهدافها.	هي الهجمات التي تستغل الثغرات الأمنية المعقدة وغير المعروفة أحياناً (الهجمات الفورية) باستخدام أدوات ومنهجيات متطورة.	تركز هذه الهجمات على الفجوات والثغرات الأمنية الجديدة التي تسببها التقنيات الناشئة، وتعتمد على البحث عن هذه الثغرات واستغلالها.
جهة التهديد	المهاجمون الذين لا يمتلكون خبرة، مثل الموظفين الساخطين والمنافسين التجاريين ونشطاء القرصنة وبعض مجموعات الجريمة المنظمة.	المهاجمون الذين لا يمتلكون خبرة، مثل مجموعات الجريمة المنظمة وفرق التجسس والإرهابيين السيبرانيين والدول التي ترعاهم.	المهاجمون الذين يمتلكون الخبرة والإمكانات، مثل مجموعات الجريمة المنظمة وفرق التجسس والإرهابيين السيبرانيين والدول التي ترعاهم.
الأمثلة	• ثغرة أمنية لم يتم إصلاحها على موقع إلكتروني، ويتم استغلالها باستخدام مجموعة أدوات متاحة مجاناً. • البرامج الخبيثة غير المتخصصة التي يتم إدخالها للشبكة من خلال حملات التصيد الاحتيالي، مما يتيح اختراق الشبكة عن بُعد. • هجمات حجب الخدمة الموزعة (DDoS) لتعطيل الخوادم بشكل عشوائي.	• هجمات التصيد الاحتيالي الموجهة مع استخدام برامج خبيثة مخصصة. • استغلال الثغرات الأمنية "الهجمات الفورية" باستخدام برنامج اختراق مخصص. • "زرع" الموظفين المدسوسين للقيام بعمليات استطلاع/تجسس عميقة. • استغلال الموردين/مزودي الخدمات كوسيلة لاختراق البنية التحتية للمدينة الذكية.	• استغلال الثغرات الأمنية في الأجهزة "الذكية" للوصول إلى البيانات و/أو أنظمة التحكم. • الاستفادة من الثغرات الأمنية التي يسببها الاستخدام المزدوج للأجهزة الشخصية وأجهزة المؤسسات في شبكة واحدة. • استخدام التقنيات المتطورة لتجنب عمليات المراقبة والرصد و/أو تجاوز آليات الحماية.

من المهم للمدن الذكية إدراك أن العديد من الهجمات الإلكترونية لا تحدث لتحقيق مكاسب مالية خلافاً للفكرة السائدة. ووفقاً للأمم المتحدة، يعتبر الاتجار بالبشر عبر الإنترنت، والتجسس الرقمي، والهجمات الإلكترونية على البنية التحتية الحسّاسة من أهم جرائم العصر الرقمي التي يرتكبها الأفراد والجماعات في هذا العالم الافتراضي الذي ليس له حدود.

ووقعت هجمات إلكترونية على البنية التحتية الحسّاسة في الماضي، حيث تمكّن المهاجمون من إيقاف سلسلة التوريد ووقف عمليات التصنيع في المدينة بشكل كامل. ويمثل هجوم فيروس الفدية "NotPetya" في أوكرانيا إحدى هذه الهجمات، حيث تعرضت محطة للطاقة النووية لهجوم إلكتروني، وأصيب نظام مراقبة التلوث الإشعاعي في مفاعل تشرنوبل بالبرمجيات الخبيثة، مما أدى إلى استخدام التحكم اليدوي.

في الآونة الأخيرة، أشارت التقارير الى تزايد الهجمات الإلكترونية على البنى التحتية الحسّاسة مثل الكهرباء والغاز وأنظمة إمدادات المياه، ولكن كانت أنظمة الطاقة الكهربائية هي الأكثر تعرضاً لها. يُعزى السبب الرئيسي لهذه الهجمات إلى عدم تطوير أنظمة التحكم الصناعي (ICS) وأنظمة التحكم الإشرافي وجمع البيانات التي يتم استخدامها على نطاق واسع من أجل تحسين كفاءة صيانة الأنظمة وتقليل تكاليف البنية التحتية الحسّاسة. ولكن التقنيات التشغيلية المعقدة تؤدي إلى ارتفاع مستوى المخاطر رغم فوائدها. وتعمل منصات التقنيات التشغيلية كبوابة للهجمات التي تتيح اختراق أنظمة التحكم عبر البرمجيات الخبيثة. وتقوم المدن الذكية بتشغيل البنى التحتية الحسّاسة دون ربط أنظمة التحكم الخاصة بها بالشبكات الخارجية، بما في ذلك الإنترنت، فيما يمثل إجراءً مضاداً للحد من هذه المخاطر.

تؤكد مثل هذه الهجمات الإلكترونية على حاجة المدن الذكية إلى إعادة النظر في استراتيجياتها وآلياتها الدفاعية لمواجهة التهديدات الإلكترونية التي تؤثر على أنظمة التحكم بشكل أفضل. ومن المهم أن تأخذ المدن الذكية في اعتبارها أن الهجوم على البنية التحتية الحسّاسة قد يؤدي إلى عواقب مالية وتشغيلية واجتماعية سلبية للغاية. ولذلك من أجل مواجهة التهديدات والهجمات السيبرانية بشكل أفضل، ينبغي على المدن الذكية اتخاذ مجموعة من الخطوات لتقييم التهديدات السيبرانية وتحديد الجهات المسؤولة عن الهجمات، قبل تنفيذ الإجراءات المضادة.

الإجراءات التي يتعين اتخاذها لمواجهة التهديدات المتطورة

إجراء تقييم استباقي ودوري للمخاطر الإلكترونية

يجب أن تتضمن عملية التقييم الاستباقي الممنهج للمخاطر السيبرانية الظروف المحيطة بهذه المخاطر من خلال التحقق من:

- العمليات التشغيلية والتقنية التي تشمل الإجراءات المنفّذة داخل البنى التحتية الحسّاسة مثل أنظمة الأغذية أو الماء أو الطاقة.
- الأنظمة والتطبيقات المستخدمة لتقديم الخدمات.
- البنية التحتية الأساسية لتقنية المعلومات والمكونات المتصلة بالشبكة والأجهزة المترابطة.
- أنماط مرور البيانات عبر الشبكة والتي توفر رؤية واضحة حول الأنشطة الغريبة التي تنفذها جهات التهديد.
- نشاط المستخدم (اختبارات قابلية التتبع وعمليات تسجيل الدخول إلى النظام).

وضع الخطط وإعداد قدرات الاستجابة للحوادث وتنفيذها

إنشاء خطة الاستجابة لحوادث الأمن السيبراني أو تطويرها:

- توثيق نقاط التصعيد المحدثة وجهات الاتصال المرتبطة بالاستجابة للحوادث.
- تحديد الأنشطة التي يجب تنفيذها بعد اكتشاف عملية الاختراق.
- وضع خطط مفصلة للاستجابة للحوادث تتضمن أدوار ومسؤوليات الجهات المعنية وفريق عمل متعدد المهام.
- إجراء تمارين المحاكاة والتمارين التجريبية عبر البنية التحتية الحسّاسة.
- إنشاء مكتب خصوصية البيانات المسؤول عن جمع البيانات وإدارة الموافقات على جمعها والتعامل مع النزاعات المتعلقة بالبيانات الشخصية.

إجراء عمليات المراقبة الأمنية على مدار الساعة للبنية التحتية للتقنيات التشغيلية وتقنية المعلومات

إجراء المراقبة الأمنية على جميع المستويات:

- يجب على الهيئات المسؤولة عن المدينة الذكية وجميع الجهات الحكومية فهم الموقف الأمني الحالي لبيئة الأمن السيبراني.
- وضع الضوابط الأمنية الدقيقة لجهات استضافة البيانات والشبكات والأجهزة المتصلة بالبنية التحتية للأمن السيبراني.
- تطوير القدرات اللازمة للمراقبة الأمنية لمنظومة الأمن السيبراني على مدار الساعة من خلال استخدام مركز قيادة وتحكم شامل (الذي يساعد في إدارة الأنظمة المادية للأمن السيبراني وتنفيذ مهمات الاستجابة الفورية للتهديدات/الهجمات بكفاءة).

إجراء عمليات المراجعة المستقلة لمنظومة الأمن السيبراني

اعتماد إجراءات وضوابط أمنية أكثر صرامة:

- إجراء عمليات التدقيق الأمني لتغطية جميع مكونات منظومة الأمن السيبراني، بما يتجاوز نطاق التطبيقات والضوابط العامة.
- إجراء مراجعات أمنية تقنية مستقلة وتمارين محاكاة للاختراقات/للهجمات على أساس دوري بمشاركة جميع الأطراف المعنية الذين يقومون بتشغيل البنى التحتية الحسّاسة.
- تحسين عملية جمع بيانات سجل الأمن وتخزينها (على سبيل المثال، تخزين سجلات الأمن السيبراني في خادم منفصل).


