منشآت
monsha'at
الهيئة العامة للمنشآت الصغيرة والمتوسطة
Small & Medium Enterprises General Authority

مركز الابتكار

كتيّب

البنية التحتية الوطنية الحيوية

Critical National Infrastructures CNIs

إعداد وتقديم
د. عادل الشمراني

Thakaa_center Thakaacenter

سياسة الاستخدام

إن المعلومات الواردة في هذا التقرير جُمِعَت ونُسِّقت بجهود موظفي مركز ذكاء التابع للهيئة العامة للمنشآت الصغيرة والمتوسطة "منشآت"، ولا ينبغي لقارئها أن يعمل بها دون مشورة مناسبة من المتخصصين.

للمزيد من المعلومات، نرجو التواصل معنا على البريد الإلكتروني: **support@thakaa.sa**

ماهي البنية التحتية الوطنية الحيوية:

البنية التحتية الوطنية الحيوية تمثل الركيزة الأساسية للأمم، حيث تضم مجموعة متنوعة من الأنظمة والأصول الأساسية الضرورية لاستقرارها وقوتها العامة. وفي هذا المقال سوف نتطرق لعدة مجالات تعتبر في نطاق البنية التحتية الوطنية الحيوية ومنها:

في مجال البنية التحتية للطاقة، تسهم أنظمة الشبكة، ومرافق النفط والغاز، وميادين الطاقة المتجددة بشكل كبير في توليد وتوزيع الطاقة في البلدان.

قطاع النقل، يشمل ليس فقط الطرق والجسور والمطارات ووسائط النقل العامة، ولكن أيضاً الشبكات المعقدة للخدمات اللوجستية التي تضمن التدفق السلس للسلع والخدمات.

بنية الاتصالات، بدءاً من مزودي خدمات الإنترنت إلى مراكز البيانات، تشكل العمود الرقمي للدولة، وتلعب دوراً حاسماً في التواصل الحديث وتبادل المعلومات.

تشمل خدمات الطوارئ، بما في ذلك إنفاذ القانون ومكافحة الحرائق ووحدات الاستجابة الطبية، الدفاع الأولي للسلامة العامة.

الخدمات المالية، بعد البنوك التقليدية، تشمل الشبكة المعقدة للمعاملات الرقمية وأنظمة الاقتصاد التي تشكل أساس استقرار الأمة المالي.

البنية الصحية تشمل لا تقتصر على المستشفيات والعيادات، ولكن أيضاً صناعة الأدوية ومؤسسات البحوث الطبية وأنظمة الصحة العامة.

قطاع الزراعة، الذي يعتبر حاسماً لإنتاج وتوزيع الغذاء، يلعب دوراً ليس فقط في الاعتيان لكن أيضاً في الاستقرار الاقتصادي. المرافق الحكومية، بما في ذلك مراكز البيانات ومراكز الإدارة، تضمن الوظائف الفعّالة للحكومة.

في مجال الدفاع والأمان، المنشآت العسكرية ووكالات الاستخبارات والبنية التحتية الأمنية الأخرى ضرورية لسيادة الأمة وحمايتها. المشهد المتغير للتهديدات يبرز أهمية بنية الأمان الرقمية، بما في ذلك الأنظمة والتدابير لحماية من التهديدات الرقمية وضمان التشغيل الآمن للشبكات الرقمية.

البنية التحتية الفضائية، بما في ذلك الأقمار الصناعية والمرافق الفضائية ذات الصلة، أمور حيوية للاتصالات والملاحة ومراقبة الطقس والأمان الوطني.

بنية الطاقة النووية، بما في ذلك محطات توليد الطاقة ومرافق البحث، تضيف تعقيدًا للمشهد الحيوي، مطالبة بتدابير أمان صارمة وإجراءات استجابة طويلة.

للحفاظ على هذه البنية التحتية الوطنية الحيوية، تقوم الحكومات بتطوير خطط وسياسات شاملة تدمج التدابير الأمنية الفعّالة، وبروتوكولات الأمان الرقمي، وإستراتيجيات التأهب للطوارئ، وأطُر إدارة المخاطر.