Close
Setting
General:
Input latency 100ms
Memory 2048mb
Units Metric
Network:
Workgroup SES-008
Security 256-bit encryption
Firewall enabled
Advsec enabled
IP status Static
Time and Date:
Time zone +2:00
Date Format dd/mm/yy
24h enabled
Time Format 00:00:00
Monitoring Options:
Refresh Rate 100
Sensors Buffer 1024
DATABASE

آراء المشاركين في الدراسة

كثيراً ما يتم تسليط الضوء على أهمية وجود مركز القيادة والتحكم، فما هي القدرات الأساسية التي يجب توافرها في هذا المركز؟

الدكتور/ طه خدرو

شريك في قسم الاستشارات التقنية في شركة "إرنست ويونغ"

رئيس قسم الوجهات والمدن الذكية في شركة "إرنست ويونغ" في منطقة الشرق الأوسط وشمال أفريقيا ومشارك في برنامج "المدن المستقبلية العالمية" التابع لشركة "إرنست ويونغ".

يعتبر وجود مركز القيادة والتحكم الشامل والمتكامل في المدينة الذكية أمراً بالغ الأهمية، كما يجب أن يتضمن القدرات أو العناصر التالية: مركز العمليات الأمنية، والشبكة العاملة، وإدارة الأزمات، وعمليات المدينة (أي جمع البيانات من مختلف الأنظمة والأجهزة وأجهزة الاستشعار، وإدارة الشبكة السيبرانية، وإدارة حالات الطوارئ (الخاملة أو النشطة)، وما إلى ذلك). وتمثل مراكز القيادة والتحكم آلية للاستجابة السريعة بأعلى مستويات الكفاءة في حال حدوث هجمات أو حالات طوارئ، كما توفر قدرات المراقبة الدائمة.

العوامل الرئيسية التي يجب على الحكومات مراعاتها عند تبني منهجية "دمج الحلول الأمنية في تصميم المدن الذكية"

تُستخدم التقنيات الجديدة مثل الذكاء الاصطناعي والتقنيات الحيوية وتعلم الآلة والبيانات الضخمة والحوسبة الكمومية وتقنية الجيل الخامس على نطاق واسع لتوفير الخدمات الذكية لسكان المدن الذكية. وتواصل المدن الذكية استخدام التقنيات الرقمية والحلول المبتكرة بمعدل سريع مع تنفيذ برامج التحول التي تشمل قدراً هائلاً من التقنيات الجديدة. وأدت التطورات التقنية إلى قيام المدن الذكية بتحويل العمليات التناظرية القديمة إلى عمليات رقمية وتحسين أسلوب الحياة بشكل كبير وتعزيز رفاهية السكان والموظفين القائمين على إدارة المدن الذكية.

بدأت المدن الذكية أيضاً استخدام الحوسبة الكمية على نطاق واسع للمساعدة في التحقق من سلامة أجهزة المدن الذكية وزيادة سرعة التحقق من سلامتها، وذلك لأن الحوسبة الكمية تتيح تخزين كميات كبيرة من البيانات بالإضافة إلى سهولة نقلها عبر مختلف الشبكات المترابطة داخل البنية التحتية للمدينة الذكية. وللحوسبة الكمية استخدامات متعددة داخل المدينة الذكية تشمل على سبيل المثال لا الحصر، تحسين حركة المرور داخل المدينة وشبكاتها الكهربائية. وسيحفز ذلك حكومة المدينة الذكية على إعادة التفكير في مناهجها الأمنية إذا استغلها المهاجمون أو استهدفوها.

كما تستخدم بعض المدن الذكية المتقدمة أيضاً أنظمة مترابطة توفر مصدراً واحداً للبيانات المجمعة من أنظمة متعددة، وذلك من أجل تمكين عملية اتخاذ القرار القائمة على البيانات والحصول على رؤى قوية لإدارة البنى التحتية الحساسة. فعلى سبيل المثال، بدأت المدن الذكية في منطقة الشرق الأوسط تنفيذ تقنية "المياه عبر الإنترنت" لربط شبكة توزيع المياه بالكامل باستخدام البنية التحتية المتطورة والمتكاملة لضمان تقليل هدر المياه إلى أدنى حد.

ومع ذلك، يتطلب هذا التكامل والترابط بين الأنظمة المتعددة التعاون على المستوى التنظيمي والإجرائي والتجاري والقانوني والتقني. ومن الضروري للمدن الذكية أن تضمن دمج التقنيات بشكل مناسب في تصميم المدينة وهيكلها في جميع مراحل برنامج التحول أو خلال إنشاء بنية تحتية جديدة.

إضافة إلى ذلك، يجب أن تدرك المدن الذكية أن دمج التقنيات الجديدة والأنظمة المتعددة المترابطة يمثل فرصة سانحة للهجمات التي يقوم بها النشطاء القراصنة والمهاجمين السيبرانيين. ويعود السبب في ذلك إلى قدرة المهاجمين على الوصول إلى نقاط دخول متعددة والتي توجههم في النهاية إلى مصدر واحد للبيانات. ولذلك، يؤدي اختراق نظام واحد إلى الوصول غير المصرح به إلى ملايين السجلات التي تتضمن المعلومات الشخصية مثل الأسماء والعناوين وأرقام الضمان الاجتماعي.

يعتمد إنشاء المدينة الذكية التي تتسم بالكفاءة والفعالية على إمكانية توفير الحلول الشاملة للقطاعات المتعددة ومنصات إنترنت الأشياء التي تركز على المستخدم مع توفير إجراءات إدارية فعالة لعمليات المدينة الذكية.

١١ آراء المشاركين في الدراسة

كيف تستطيع المدن الذكية دمج الحلول الأمنية في مرحلة التصميم عند إدارة البنية التحتية لها؟

مسفر المسفر

مدير إدارة أمن المعلومات في المدينة المعرفية الذكية التي يجري بناؤها في منطقة الشرق الأوسط

دعني أبدأ الحديث بالقول المأثور والذي يعد صحيحاً حتى وقتنا هذا: "درهم وقاية خير من قنطار علاج". يجب اعتبار دمج الحلول الأمنية في تصميم المدن الذكية عنصراً أساسياً في التصميم الشامل للمدينة الذكية وينبغي دمجه في جميع طبقات المدينة الذكية وأنظمتها (مثل النقل الذكي والطاقة الذكية). ويجب على مهندسي ومصممي المدن الذكية في المستقبل بذل عناية فائقة وجهود كبيرة لتحقيقه، حيث ستكون مهمتهم في المستقبل إنشاء بنية تحتية عالية الكفاءة وذات قدرة تشغيلية فائقة يمكن الاعتماد عليها، كما ينبغي أن تمتاز بانخفاض استهلاك الطاقة وقلة الانبعاثات والتلوث، وأن تكون قليلة التكلفة وسهلة الإصلاح وقابلة للتحديث في المستقبل. كما يجب تصميم الشبكات الرئيسية مع الاهتمام الشديد بالشبكات الفرعية التي يمكن تشغيلها في حال توقف الشبكات الرئيسية عن العمل، سواء بسبب الكوارث الطبيعية أو تعطل أحد أجزائها أو هجمات المخترقين أو الإرهابيين التقنيين.

يتناول القسم التالي العوامل الرئيسية التي يجب على الحكومات مراعاتها عند تصميم المدن الذكية. كما يعرض دراسة تفصيلية للعناصر الحسّاسة التي تؤثر على المدن الذكية والجوانب التي تحتاج إلى التعامل معها. وينبغي على الحكومات إدارة هذه العوامل بكفاءة من أجل بناء مدينة ذكية تتسم بالكفاءة والمرونة، كما يجب دمجها في الاستراتيجيات المختلفة التي تضعها الجهات المسؤولة عن إدارة المدن الذكية.

تشمل العوامل الرئيسية التي يجب على الحكومات مراعاتها عند تصميم المدن الذكية ما يلي:

1. التواصل والتعاون
2. البيانات الضخمة وأساليب التحليل التنبؤية
3. بيئة الاختبار
4. الهيكل الأمني
5. انعدام الثقة والتقسيم متناهي الصغر
6. الأمن المادي
7. الشراكة بين القطاعين العام والخاص

العامل الأول

التواصل والتعاون

انطلاقاً من خبرتنا في مناطق أفريقيا والشرق الأوسط، وجدنا أن المدن الذكية ترى وظائف الأمن السيبراني الخاصة بها عالقة في وضع دفاعي، وليست جاهزة بعد لأداء دور محوري في تمكين برنامج التحول.

ويقدم الاستبيان العالمي لأمن المعلومات صورة متشائمة بشأن الواقع الحالي، ويبرز المشكلات الحالية التي تواجهها المؤسسات المتعلقة ببناء علاقات مفيدة مع مختلف القطاعات والإدارات لمواجهة التحديات الأمنية.

---

20. إرنست ويونغ – استبيان أمن المعلومات العالمية 2020

يظهر الاستبيان العالمي لأمن المعلومات أن:

%72 من المؤسسات تشير إلى أن العلاقة بين الأمن السيبراني والتسويق محايدة في أفضل الأحوال، أو تفتقر إلى الثقة أو غير موجودة من الأساس.

%54 منها تشير إلى نفس الأمر فيما يتعلق بفريق البحث والتطوير.

%51 من المؤسسات ترى نفس الأمر بالنسبة لفرق العمل، حتى أن فرق الأمن السيبراني تكون على علاقة سيئة بالفريق المالي الذي تعتمد عليه في الحصول على الميزانية اللازمة لها.

%56 من الشركات تقول إنها متأخرة في برنامج التحول. ويُنظر إلى الأمن السيبراني في هذه الحالة على أنه عقبة أمام مشاريع التحول، وليس عامل تمكين رئيسياً يساعد المدن الذكية على الابتكار بثقة. لذلك من الضروري أثناء تصميم المدن الذكية أن تتواصل الحكومات مع مختلف القطاعات والجهات بانتظام للتعاون معها بشكل وثيق أكثر من ذي قبل.

العامل الثاني

البيانات الضخمة وأساليب التحليل التنبؤية

من المهم أيضاً أن تعيد الحكومات النظر في ممارسات جمع البيانات، نظراً لإمكانات اكتساب الأفكار والرؤى من البيانات المستخلصة من أجهزة استشعار والأجهزة المختلفة التي تعمل داخل المدينة الذكية. وتعتبر إدارة البيانات الضخمة عنصراً مهماً لإدارة البنية التحتية للمدن الذكية، حيث توفر طريقة منظمة لتحليل مجموعات البيانات الكبيرة والمعقدة والتعامل معها. وتستخدم المدن الذكية الممارسات المناسبة لإدارة البيانات مع أساليب التحليل التنبؤية على نطاق واسع، مما يساعدها على تحديد متطلبات العملاء بشكل استباقي، وتمكّنها من اتخاذ القرارات المستقبلية، واستخلاص المعلومات القيمة من أجل تعزيز رفاهية السكان. ونشير هنا بشكل أساسي إلى المدن الذكية المعتمدة على البيانات والتي تستفيد منها في التعامل مع البنية التحتية للمدن الذكية بكفاءة، مثل العدادات الذكية وأنظمة الإنارة الذكية والإدارة الذكية للنفايات.

بفضل تقدم التقنيات الناشئة وتطورها أصبح بالإمكان استخدام تقنية "المياه عبر الإنترنت" للحد من الهدر، إضافة إلى استخدام البيانات بشكل متقن من أجل أتمتة عمليات إدارة المياه. كما تستفيد أنظمة النقل والمواصلات داخل المدينة من البيانات الضخمة لتحسين المسارات والجداول الزمنية وتقليل الازدحام المروري وتعزيز الحفاظ على البيئة. وتساعد عمليات تحليل البيانات الضخمة والبيانات التاريخية في خفض الحوادث، فمن خلال تحليل تاريخ الحوادث، تتعرف السلطات المرورية على أسباب الحوادث ومنعها بشكل عملي. إضافة إلى ذلك، شهدت القطاعات كثيفة الأصول، مثل قطاعي الطاقة والمرافق الخدمية، استخدام البنية التحتية الذكية مثل شبكات الكهرباء الذكية وشبكات المياه الذكية وشبكات الطاقة الذكية. وأتاح النشر السريع للشبكات الذكية تحليل بيانات توليد الطاقة واستهلاكها بصورة فورية. كما يمكن أن يساعد تحليل عادات استهلاك الطاقة لدى السكان والمشاريع الصناعية في التنبؤ بمتطلبات إمدادات الطاقة في المستقبل.

تُجمع البيانات الضخمة من العديد من أنظمة التقنيات التشغيلية وتستخدم لإدارة البنى التحتية الحسّاسة. ويبرز ذلك أهمية تطبيق الحكومات لمستوى كافٍ من الضوابط الأمنية على مخازن المعلومات والبيانات، حيث إن اختراق هذه المخازن أو قواعد البيانات ربما يؤدي إلى أضرار كارثية. وقد تمكّن المخترقون في الماضي من اختراق أنظمة المدن الذكية وقواعد بياناتها، مما أدى إلى توقف البنية التحتية الحسّاسة عن العمل تماماً.

غالباً ما تكمن تحديات استخلاص الأفكار والرؤى المناسبة من البيانات التي جُمعت من أجهزة الاستشعار والأجهزة الأخرى المتصلة بالشبكات داخل المدينة الذكية في البيانات نفسها، وليس في أساليب التحليل وأدواتها، حيث تُخزّن البيانات في أنظمة منفصلة وبتنسيقات وأشكال متنوعة. وتصبح أدوات التحليل غير قادرة على أداء مهمتها على أكمل وجه بسبب افتقار البيانات للتجانس، مما يؤدي إلى توليد معلومات غير دقيقة أو خاطئة تؤثر على عملية صنع القرار. لذلك، يجب أن يراعي تصميم المدينة الذكية إدارة البيانات الضخمة بطريقة سليمة منذ البداية وإنشاء هيكل لتدفق البيانات إلى أدوات التحليل.

إضافة إلى ذلك، يتزايد استخدام المدن للأنظمة المركزية لتخزين البيانات التي يتم جمعها من أنظمة المدينة المتعددة وحفظها في مركز موحد. إلا أن هناك جانب سلبي للربط بين البنية التحتية الافتراضية والمادية في المدينة الذكية يتمثل في زيادة مخاطر الأمن السيبراني. فالمدن الذكية عرضة للعديد من أساليب الهجمات الإلكترونية مثل الهجمات عن بُعد والتشويش على الإشارات والبرمجيات الخبيثة والتلاعب في البيانات وهجمات حجب الخدمة الموزعة (DDoS).

يجب حماية الأجهزة المتصلة بالشبكة باستخدام حلول أمنية شاملة لإنترنت الأشياء. كما يجب استخدام تقنية آمنة للتشغيل، وذلك لمنع القراصنة من استبدال البرمجيات الثابتة بنسخٍ مصابة ببرمجيات خبيثة وبالتالي منع الهجمات السيبرانية.

يجب على القطاعات الغنية بالأصول ضمان التحقق من سلامة الأجهزة الذكية المتصلة بالشبكة قبل استلام البيانات أو إرسالها إليها. وينبغي تقييد إمكانات الأجهزة التي لم يتم التحقق منها على الوصول للبيانات وفحصها قبل توصيلها بشبكة إنترنت الأشياء التي تغذي بشكل عام البنى التحتية الحسّاسة. وفي حال رصد انتهاكات أمنية مثل البرمجيات الخبيثة أو الثغرات الأمنية في الأجهزة المتصلة بالشبكة أو البيانات المرتبطة بها، يجب على إدارة تقنية المعلومات في المدينة الذكية أن تتخذ إجراءات استباقية لقطع اتصال هذه الأجهزة اعتماداً على السلوك الغير طبيعي[21].

---

21. فكرة أساليب التحليلات – المدن الذكية المستقبلية: هي تتم حمايتها ضد التهديدات التي تمس الأمن السيبراني؟

العامل الثالث

بيئة الاختبار

تعتمد المدن الذكية على التقنيات الرقمية وأصول تكنولوجيا المعلومات لتقديم خدمات أكثر كفاءة وفعالية للسكان. وغالباً ما تكون هذه التقنيات والحلول مبتكرة و "جديدة" ولم يتم استخدامها على نطاق واسع من قبل. ولكن في هذه الحالة، لن تكون نقاط الضعف والثغرات الأمنية المرتبطة بالتقنية الثورية الجديدة معروفة بالنسبة لإدارة المدينة الذكية. لذلك يجب على المدن الذكية اختبار أي تقنية جديدة قبل ربطها بشبكات إنترنت الأشياء وتقنية المعلومات والتقنيات التشغيلية. وقد بدأت المدن الذكية في تبني هذا النهج كما حدث في بلدية فايله في مملكة الدانمارك، حيث تعمل بلدية فايله على اختبار التقنيات الجديدة التي يمكن أن تصنع مساحات حضرية أكثر ذكاءً وحفاظاً على البيئة وتوسيع نطاق تطبيقها.[22]

تستخدم المدن الذكية منصات الاختبار لإجراء الفحص الأمني والتشغيلي للأجهزة المتصلة بالشبكة وأجهزة الاستشعار المتصلة بإنترنت الأشياء. فعلى سبيل المثال، تمثل مدينة كيستا للعلوم مختبراً واقعياً لشركة "أربان آي سي تي أرينا" (Urban ICT Arena)، وتتضمن سكاناً ومبانٍ وحركة مرور وظروفاً معيشية حقيقية، إلى جانب منصات اختبار مخصصة. وتم إنشاء البنية التحتية اللازمة للاختبارات، وأصبحت المدينة نموذجاً لفحص أجهزة المدينة الذكية مثل أجهزة الاستشعار والمعدات بصورة مثالية.[23]

ويجب على المدن الذكية والحكومات استخدام هذه المختبرات ومنشآت الاختبار في جميع القطاعات، لا سيما البنى التحتية الحسّاسة، قبل البدء في نشر التقنيات أو الأنظمة أو الأجهزة أو الأصول الجديدة في البنية التحتية للمدينة الذكية. سيساعد ذلك إدارات تقنية المعلومات في تحديد الثغرات الأمنية المحتملة ونقاط الضعف التي ربما تتطلب مستويات أعلى من الضوابط والاشتراطات الأمنية لصد المهاجمين.