يُعتبر التعاون بين القطاعين العام والخاص أمراً أساسياً، يُشجع على بناء جهد جماعي للتصدي للتحديات المتنوعة، من الكوارث الطبيعية إلى التهديدات الرقمية، وضمان استمرارية وأمان الوظائف الحيوية للأمة في مواجهة التحديات والطوارئ المتنوعة. هذا الترابط الدقيق للأنظمة داخل الشبكة العنكبوتية يبرز أهمية التدابير الاستباقية والتخطيط الإستراتيجي لتعزيز قوة الأمة في مواجهة مشهد متغير من التهديدات والحالات الطارئة المحتملة.

الأمن السيبراني والبنية التحتية الوطنية الحيوية:

تأمين البنية التحتية الوطنية الحيوية من منظور الأمان السيبراني يتطلب نهجاً متنوعاً وشاملاً، نظراً للطبيعة المتطورة لتهديدات الإنترنت وتوسع سطح الهجوم المستمر في الأنظمة الرقمية الحديثة. يشكل التهديد المتقدم المستمر (APTs)، الذي يكون غالباً تنظيمه من قبل دول أو مجموعات إجرامية سيبرانية عالية التنظيم، خطراً كبيراً على البنية التحتية الوطنية الحيوية بسبب أهميتها الإستراتيجية. يصبح التنبؤ المستمر وتبادل معلومات التهديد وآليات الكشف المتقدمة مكونات حاسمة لإستراتيجية دفاعية نشطة لتحديد والرد بفعالية على التهديدات المتقدمة المستمرة. تكامل أجهزة الإنترنت من الأشياء (IoT) داخل البنية التحتية الحيوية يضيف تعقيدات إضافية، حيث قد تكون لدى هذه الأجهزة ثغرات يمكن استغلالها. يتطلب ضمان أمان IoT تنفيذ وسائل قوية للتحقق من الهوية وبروتوكولات تواصل آمنة، وتحديثات منتظمة لتقليل المخاطر المحتملة.

وبالإضافة إلى ذلك، يزيد الاعتماد على أنظمة التحكم الصناعية (ICS) وأنظمة مراقبة وتحكم العمليات (SCADA) من الرهانات، حيث يمكن أن يؤثر أي اختراق على العمليات الأساسية. تصبح الشبكات المعزولة، والمراقبة الأمنية الدورية، والالتزام بمعايير الأمان الخاصة ببيئات ICS/SCADA إجراءات أساسية للحماية.

ومن المتوقع بأن استغلال الثغرات التي تكون مجهولة بواسطةZero-day exploits تسلط الضوء على الحاجة إلى أنظمة قوية للكشف عن الاختراق وتحليل السلوك، وخطط الاستجابة السريعة.

يظهر أمان الحوسبة السحابية كاعتبار حيوي، حيث تعتمد الدول في بناء البنية التحتية الوطنية الحيوية بشكل متزايد على خدمات الحوسبة السحابية لتحقيق الكفاءة والتوسع. يصبح تطبيق ضوابط الوصول الصارمة، وتشفير البيانات أثناء النقل وفي وضع التخزين، والتقييمات الأمنية الدورية لبنية الحوسبة السحابية من أهمية قصوى. يتيح تأثير الحوسبة الكمومية على معايير التشفير ضرورة للمؤسسات للبحث واعتماد خوارزميات التشفير المقاومة للكم تحضيراً للتحديات المستقبلية. تستند إستراتيجيات الأمان الوطني، التي تشمل غالباً التعاون بين الوكالات الحكومية والكيانات الخاصة وأطراف أخرى، إلى الاستفادة الكبيرة من رفع مستوى أمان البنية التحتية الوطنية بشكل عام. في الوقت نفسه، يسهم التدريب المستمر والتمارين المحاكية في تمكين الأفراد من فهم والاستجابة بفعالية للتهديدات السيبرانية، مما يضمن مرونة خطط الاستجابة. التعاون، على الصعيدين الوطني والدولي، يكون أمراً أساسياً، نظراً للطبيعة العابرة نظراً لطبيعة التهديدات العابرة للحدود السيبرانية السيبرانية، مما يبرز أهمية تبادل المعلومات والبحث المشترك ووضع قواعد للسلوك المسؤول في السيبرانية. في هذا السياق الدينامي، حيث تتطور تهديدات الإنترنت باستمرار، يكون الحفاظ على موقف قوي وتكييفي في الأمان السيبراني ضرورياً لحماية استمرار البنية التحتية الوطنية الحيوية.