---

22. مستكشف الفرص العالمية – اختبار وتوسيع نطاق التقنية الجديدة لإنشاء المدينة الذكية

23. المدينة الذكية السويدية - Urban ICT Arena – منصات الاختبار لإحداث التحول الرقمي في البيئة الحضرية

العامل الرابع

الهيكل الأمني

يجب أن تضع المدن الذكية معايير هيكلية لجميع الأنظمة، بغض النظر عن تصنيف النظام من حيث المخاطر وقطاع العمل. ويجب إنشاء إدارة معنية بالهيكل الأمني تُجري عمليات تقييم للمعايير الموضوعة وتحديثها وإضافة معايير جديدة مع تطور التهديدات والمخاطر، كما يجب أن تقوم بعمليات المراقبة المستمرة للامتثال لهذه المعايير. إضافة إلى ذلك، يجب توفير آليات لنشر تقارير عدم الامتثال علناً، بحيث تقوم المدن برصد حالات عدم الامتثال وإعلانها بصورة فورية.

ويجب إنشاء هيكل المدينة الذكية معتمداً على خمسة مستويات متكاملة [24]

1. هيكل المدينة وما يتضمنه من مباني ومنشآت (الشوارع والمباني)
2. شبكة البنية التحتية وما تحتويه من مرافق أجهزة تقنية
3. جمع البيانات ودمجها
4. منصات تقنية المعلومات التي تعالج بيانات الجهات الخارجية وتجهزها من أجل استخدامها
5. الخدمات المستخلصة من البيانات والتي يتم تقديمها للسكان

يجب أن يكون التكامل بين هذه المستويات والمعايير الأمنية المرتبطة بها على رأس أولويات المدن الذكية. وتعتمد قيمة البيانات والمعلومات التي يتم جمعها عبر القطاعات المختلفة على شبكة البنية التحتية التي ترتبط بمنصات تقنية المعلومات والتطبيقات المستخدمة والاستراتيجية الأمنية الشاملة. يؤدي ذلك في النهاية إلى تقديم أعلى مستويات الخدمات للسكان مع تعزيز كفاءة إدارة البنية التحتية للمدينة.

---

24. إرنست ويونغ – كيف تبدو المدن الذكية في المستقبل؟

العامل الخامس

انعدام الثقة والتقسيم متناهي الصغر

تتبنى المؤسسات والحكومات بشكل عام نموذج انعدام الثقة، وهو مفهوم أمني يتطلب التحقق من جميع المستخدمين (وكذلك العاملين في البنى التحتية الحسّاسة والمؤسسات الحكومية) وفحص وضعهم الأمني بشكل مستمر قبل منحهم إمكانية الدخول إلى الأنظمة والبرمجيات الحسّاسة. وينبغي على المدن الذكية زيادة جهود التدقيق والفحص وتعزيز منهجية انعدام الثقة من خلال تنفيذ الآليات الدفاعية الخاصة بالشبكة. كما يجب على المدن الذكية أن تضيف التقسيم متناهي الصغر إلى ترسانتها الدفاعية الأمنية، نظراً للكم الهائل من الأجهزة المتصلة بالشبكة في المدينة الذكية وعدد الثغرات المحتملة. ويوفر التقسيم متناهي الصغر إمكانية إنشاء حواجز تساعد على احتواء أي تهديد محتمل، أو إيقاف أي هجمات أو عزل أي جهاز مصاب لحماية الخدمات الأخرى[25]. إضافة إلى ذلك، يجب على الحكومات إنشاء مناطق ثقة منفصلة داخل تصميم الشبكة وهيكل الأنظمة المرتبط بالبنى التحتية الحسّاسة، وذلك من أجل ضمان أن تظل التقنيات التشغيلية وأنظمة إنترنت الأشياء المرتبطة عموماً بالبنى التحتية الحسّاسة، مثل شبكات الطاقة والمياه والكهرباء، خاضعة لضوابط أمنية عالية المستوى مقارنة بشبكات تقنية المعلومات العامة.

يجب على مهندسي ومصممي المدن الذكية في المستقبل بذل عناية فائقة وجهود كبيرة لتحقيق منهجية "دمج الحلول الأمنية في تصميم المدن الذكية"، حيث ستكون مهمتهم في المستقبل إنشاء بنية تحتية عالية الكفاءة وذات قدرة تشغيلية فائقة يمكن الاعتماد عليها، كما ينبغي أن تمتاز بانخفاض استهلاك الطاقة وقلة الانبعاثات والتلوث، وأن تكون قليلة التكلفة وسهلة الإصلاح وقابلة للتحديث في المستقبل.

25. IIoT World – استخدام نهج الثقة الصفرية لحماية مشاريعكم للمدن الذكية من القراصنة

العامل السادس

الأمن المادي

يعتبر الأمن المادي لمنشآت معالجة المعلومات ومراكز البيانات في المدينة الذكية أمراً بالغ الأهمية، حيث تحتوي هذه المرافق على البيانات المهمة المستخدمة لتشغيل البنى التحتية للمدينة الذكية.

وتُستخدم كاميرات المراقبة على نطاق واسع في المدن الذكية لأغراض حفظ الأمن وتحديد السلوكيات الغريبة. وربما يكون من الصعب على فرق المراقبة أداء واجباتهم على مدار الساعة بكفاءة بإجراء عمليات المراجعة والمعالجة والتحليل لساعات لا حصر لها من مقاطع الفيديو المسجلة عن طريق مئات - أحياناً آلاف - الكاميرات في المدينة الذكية. ولكن يمكن لأدوات تحليل محتوى الفيديو القائمة على الذكاء الاصطناعي أن توفر معلومات دقيقة بكفاءة عالية، مثل بيانات الأشخاص والأنظمة الحسّاسة وبيانات الاتجاهات العامة لتعزيز الكفاءة التشغيلية.

ينبغي على المدن الذكية أن تجمع بين الذكاء الاصطناعي وأنظمة الأمن المادي، مثل أنظمة قراءة بطاقات الهوية وأنظمة الدوائر التلفزيونية المغلقة. كما يجب أن يكون لحالات السكن المشترك تقسيمات مفصلة تحميها الأنظمة المادية السيبرانية، وأن يتم تتبعها ومراقبتها بشكل مستمر.

العامل السابع

الشراكة بين القطاعين العام والخاص

يُعرّف البنك الدولي الشراكات بين القطاعين العام والخاص بأنها علاقة متوسطة إلى طويلة الأجل بين القطاعين العام والخاص، حيث يلتزم القطاع الخاص بتقديم بعض الخدمات للقطاع العام بموجب اتفاق واضح بشأن الأهداف المشتركة لتقديم خدمات البنية التحتية العامة و/أو الخدمات العامة. ويعتبر توظيف الشراكة بين القطاعين العام والخاص لسد فجوات التمويل والمهارات حلاً محتملاً للتحديات المرتبطة بالبنية التحتية وأنظمتها، وقد أثبت نجاحه في المملكة المتحدة وأستراليا وكندا.[26]

يمكن للقطاع الخاص مساعدة المؤسسات الحكومية ومؤسسات القطاع العام في مواجهة تحديات التحول الحضري السريع. ولذلك ينبغي على الحكومات أثناء تصميم المدينة الذكية دراسة نموذج التعاون مع مؤسسات القطاع الخاص وتحديد منهجية ملائمة للاستفادة من مهاراتها. يمكن إبرام عقود الشراكة الذكية بين القطاعين العام والخاص، بما في ذلك استخدام التقنيات الذكية، لمشاريع المدن الذكية مثل تركيب شبكات أجهزة الاستشعار أو تطوير سياسات البيانات المفتوحة، والحماية من تسرب البيانات، إضافة إلى تحليل التهديدات السيبرانية وتقليلها.

تشير الورقة البحثية الموثقة المستندة إلى ورشة العمل التي أقامتها مؤسسة "يوريا" إلى وجوب مشاركة الحكومات المحلية مع كبرى شركات تقديم الخدمات والشركات التقنية، وكذلك مع الشركات المحلية الصغيرة والمتوسطة الحجم والشركات الناشئة. وربما تتضمن الشراكات الذكية بين القطاعين العام والخاص إجراء إصلاحات شاملة للتشريعات وإجراءات توفير الخدمات. وهناك مجموعة كبيرة من الاتفاقات القانونية المتوفرة للأطراف المختلفة لإقامة الشراكات من أجل تنفيذ المدن الذكية الآمنة بصورة أفضل.

---

26. إرنست ويونغ – هل مدينتكم ذكية مثلما هم سكانها؟
27. مايكروسوفت – بناء وكالة وطنية فعالة للأمن السيبراني ٢

دور الحكومات في الأمن السيبراني

تؤدي الحكومات دوراً محورياً في مدن المستقبل من خلال توفير المنتجات والخدمات الذكية وتطوير الاقتصاد الرقمي. ويجب على الحكومات تشجيع وتحفيز الشركات الخاصة على المشاركة من أجل توفير البنية التحتية اللازمة، وتدريب العاملين في القطاع الرقمي، وتمكين الوصول الآمن للخدمات الرقمية.[28]

تشكّل البنية التحتية التي تضم الأجهزة والأنظمة المترابطة أساساً لأي رحلة تحول رقمي. ويجب تطوير البنية التحتية باستمرار، بما يتماشى مع التقنيات التي تعتمدها المدن الذكية وتنفذها. ومع ذلك، فإن مجرد تحديث البنية التحتية لاستيعاب التقنيات الثورية لن يؤدي إلا إلى نشوء عدد كبير من التحديات الأمنية. ولذلك يجب أن يكون هدف الحكومات هو بناء بنية تحتية آمنة يمكن الاعتماد عليها وتتمتع بضوابط واشتراطات أمنية كافية لحماية أصول المدينة الذكية.

شهدت الفترات الأخيرة اتجاهاً في تعيين الحكومات لهيئة مركزية موثوقة تتمتع بصلاحية تحديد إرشادات وتوجيهات الأمن السيبراني وإنفاذها وتنظيمها على مستوى المدينة الذكية أو مستوى الدولة. وتعتمد الحكومات في كثير من الأحيان على هيئة مركزية اتحادية. وهناك اعتقاد شائع بأن وكالة الأمن السيبراني الوطنية المستقلة يمكن أن تعزز كثيراً من قوة منظومة الأمن السيبراني في الدولة إذا تم إنشاؤها بشكل مناسب. إضافة إلى ذلك، يمكن للحكومات تحديد أولويات خاصة بمواردها المحدودة من خلال دمج مهام تنسيق الأمن السيبراني الأساسية على المستوى الوطني، ووضع المعايير، والاستجابة للحوادث، وعقد الشراكات والتعاون مع إحدى الوكالات المركزية الدولية.[29]

ويجب على هذه الوكالات المركزية والجهات والإدارات الأخرى على مستوى القطاعات المشاركة في الأمن السيبراني أن تتفهم التهديدات، وأن تتبنى آليات الدفاع المناسبة لحماية المدينة من المتسللين، وتنفيذ الضوابط الأمنية لحماية المعلومات الشخصية من مجرمي الإنترنت، مع الحفاظ على خصوصية البيانات والاستفادة منها ضوابط الأمن والسلامة في تصميم المدينة الذكية.

نستعرض فيما يلي رؤية تفصيلية للمحاور الرئيسية التي يجب أخذها في الحسبان عند إعداد برنامج الأمن السيبراني ضمن منظومة المدينة الذكية.

---

28. إرنست ويونغ – كيف نبني الدولة الرقمية

29. مايكروسوفت – بناء كلية وطنية فعالة للأمن السيبراني

المحور الأول

حماية البنية التحتية للمدينة الذكية من المخترقين

تصبح المدن أكثر ذكاءً وتتطوراً لاتخاذ القرار الصائب من خلال تعزيز الاستفادة من بيانات أنظمة تقنية المعلومات والاتصالات وأجهزة الاستشعار والأجهزة والأصول الأخرى المتصلة بشبكة المدينة الذكية. ومع ذلك، تحتاج الحكومات إلى إعادة التفكير في استراتيجياتها ووضع الأمن السيبراني على رأس أولوياتها، حيث يؤدي انتشار هذه الأجهزة إلى عدد من الثغرات المتاحة للمهاجمين السيبرانيين ويفرض التهديدات على المدينة الذكية. كما يجب النظر إلى الأمن السيبراني من منظور أوسع، لمنع المتسللين من اختراق البنية التحتية وأنظمة المدينة الذكية.

توصيات مقدمة للحكومات

يجب أن تفهم الحكومات، باعتبارها منظمات مجتمعية، التكامل المعقد للبنية التحتية وأنظمة النقل وشبكات المرافق واستخدام الأراضي والتركيبة السكانية، وذلك لتحديد الدور الذي يتعين عليها القيام به في توجيه عملية التحول وتعزيز التعاون بشكل أفضل. ويساعد وجود وكالة مركزية للأمن السيبراني على مستوى المدينة في التخفيف من هذا التحدي بشكل كبير، ويعمل على توفير بيئة تحفز تقديم الأفكار ومناقشتها وتنفيذها من خلال التعاون على مستوى المدينة. وبناءً على تجاربنا وخبراتنا، قدّمنا منهجاً شاملاً للأمن السيبراني، وساعد عملنا كفريق مشترك مع مؤسسة القمة العالمية للحكومات على تعزيز فهم العوامل المحركة لتبني إجراءات الأمن والامتثال لها في المدن الذكية في جميع أنحاء العالم بشكل أفضل.

المحور الثاني

وضع الاستراتيجية الأمنية القائمة على المخاطر والتي تتناسب مع أهداف المدينة الذكية

هناك إجماع متزايد على أن الحكومات عادةً ما تخفق في دمج الأمن السيبراني في جميع العمليات، بدءاً من مرحلة وضع الاستراتيجية وصولاً إلى مرحلة التصميم. يرجع السبب في ذلك إلى التدرج الهرمي الروتيني والبيروقراطية والافتقار إلى تحديد أدوار الجهات والوكالات الحكومية على مستوى القطاع. سيساعد وضع الاستراتيجية الأمنية التي تتناسب مع أهداف المدينة الذكية في تحديد التوجه الاستراتيجي للجهات المختلفة المشاركة في ضمان تنفيذ سياسات الأمن السيبراني وبرامج الأمن الشامل من خلال عملية اتخاذ القرارات الدقيقة والمنظمة.

توصيات مقدمة للحكومات

يجب على الحكومات ترسيخ الركائز الأساسية لاستراتيجية الأمن السيبراني التي ستمكنها من تحقيق النتائج المرجوة ورسم خارطة طريق لتعزيز الموقف الأمني. ويجب أن تأخذ الاستراتيجية وخارطة الطريق في الاعتبار متطلبات جميع القطاعات، كما ينبغي منح الأولوية لحماية البنية التحتية الحسّاسة. إضافة إلى ذلك، يجب أن تكون الاستراتيجية قائمة على المخاطر وملائمة لتمكين القطاعات من ابتكار التقنيات الثورية وتنفيذها دون المساس بأمن البنية التحتية الحالية.

المحور الثالث

تطوير السياسات والإرشادات التوجيهية والمعايير الرسمية وتنفيذها على مستوى المدينة

تعتبر مجموعة السياسات والإرشادات والمعايير الأمنية الرسمية عنصراً أساسياً لأنها توثّق العمليات الموحدة التي يجب أن تتبعها الجهات في جميع القطاعات. كما توفر وسيلة لدمج الأمن في جميع العمليات الحيوية، وتتميز بأهمية كبيرة بالنسبة لأمن الخدمات الذكية التي تقدمها الحكومات.

توصيات مقدمة للحكومات

يجب على الحكومات تحديد الإرشادات التوجيهية الأمنية على مستوى المدينة والتأكد من تطبيقها من خلال وكالة مركزية للأمن السيبراني. ويجب على الحكومات عند تطبيق هذه السياسات فهم المخاطر أو الأنشطة المحددة داخل القطاعات، بحيث تتيح للجهات داخل كل قطاع تخصيص و/أو إضافة ضوابط أمنية محددة ضمن السياسات والمعايير الأمنية وفقاً لطبيعة التهديدات الموجودة (التهديدات التي يتم التدرب على مواجهتها) وتلبية الاحتياجات المحددة للتقنية المعنية.

المحور الرابع

وضع الهيكل الأمني محدد السياق الذي يتوافق مع متطلبات جميع الجهات المعنية

يمكن استخدام هيكل أمني محدد بدقة لإدارة حلول أمن المعلومات والتقنيات التي تعزز قابلية التشغيل المتبادل والمرونة، مع تلبية متطلبات إدارة المخاطر في المدينة الذكية.

توصيات مقدمة للحكومات

يجب على الحكومات تحديد هيكل أمني يتضمن: وصف هيكلي، ووظائف الأمن المحددة (مع الضوابط الأمنية)، والمعلومات المتعلقة بأمن واجهات الأنظمة الخارجية، والمعلومات التي يجري توفيرها عبر هذه الواجهات، وآليات الحماية المرتبطة بكل واجهة، ودمج الأمن السيبراني في جميع تطبيقات التقنيات والمشاريع التي يتم تنفيذها على مستوى المدينة أو القطاعات.