الأمن السيبراني والبنية التحتية الوطنية الحيوية:

استغلال البنية التحتية الوطنية الحيوية من خلال هجمات الإنترنت يمكن أن يكون له عواقب خطيرة وواسعة النطاق، حيث يؤثر ذلك ليس فقط على البنية المستهدفة ولكن أيضاً على الأمان الوطني والسلامة العامة ورفاهية الدولة بأكملها. تنشأ خطورة استغلال البنية التحتية الوطنية من الدور الحيوي الذي تلعبه هذه البنى في وظائف المجتمعات والاقتصادات. فيما يلي عدة جوانب يجب أخذها في اعتبارك:

1. تهديد للأمان الوطني:

العديد من مكونات البنية التحتية الحيوية، مثل أنظمة الدفاع والاتصالات وشبكات الطاقة، ضرورية للأمان الوطني. يمكن أن يؤدي استغلال هذه الأنظمة إلى تعطيل قدرة الدولة على الدفاع عن نفسها والرد على التحديات الخارجية والحفاظ على السيادة.

2. تأثير اقتصادي:

يمكن أن يكون للتعطيل أو التلاعب في البنية التحتية الحيوية تاثيراً اقتصادياً هائلاً. تعتمد الصناعات والشركات والمؤسسات المالية على البنية التحتية لاستقرار عملياتها. يمكن أن تؤدي الهجمات السيبرانية على البنية التحتية الحيوية إلى تراجع اقتصادي وخسائر مالية وانقطاعات في سلاسل التوريد.

3. مخاطر السلامة العامة:

بعض البنى التحتية الحيوية، مثل أنظمة النقل وخدمات الطوارئ ومرافق الرعاية الصحية، مرتبطة مباشرة بسلامة الجمهور. يمكن أن يؤدي استغلال هذه الأنظمة إلى حدوث حالات منازعة، معرضة حياة الأفراد للخطر وتعترض الاستجابة الفورية لحالات الطوارئ والكوارث.

4. اضطراب اجتماعي:

يعتمد استقرار الحياة الاجتماعية على الوظائف السليمة للخدمات الأساسية مثل إمدادات المياه والكهرباء وشبكات الاتصالات. يمكن أن تؤدي الهجمات السيبرانية على هذه الخدمات إلى اضطراب اجتماعي، مما يؤثر على حياة المواطنين اليومية ويخلق شعوراً بعدم الأمان في المجتمعات.

5. تهديدات السيبرانية-الجسدية:

يمكن أن يؤدي استغلال البنية التحتية الحيوية إلى تهديدات سيبرانية-جسدية، حيث تتسبب الهجمات الرقمية في عواقب واقعية. على سبيل المثال، يمكن أن يؤدي التلاعب بأنظمة التحكم الصناعي في منشآت التصنيع أو الطاقة إلى حدوث أضرار جسدية، أو كوارث بيئية، أو حتى فقدان الأرواح.

6. انتهاكات البيانات وقضايا الخصوصية:

تتعامل بعض البنى التحتية الحيوية، مثل نظم الرعاية الصحية والأنظمة المالية، مع كميات ضخمة من البيانات الشخصية الحساسة. يمكن أن يؤدي استغلال البنية التحتية الحيوية إلى انتهاكات ضخمة للبيانات، مما يعرض خصوصية وأمان الأفراد للخطر، ويمكن أن يسهم في سرقة الهوية أو الاحتيال المالي.