المحور الخامس

اتباع منهج شامل لإدارة الأصول والحفاظ على مخزون الأصول المركزية

تستخدم المدن الذكية مجموعة متنوعة من أصول البنى التحتية الحسّاسة، والتي تشمل البنية التحتية للتقنيات التشغيلية وإنترنت الأشياء. وتعتبر إدارة الأصول تحدياً كبيراً يجب التعامل معه في المراحل الأولى لبناء المدينة الذكية.

توصيات مقدمة للحكومات

لمواجهة هذا التحدي، يجب على الحكومات تشجيع القطاعات على إنشاء بيان مركزي مفصّل للأصول مع أتمتة تحديث هذا البيان (حيثما كان ذلك ممكناً). ويساعد ذلك المدن الذكية في تتبع المشكلات وتحليلها، مثل الموقع الفعلي ومتطلبات الصيانة والإهلاك وقياس الأداء والتخلص من الأصول بصورة نهائية. وتجدر الإشارة إلى أن أصول التقنيات التشغيلية أو إنترنت الأشياء (مثل أجهزة الاستشعار وأجهزة الكشف) ربما تحتاج إلى منهج أكثر تفصيلاً من أصول تقنية المعلومات. كما يجب تصنيف الأصول الموجودة في البيان المفصّل، وينبغي على الحكومات استثمار قدر كبير من الوقت في تحديد الأصول ذات القيمة العالية من أجل منحها الأولوية الأمنية وتخصيص آليات الحماية لها.

المحور السادس

تبني نهج شامل للتحكم في إمكانية دخول المستخدمين للشبكة وإدارة صلاحيات المستخدمين

ربطت المؤسسات التي تمثل بنية تحتية حسّاسة أنظمة تقنية المعلومات مع أنظمة الإنتاج وبيئات التقنيات التشغيلية التي كانت منفصلة في السابق. وأدى ربط أنظمة التحكم الصناعي وأنظمة التحكم الإشرافي وجمع البيانات وأنظمة التقنيات التشغيلية الأخرى بشبكات الشركات إلى ظهور المخاطر الخاصة بأنظمة تقنية المعلومات في أنظمة التقنيات التشغيلية، والتي تتضمن اختراق نقاط الوصول. وتعتبر نقاط الوصول هذه بوابة لأنظمة الإنتاج الحسّاسة في المدينة، والتي تتحكم في إنتاج الكهرباء والمياه والغاز وتوزيعها، والخدمات الحيوية الأخرى التي تقدمها المدينة الذكية للسكان.

توصيات مقدمة للحكومات

يجب على الحكومات استخدام حلول إدارة صلاحيات الهوية لحماية البنية التحتية الحسّاسة (PIM/CIP) التي يوفرها العديد من شركات تقديم الخدمات، وذلك لإدارة صلاحيات الدخول لأنظمة البنية التحتية الحسّاسة. كما يجب أن تُخصص صلاحيات الدخول الممنوحة للمستخدمين بما يتماشى مع معيار الجودة ISO/IEC 27002:2013 على أساس الحاجة إلى الاستخدام وعلى أساس كل حدث على حدة، وبما يتوافق مع سياسات التحكم بالوصول للأنظمة. كما يجب التحكم في تخصيص صلاحيات الدخول للأنظمة المستخدمة لتشغيل البنى التحتية الحسّاسة من خلال عملية رسمية لإصدار صلاحيات المستخدمين طبقاً لسياسات التحكم بالوصول.

المحور السابع

إدارة العلاقات مع الجهات الخارجية باستخدام منهجية قائمة على المخاطر

توصي منهجية إدارة المخاطر السيبرانية لسلسلة الإمداد (C-SCRM) التابعة للمعهد الوطني للمعايير والتقنية (NIST) المؤسسات بإعداد برنامج متكامل لتقييم المخاطر السيبرانية للجهات الخارجية من خلال توضيح مجالات التعاون بين جميع الوحدات الوظيفية والإدارات والقطاعات.

توصيات مقدمة للحكومات

يجب على المدن الذكية إنشاء آلية مركزية لإدارة المخاطر السيبرانية للجهات الخارجية تعتمد على منهجية قائمة على المخاطر، وذلك نظراً لصعوبة فحص كل علاقة مع جهة خارجية بشكل مفصّل، وبالتالي إدارة العلاقات ذات المخاطر المرتفعة بشكل مركزي على مستوى المدينة، في حين يمكن لجهات محددة على مستوى القطاع دراسة العلاقات ذات المخاطر المنخفضة.

المحور الثامن

تحسين الوعي الأمني باستخدام منهجية متكاملة تتضمن مشاركة القطاعين العام والخاص

غالباً ما يستطيع مرتكبو الجرائم السيبرانية اختراق أنظمة البنية التحتية الحسّاسة من خلال استهداف الموظفين العاملين في هذه الأماكن. ويتعرض السكان للاستهداف من المجرمين الذين ينتحلون شخصيات هؤلاء الموظفين بصورة متكررة، ويُجبرونهم على الإفصاح عن المعلومات الشخصية بذريعة الاستخدام الحكومي. وبالتالي، يجب على المدن الذكية بناء جدار حماية بشري يدرك ماهية التهديدات السيبرانية من خلال برامج التدريب والتوعية الصارمة والمستمرة للسكان.

توصيات مقدمة للحكومات

يجب على الحكومات التركيز على جمع الأفكار والموارد ونقاط القوة من جميع القطاعات في مكان واحد، ونوصي أن تتبنى المدن الذكية منهجية مشابهة للمنهجية التي تطبقها سنغافورة، حيث عمدت هيئة تطوير الاتصالات المعلوماتية (IDA) بالتعاون

من شركائها أصحاب التوجهات المشابهة من القطاعين العام والخاص إلى تشكيل اتحاد الوعي الأمني السيبراني في عام 2008. ويتيح تبني هذا النموذج للمدن الذكية ضمان أخذ متطلبات جميع القطاعات في الحسبان، والتأكد من تغطية برامج التوعية لجميع التهديدات أو المواضيع التي تؤثر على المدينة. وتساعد إقامة حملات التوعية عن طريق هذه الاتحادات، بمشاركة ممثلين عن مجموعات السكان، في إقناع السكان بأهمية هذه البرامج، حيث سيشعر السكان بثقة أكبر تجاه الإجراءات الجاري اتخاذها وسيشاركون بنشاط في حملات التوعية.

المحور التاسع

إجراء عمليات لامركزية لتقييم المخاطر مع توحيد المخاطر المحددة على مستوى المدينة

تعتبر تقييمات المخاطر السيبرانية عنصراً جوهرياً في جميع أنواع العمليات التشغيلية، فهي تكشف الجوانب الحسّاسة المعرضة للمخاطر، وتحدد مستوى الضوابط الأمنية اللازمة لكل جانب. وتساعد عمليات تقييم المخاطر في تحديد الجوانب التي يجب تحسينها والضوابط الأمنية التي تحتاج للتطوير.

توصيات مقدمة للحكومات

يجب على المدن الذكية إجراء عمليات تقييم دورية للمخاطر السيبرانية في البيئات المستهدفة (مثل بيئات الأعمال الحسّاسة، والعمليات والبنية التحتية التقنية الداعمة). ولكن تجدر الإشارة إلى أن الاعتماد على القطاعين العام والخاص لإجراء عمليات تقييم المخاطر الخاصة بكل قطاع لا يخلو من بعض السلبيات، مثل الافتقار إلى المنهجية الموحّدة. وبالتالي يجب على المدن الذكية الاستفادة من الممارسات التي طبقتها الدول الأخرى لتحقيق التوازن بين المنهجية المركزية والاتحادية في تقييم المخاطر. فعلى سبيل المثال، صمم المكتب السويسري للحماية المدنية مجموعة أدوات تتماشى مع الاستراتيجية الوطنية للحماية ضد المخاطر السيبرانية في سويسرا، وذلك للتغلب على هذا التحدي وإجراء عمليات تقييم المخاطر وفق منهج موحد. وعلى هذا النحو، يمكن للمدن الذكية التفكير في إعداد إطار موحد لتقييم المخاطر يحدد ضوابط هيكل برامج التقييم ويعممها على جميع القطاعات والمؤسسات الخاصة والإدارات. وبينما نتوقع أن تكون عمليات تقييم المخاطر إلزامية وأن تُنفذ على فترات زمنية محددة مسبقاً، من المهم جداً للوكالة الأمنية المركزية تحديد المخاطر على مستوى المدينة والإجراءات الإضافية التي يجب اتخاذها. وينبغي أن تعتمد هذه الإجراءات على دراسة مفصّلة وتحليل متعمق لبيانات المخاطر التي جمعتها القطاعات المختلفة.

المحور العاشر

تعزيز الاستجابة للحوادث على مدار الساعة من خلال تأسيس مركز العمليات الأمنية على مستوى والمدينة القطاعات

من الضروري أن تشكّل المدينة الذكية فريقاً محلياً مخصّصاً للاستجابة للطوارئ الحاسوبية (CERT) أو فريقاً للاستجابة لحوادث الأمن الحاسوبية (CSIRT) الخاصة بها، بهدف تقليل الاعتماد على الفرق المماثلة على المستوى الوطني، مما يساهم في الاستجابة للحوادث التي تواجهها المدينة بصورة كافية وفورية.

توصيات مقدمة للحكومات

يجب على قطاعات المدينة الذكية تأسيس فريق محلي مخصّص للاستجابة للطوارئ الحاسوبية (CERT) أو فريق الاستجابة لحوادث الأمن الحاسوبية (CSIRT) طالما سمحت ميزانية المدينة بذلك، وتتعزز قدرة فريق الاستجابة للطوارئ الحاسوبية المخصص لكل قطاع على الاستجابة الفورية بفضل إمكانية الاستفادة من الخبرات التشغيلية للقطاع ومعرفته العميقة بمتطلباته. ويساهم هذا الأمر في تخفيف الاعتماد على فريق الاستجابة للطوارئ الحاسوبية الخاص بالمدينة ويضمن تركيز هذا الفريق على الحوادث الكبيرة التي تتجاوز عتبة محددة (والتي تتحدد بالتنسيق والتعاون مع الجهات الحكومية والقطاعات الأخرى). كما يجب على المدن الذكية إلزام الجهات الخارجية ومقدمي خدمات البنية التحتية بالإبلاغ عن الحوادث بصورة فورية. على سبيل المثال، أصدرت الحكومة الإسبانية مرسوماً يُلزم مشغلي الخدمات الأساسية (مثل البنية التحتية الحسّاسة) ومزودي الخدمات الرقمية بالإبلاغ عن الحوادث التي يتعرضون لها في الخدمات الشبكية والمعلوماتية ضمن فترة زمنية محددة.

المحور الحادي عشر

تعزيز القدرات الخاصة بإجراء التحليل الجنائي والكشف الإلكتروني عن الأدلة

في ظل التهديدات الحالية، لن يمر وقت طويل قبل أن يتمكن مرتكبو الجرائم السيبرانية من الوصول إلى البنية التحتية والتمكّن من سرقة المعلومات السرية أو إصابتها بالملفات الخبيثة أو التحكم بالأنظمة الحسّاسة بغرض طلب فدية. وفي هذه الحالة، تحتاج الحكومات إلى إجراء عمليات التحليل الجنائي الرقمي ومعالجة الأدلة وتقديمها إلى جهات إنفاذ القانون.

توصيات مقدمة للحكومات

قامت الغالبية العظمى من الدول الأعلى تصنيفاً ضمن مؤشر الأمن السيبراني الوطني، مثل اليونان وإستونيا، بتأسيس وحدات مخصصة للتحاليل الجنائية الرقمية لتمكين المدن الذكية من تحديد عمليات الاختراق أو هجمات المتسللين، وجمع الأدلة من الحوادث المعروفة والحصول على البيانات لتحليل وتحديد المصدر وأسلوب الهجوم والهدف منه وتأثيره. ويجب تجهيز وحدات الأدلة الجنائية الرقمية بمختبرات التحليل الجنائي ومجموعة أدوات التحليل الجنائي الرقمي التي تساعدها على أداء مهامها بدقة وفي الوقت المناسب.

المحور الثاني عشر

حماية البيانات الشخصية من خلال تبنّي منهجية دمج الحلول الأمنية في تصميم المدن الذكية

تعد الخصوصية من حقوق الإنسان الأساسية التي تحميها القوانين الوطنية بطرق مختلفة. وعلى الرغم من الفائدة الكبيرة لهذه المعلومات بالنسبة لمؤسسات تحليل البيانات والجهات الحكومية التي تقدّم أفضل الخدمات، إلا أن استخدام البيانات للحصول على الأموال يسبب مشاكل في الخصوصية. وتدرك الجهات التنظيمية أهمية بيانات الخصوصية وتعمل على تطبيق وتنفيذ العديد من متطلبات الحماية والخصوصية، ولكن المدن الذكية تواجه في الوقت الحاضر تحديات في جمع البيانات الشخصية والإفصاح عنها وإدارة الموافقات على استخدامها، وذلك بسبب غياب العمليات الواضحة والفهم العام للمتطلبات التنظيمية التي تؤدي إلى تعقيدات معينة أثناء الامتثال لها.

توصيات مقدمة للحكومات

يجب على الحكومات تخزين البيانات ضمن بنية تحتية آمنة لتقنية المعلومات لتقليل احتمال انتهاك خصوصية أصحابها، وتفرض قيوداً على جمع المعلومات الشخصية بالحد الأدنى من جهة، والاحتفاظ بها لأقصر فترة زمنية ممكنة من جهة أخرى. وتمثل استخدامات بيانات التتبع وآثارها المترتبة على الخصوصية التي أحدثتها المراقبة والمتابعة الجماعية أحد العوامل الرئيسية التي لا ينبغي التغاضي عنها في برنامج الخصوصية. كشفت نتائج الاستبيان العالمي لخصوصية المستهلكين الذي أجرته "إرنست ويونغ" في العام 2020 أن تفشي جائحة كوفيد-19 زاد من استعداد المستهلكين لمشاركة بياناتهم الشخصية من أجل الصالح العام، إلا أن الثقة ما زالت مشكلة كبيرة، حيث يرى ما يقارب نصف المستهلكين على مستوى العالم (47٪) أن حكوماتهم ستستخدم هذه البيانات في أغراض تتجاوز الأغراض المعلن عنها. وفي سبيل التعامل مع هذا التحدي المرتبط بالخصوصية وحماية المعلومات الشخصية، نوصي باعتماد منهجية "دمج حلول الخصوصية في تصميم المدن الذكية" التي تدمج حلول الخصوصية ضمن أي نظام أو منتج أو جهاز جديد طوال فترة استخدامه، بدءاً من مرحلة التصميم ووصولاً إلى مرحلة التنفيذ. إضافة إلى ذلك، من الضروري إنشاء مكتب لخصوصية البيانات على مستوى المدينة الذكية لإدارة البرنامج الشامل لخصوصية البيانات وحمايتها.

---

30. إرنست ويونغ – استبيان خصوصية المستهلكين العالميين 2020

البنية التحتية الآمنة

يجب أن تهدف الحكومات إلى تطوير بنية تحتية آمنة وموثوقة تتمتع بضوابط وعمليات أمنية كافية لحماية أصول المدينة الذكية.

تشكل البنية التحتية التي تتضمن الأنظمة والأجهزة المتصلة عاملاً أساسياً لعملية التحول الرقمي، ويجب أن تخضع هذه البنية التحتية للتطوير المستمر تماشياً مع التقنيات الجديدة التي يتم استخدامها باستمرار.

١١ آراء المشاركين في الدراسة

ما هي الإجراءات الرئيسية التي يجب اتخاذها لحماية المعلومات الشخصية للسكان؟

مسفر المسفر

مدير إدارة أمن المعلومات في المدينة المعرفية الذكية التي يجري بناؤها في منطقة الشرق الأوسط

1. **وضع قانون لحماية البيانات:**
يجب على المدن الذكية إنشاء رابطة لحماية البيانات والتشاور مع الخبراء القانونيين أو خبراء أمن تقنية المعلومات لإعداد مستند رسمي يوضّح المبادئ التي يجب اتباعها في عملية جمع المعلومات وأسباب الاحتفاظ بها.

2. **حماية البيانات المادية والرقمية:**
يجب على المدن الذكية تطبيق إجراءات حازمة لحماية البيانات المادية والرقمية من السرقة أو سوء الاستخدام. وفي حال تخزين البيانات ضمن أجهزة غير متصلة أو في مكان مادي وأُغلقت عليها الأبواب والأدراج، يجب استخدام أنظمة المراقبة لتأمينها، وحماية الأجهزة المتنقلة التي تتضمن البيانات الحسّاسة.

3. **الحصول على الموافقات الصريحة:**
يجب أن تنص قوانين حماية البيانات على ضرورة الحصول على موافقة مسبقة قبل تسجيل أي بيانات شخصية، ويجب على المدن الذكية استخدام نماذج الموافقات التي تتيح الحصول على موافقة الشخص الذي تُجمع بياناته.

الخاتمة

يفرض التحول الحضري ومتطلبات السكان المتزايدة ضغوطات كبيرة على البنية التحتية في المدن التي تعتمد بصورة متزايدة على التقنيات والخدمات المبتكرة لتقديم النتائج المرجوة منها وتعزيز قدرة الموظفين على توفير بيئة آمنة ومضمونة. ولكن الهجمات السيبرانية في ازدياد، ويبدو أن المهاجمين يستخدمون أساليب متطورة في قرصنة الأنظمة الحسّاسة والتأثير سلباً على البنية التحتية للمدينة. ولذلك نشجع الحكومات على تبني منهجية متعددة المستويات للاستجابة للهجمات السيبرانية وصدّ الهجمات الأكثر شيوعاً باتباع منهجية مخصصة للتهديدات الناشئة والمتطورة.