7. هلع وفوضى على نطاق وطني:

يمكن أن يخلق استغلال البنية التحتية الحيوية على نطاق واسع شعوراً بالخوف والهلع والفوضى بين السكان. يمكن أن يؤدي انقطاع الاتصالات، وانقطاع التيار الكهربائي، أو انقطاع الخدمات الأساسية إلى فقدان الثقة العامة في الحكومة والسلطات.

8. عواقب طويلة الأمد:

يمكن أن يكون استعادة الوضع بعد هجوم كبير على البنية التحتية عملية طويلة وصعبة. يمكن أن تشمل العواقب طويلة الأمد علاوةً على الإنفاق في الأمن السيبراني، وتغييرات في السياسات الوطنية، والحاجة إلى تحديثات شاملة للأنظمة المتأثرة.

9. الآثار الإستراتيجية:

قد يكون لدى الدول أو الجهات الخبيثة التي تستغل البنية التحتية أهداف إستراتيجية، مثل ضعف موقف الدولة على الساحة العالمية أو اكتساب رافعة في المفاوضات الجيوسياسية. يمكن أن يكون استغلال البنية التحتية الحيوية جزءاً من إستراتيجية أوسع لتحقيق أهداف سياسية أو عسكرية.

10. تأثير عبر الحدود:

الهجمات السيبرانية على البنية التحتية الحيوية لا تقتصر عند الحدود. يمكن أن يكون لاستغلال البنية التحتية على نطاق وطني تأثيرات تمتد عبر الحدود على مستوى عالمي، مما يؤثر على الدول المجاورة والتجارة الدولية والأنظمة العالمية المترابطة.

هجمات سيبرانية على البنية التحتية الحيوية :

كما نعرف بأنه أصبحت الهجمات الإلكترونية ضد البنية التحتية الحيوية أكثر شيوعاً وتعقيداً قد يستهدف المهاجمون البنية التحتية الحيوية لأسباب متنوعة، بما في ذلك المكاسب المالية أو التجسس أو التعطيل.

تشمل بعض أكثر أنواع الهجمات الإلكترونية شيوعاً ضد البنية التحتية الحيوية ما يلي:

- **هجمات تعطيل الخدمة (DoS):**
تقوم هذه الهجمات بتعطيل أنظمة البنية التحتية الحيوية بإرسال محاولات اتصال بشكل كبير جداً، مما يمنع المستخدمين من الوصول إليها.

- **هجمات البرامج الضارة:**
تنطوي هذه الهجمات على زرع برامج ضارة لأنظمة البنية التحتية الحيوية بهدف سرقة البيانات أو تعطيل العمليات أو السيطرة على الأنظمة.

- **هجمات التصيد الاحتيالي:**
تحاول هذه الهجمات خداع موظفي البنية التحتية الحيوية للكشف عن معلومات حساسة أو النقر فوق الروابط الضارة.

- **هجمات الوسيط MITM:**
تعترض هذه الهجمات الاتصالات بين أنظمة البنية التحتية الحيوية بهدف سرقة البيانات أو تعديل التعليمات. هجمات سلسلة التوريد: تستهدف هذه الهجمات موردي البنية التحتية الحيوية من أجل الوصول إلى شبكات البنية التحتية الحيوية أو أنظمتها.

أمثلة لهجمات سيبرانية على أنظمة البنية التحتية الحيوية:

Stuxnet (2010): Stuxnet هو هجوم متطور بالبرامج الضارة استهدف البرنامج النووي الإيراني. يُعتقد أنه تم تطويره من قبل الولايات المتحدة وإسرائيل. تسبب Stuxnet في دوران أجهزة الطرد المركزي في منشأة تخصيب اليورانيوم في مدينة نطنز بشكل لا يمكن السيطرة عليه، مما أدى إلى إتلافها.

BlackEnergy (2015): BlackEnergy هي مجموعة من البرامج الضارة تم استخدامها في عدد من الهجمات ضد البنى التحتية الوطنية الحرجة. في عام 2015، تم استخدام BlackEnergy لمهاجمة شبكة الكهرباء الأوكرانية، مما تسبب في انقطاعات واسعة النطاق.

WannaCry (2017): WannaCry هو هجوم انتزاع فدية أثر على أكثر من 200 ألف جهاز كمبيوتر في 150 دولة. استهدف WannaCry عدداً من البنى التحتية الوطنية الحرجة، بما في ذلك المستشفيات وشبكات النقل وشبكات الكهرباء.

NotPetya (2017): NotPetya هو هجوم انتزاع فدية يُعتبر على نطاق واسع أكثر الهجمات الإلكترونية تكلفة في التاريخ. استهدف NotPetya البنى التحتية الوطنية الحرجة في أوكرانيا وبلدان أخرى، مما تسبب في أضرار بمليارات الدولارات.

SolarWinds supply chain attack (2020): كان هجوم سلسلة توريد SolarWinds هجومًا متطورًا استهدف تحديثات البرامج من شركة SolarWinds. تمكن المهاجمون من إدراج التعليمات البرمجية الضارة في تحديثات SolarWinds، والتي تم تثبيتها بعد ذلك من قبل العملاء حول العالم. استهدف هجوم SolarWinds عددًا من البنى التحتية الوطنية الحرجة، بما في ذلك حكومة الولايات المتحدة وشركات Fortune 500.

Colonial Pipeline ransomware attack (2021): كان هجوم Colonial Pipeline ransomware هجوماً انتزاع فدية استهدف Colonial Pipeline، وهي واحدة من أكبر خطوط أنابيب النفط في الولايات المتحدة. أجبر الهجوم خط الأنابيب على الإغلاق لعدة أيام، مما تسبب في نقص في البنزين وارتفاع الأسعار على طول الساحل الشرقي للولايات المتحدة.

هجوم الفدية على Maroochy Water Services (2018): استهدف هذا الهجوم محطة معالجة مياه في كوينزلاند بأستراليا. استخدم المهاجمون انتزاع الفدية لتشفير أنظمة المصنع، وطالبوا بفدية قدرها مليون دولار. أُجبر المصنع على الإغلاق لعدة أيام، مما عطل إمدادات المياه لأكثر من 270 ألف شخص.

Industroyer (2016): Industroyer عبارة عن مجموعة من البرامج الضارة مصممة لمهاجمة أنظمة التحكم الصناعية. في عام 2016، تم استخدام Industroyer لمهاجمة شبكة الكهرباء الأوكرانية، مما تسبب في انقطاعات واسعة النطاق.

TRITON (2017): TRITON عبارة عن مجموعة من البرامج الضارة مصممة لمهاجمة أنظمة السلامة في أنظمة التحكم الصناعية. في عام 2017، تم استخدام TRITON لمهاجمة مصنع للبتروكيماويات في المملكة العربية السعودية، مما تسبب في حريق وانفجار.

Havex (2013): Havex عبارة عن مجموعة من البرامج الضارة مصممة لاستهداف أنظمة التحكم الصناعية. تم استخدام Havex لمهاجمة عدد من البنى التحتية الوطنية الحرجة، بما في ذلك شبكات الكهرباء وخطوط أنابيب النفط والغاز ومحطات معالجة المياه.

CragRAT (2017): CragRAT عبارة عن مجموعة من البرامج الضارة مصممة لاستهداف أنظمة التحكم الصناعية. تم استخدام CragRAT لمهاجمة عدد من البنى التحتية الوطنية الحرجة، بما في ذلك شبكات الكهرباء وخطوط أنابيب النفط والغاز.

المصادر:

http://large.stanford.edu/courses/2011/ph241/grayson2/docs/w32_stuxnet_dossier.pdf

https://malpedia.caad.fkie.fraunhofer.de/details/win.blackenergy

https://www.dataprotectionreport.com/05/2017/wannacry-ransomware-attack-summary

https://www.bitdefender.com/blog/labs/massive-goldeneye-ransomware-campaign-slams-worldwide-users

https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

شكراً