يجب ألا تهتم المدينة الذكية بأمن تقنية المعلومات والتقنيات التشغيلية فحسب، بل يجب أن تتعامل مع التعقيدات الإضافية التي يفرضها إنترنت الأشياء، من أجل حماية المعلومات الحسّاسة. فضلاً عن ذلك، يجب على المدن الذكية الاستفادة من تطور بيئة الأعمال الرقمية المبتكرة مثل الأتمتة باستخدام الروبوتات وتقنية "بلوك تشين" والذكاء الاصطناعي. ويفرض انتشار الأجهزة الجديدة المتصلة بالإنترنت والأفكار المبتكرة مثل السيارات الطائرة والسيارات المتصلة بالإنترنت والهيدروجين الأخضر والحوسبة السحابية، اتباع منهجية "دمج الحلول الأمنية في تصميم المدن الذكية"، فهذه التقنيات جديدة ولم يتم تحديد متطلباتها الأمنية بعد.

تحتاج المدن الذكية إلى منهجية متطورة للتعامل مع الهجمات السيبرانية والتحلي بالمرونة لصد التهديدات السيبرانية التي لا تتوقف عن التطور.[31]

---

31. إرنست ويونغ – الأمن السيبراني المستعاد: الاستعداد لمواجهة الهجمات السيبرانية [استبيان أمن المعلومات العالمية 2018 – 2017]

أنواع الهجمات السيبرانية

الهجمات الشائعة

يستلزم صد الهجمات الشائعة تطبيق الحلول التقنية مثل برمجيات مكافحة الفيروسات وكشف الدخلاء وأنظمة الحماية (أنظمة كشف المتسللين (IDS) وأنظمة منع الاختراق (IPS))، كما يتطلب تحديثاً مستمراً لعمليات إدارة البيانات وتقنيات تشفيرها لحمايتها، حتى وإن لم يتمكن المهاجم من الوصول إليها. ومن الضروري لأي مدينة ذكية أن تعمل على تعزيز وعي السكان بالأمن السيبراني بسبب احتمال تعرضهم للهجمات السيبرانية التي تستغل نقاط الضعف (مثل تطبيقات الهاتف المتحرك) التي يستهدفها المهاجمون بصورة متكررة.

الهجمات المتقدمة

يتطلب صد الهجمات المتقدمة وجود مؤسسات مثل مراكز العمليات الأمنية (SOCs) ومراكز عمليات الشبكة (NOCs) التي تتمتع بقدرات التنسيق والتعاون والرقابة الشاملة على عمليات البنية التحتية الحسّاسة. ويشير التوجه الحالي لمراكز العمليات الأمنية على مستوى الحكومات إلى تبنيها برنامجاً دفاعياً نشطاً تعمل فيه شركات البنية التحتية الحسّاسة على مشاركة معلومات التهديدات وتحليلها بصورة فورية من أجل إصدار التنبيهات الأمنية والاستجابة لها بطريقة منسقة.

الهجمات الناشئة

يتطلب صد الهجمات الناشئة، مثل ظهور التهديدات المادية-السيبرانية، اليقين بأن بعض التهديدات لن تكون معروفة. ويجب على القائمين على إدارة المدن الذكية والحكومات حول العالم إعداد نظم حوكمة مرنة ضمن برامج الأمن السيبراني لضمان تخفيف الهجمات الناشئة والاستجابة لها بطريقة فعالة وفي الوقت المناسب. ويمكن للمدن الذكية التي تستخدم أطر الحوكمة المرنة كأساس لبرنامج الأمن السيبراني أن تتبع منهجية "دمج الحلول الأمنية في تصميم المدن الذكية"، وتطبيق الأنظمة والعمليات القادرة على الاستجابة للمخاطر غير المتوقعة والناشئة. إضافة لذلك، يوفر استخدام تقنيات الخداع (مثل المصائد الأمنية التي تسمى مصائد العسل "Honeypots") وبرامج المكافأة على اكتشاف الثغرات الأمنية "bounty-bug" (أي البرامج التي تشجع الباحثين الأمنيين على اكتشاف الثغرات الأمنية في أنظمة البنية التحتية الحسّاسة) فوائد كبيرة ويجب تضمينها في برامج الأمن السيبراني.

تسعى الحكومات والبلديات حول العالم بلا كلل من أجل مواجهة رسائل البريد الإلكتروني غير المرغوب فيها خلال تفشي جائحة كوفيد-19 والتي تستطيع تجاوز التقنيات الأمنية التقليدية للبريد الإلكتروني . فالخوف المتصاعد من فيروس كورونا يجعل المستخدمين عرضة للوقوع في فخ هذا النوع من الرسائل الإلكترونية في محاولتهم للحصول على معلومات جديدة حول عدد الإصابات والبضائع والخدمات والمرافق الطبية وغيرها. ويستغل المهاجمون هذا الوضع السائد على نطاق واسع لاستهداف المستخدمين البسطاء واستدراجهم لإفشاء المعلومات السرية (مثل اسم المستخدم وكلمة المرور). ويجب على الحكومات مراقبة هذه البيئة باستمرار وتعزيز ثقافة الأمن السيبراني في منظومة المدينة الذكية التي تضم المؤسسات الحكومية والبنية التحتية الحسّاسة وشركات الاتصالات والقطاع الخاص والسكان، إلى جانب التقنيات المبتكرة القادرة على صد هؤلاء المجرمين.

وينبغي على الحكومات تقييم الممارسات الأمنية الجيدة الواردة في هذه الورقة البحثية، وتطويرها وتعزيز أفكار الحلول المقترحة. ويمكن للحكومات إبرام شراكات بين القطاعين العام والخاص من أجل تنفيذ مشاريع المدينة الذكية في جميع القطاعات وإدارتها، وذلك للاستفادة من خبرة القطاع الخاص، والتواصل بانتظام مع مجموعات السكان لفهم متطلباتهم وتحديد الطرق المثلى لتقديم الخدمات الذكية والمبتكرة القادرة على حل المشاكل الاجتماعية والارتقاء بأسلوب الحياة. إضافة لذلك، يعتبر التعاون مع لجان القطاعات ومجموعات السكان وشركات الاتصالات والمنتديات المعنية بهذا المجال والجهات المسؤولة عن جمع معلومات التهديدات من جهة، وتوفير أطر مرنة للحوكمة من جهة ثانية، أحد عوامل التمكين الرئيسية للتعامل مع مخاطر الأمن السيبراني ومشاكله على المدى الطويل.

.

---

32. إرنست ويونغ – سبعة طرق لتجاوز المهاجمين السيبرانيين أثناء تفشي كوفيد-

نبذة

عن الشركاء

سامر عمر

مدير أول في إرنست ويونغ

البريد الإلكتروني: samer.m.omar@ae.ey.com

المشاركين في الورقة البحثية

ريتيش جوتو

شريك ورئيس قطاع الأمن السيبراني في إرنست ويونغ أفريقيا

البريد الإلكتروني: ritesh.guttoo1@mu.ey.com

سيديش مودبتكال

مدير أول - استشارات التكنولوجيا - إرنست ويونغ موريشيوس

البريد الإلكتروني: siddhesh.mudbhatkal@mu.ey.com

نبذة

عن إرنست ويونغ

إرنست ويونغ | بناء عالم أفضل للعمل

تعمل إرنست ويونغ من أجل بناء عالم أفضل للعمل من خلال المساعدة في خلق قيمة طويلة الأجل للعملاء والموظفين والمجتمع وبناء الثقة في الأسواق المالية.

توفر فرق إرنست ويونغ المتنوعة التي تعمل في أكثر من 150 بلداً، وبما تملكه من بيانات وتقنية، الثقة من خلال التدقيق المالي ومساعدة العملاء على النمو والتحول.

كما تقوم فرقنا، ومن خلال عملها في التدقيق المالي والخدمات الاستشارية ومجال القانون والاستشارات الاستراتيجية والاستشارات الضريبية والمعاملات التجارية بطرح الأسئلة الأفضل للتوصل إلى إجابات جديدة بشأن المشكلات المعقدة التي تواجه عالمنا اليوم.

تشير EY إلى المنظمة العالمية أو إلى احدى الشركات الأعضاء في إرنست ويونغ العالمية المحدودة، حيث تعتبر كل شركة في المنظمة كياناً قانونياً مستقلاً. وكونها شركة بريطانية محدودة بالتضامن، لا تقدم إرنست ويونغ العالمية المحدودة أية خدمات للعملاء. ويمكن الحصول على معلومات حول كيفية قيام EY بجمع البيانات الشخصية واستخدامها، والاطلاع على الحقوق التي يتمتع بها الأفراد بموجب قانون حماية البيانات، من خلال الرابط ey.com/privacy . لا تزاول الشركات الأعضاء في إرنست ويونغ العالمية المحدودة أعمال القانون والمحاماة عندما يكون ذلك محظوراً بموجب القوانين المحلية. وللمزيد من المعلومات حول المنظمة، يرجى زيارة ey.com

القمة العالمية للحكومات

@WorldGovSummit

#WorldGovSummit

شارك في النقاش

worldgovernmentsummit.org