مجلة
السلامة المعلوماتية والأمن السيبرني
Cyber Security Magazine

العدد 02
جوان 2022

في هذا العدد:

النشيد الوطني للجمهورية التونسية

حمـــاة الحمـــى يـــا حمـــاة الحمـــى * هلمّـــوا هلمّـــوا لمجـــد الزّمـــــن
لقـــد صرخـــتْ فـــي عروقنـــا الدمـــا * نمـــوت نمـــوت ويحيـــا الوطـــن

لتـــدو السّـــماوات برعدهـــا * لتـــرم الصّواعـــق نيرانهـــا
إلـــى عـــزّ تونـــس إلـــى مجدهـــا * رجـــال البـــلاد وشـــبّانها
فـــلا عـــاش فـــي تونـــس مـــن خانهـــا * ولا عـــاش مـــن ليـــس مـــن جندهـــا
نمـــوت ونحيـــا علـــى عهدهـــا * حيـــاة الكـــرام ومـــوت العظـــام

حمـــاة الحمـــى يـــا حمـــاة الحمـــى * هلمّـــوا هلمّـــوا لمجـــد الزّمـــــن
لقـــد صرخـــتْ فـــي عروقنـــا الدمـــا * نمـــوت نمـــوت ويحيـــا الوطـــن

ورثنـــا السّـــواعد بـــين الأمم * صخـــورا صخـــورا كهـــذا البنـــا
ســـواعد يهتـــزّ فوقهـــا العلـــم * نباهـــي بـــه ويباهـــي بنـــا
وفيهـــا كفـــا للعـــلا والهمـــم * وفيهـــا ضمـــان لنيْـــل المنـــى
وفيهـــا لأعـــداء تونـــس نقـــم * وفيهـــا لمـــن ســـالمونا السّـــلام

حمـــاة الحمـــى يـــا حمـــاة الحمـــى * هلمّـــوا هلمّـــوا لمجـــد الزّمـــــن
لقـــد صرخـــتْ فـــي عروقنـــا الدمـــا * نمـــوت نمـــوت ويحيـــا الوطـــن

إذا الشـــعب يومـــا أراد الحيـــاة * فـــلا بـــدّ أن يســـتجيب القـــدر
ولا بـــد لليـــل أن ينجلـــي * ولا بـــد للقيـــد أن ينكســـر

حمـــاة الحمـــى يـــا حمـــاة الحمـــى * هلمّـــوا هلمّـــوا لمجـــد الزّمـــــن
لقـــد صرخـــتْ فـــي عروقنـــا الدمـــا * نمـــوت نمـــوت ويحيـــا الوطـــن

الفهرس

السلامة المعلوماتيّة والأمن السيبرني

مجلة عسكرية
تثقيفية وتحسيسية

تصدرها وزارة الدفاع الوطني

❖❖❖

المدير التنفيذي
الفريق حبيب الضيف
مدير عام وكالة الاستخبارات والأمن للدفاع

❖❖❖

هيئة التحرير
رئيس التحرير
العميد مروان البرقاوي

نائب رئيس التحرير
المقدم محمد نضال الماجري

المحررون القارون
الرائد عثمان القتلاني
الرائد حسام البدوي
الرائد نادية الفزعي
النقيب سلسبيل شبيل
النقيب خالد الرحال
النقيب خالد الشابي
الملازم أول ظافر رويس

❖❖❖

هيئة الإخراج الفني
النقيب صالح الوسلاتي
الوكيل أول أماني الفريخة
الوكيل زياد الراشي

❖❖❖

التدقيق اللغوي
الوكيل أول عبد الله المشاقي

تقنيون في الإعلامية
العريف أول هيفاء الرازقي

البريد الإلكتروني
cybersecuritymagazine@defense.tn

موقع واب
وزارة الدفاع الوطني
www.defense.tn

ISSN: 2811-6437

كلمة السيّد عماد ممّيش
وزير الدّفاع الوطني

بمناسبة الاحتفال بالذكرى 66 لانبعاث الجيش الوطني، نأذن بصدور العدد الثاني من مجلة السلامة المعلوماتية والأمن السيبرني، والتي تعمل وزارة الدفاع الوطني على انتظام صدورها سنويا في إطار مجهوداتها الرامية إلى التعريف بأنشطة المؤسسة العسكرية في مجال الدفاع السيبرني، إضافة إلى مواكبتها للتطور الحاصل في ميدان التكنولوجيات الحديثة للمعلومات والتواصل المستغلة على الصعيدين المدني والعسكري.

تعتبر هذه النشرية عسكرية تثقيفية ترفيهية، تهدف بالأساس إلى تحسيس الأفراد بأهمية حماية النظم المعلوماتية والتطبيقات في ظل التطور السريع لوسائل الاتصال والتكنولوجيات الحديثة المستخدمة وما ينجر عنها من تهديدات ومخاطر على أمن المنشآت الحيوية والحساسة وأمن الأسرار وعلى السيادة الرقمية.

يمثل هذا العدد تواصلا للتوجّه الذي وقع اعتماده بالوزارة في ظل وجود إستراتيجية وطنية للأمن السيبرني 2020-2025 وانفتاح المؤسسة العسكرية على الفضاء المدني، دعمًا للعملية الاتصالية الداخلية خاصة ولتحسيس العسكريين بأهم التهديدات السيبرنية المستجدة وسبل مجابهتها، إضافة إلى نشر الثقافة الرقمية والتعريف بأبرز أنشطة الوزارة السنوية في المجال كالملتقيات العلمية والدورات التكوينية الوطنية والدولية، وذلك تعميما للفائدة لتشمل غير المختصّين في المجال.

في الختام، أتوجه بالشكر لكامل أفراد الفريق الساهر على إعداد هذا العدد من مجلة السلامة المعلوماتية والأمن السيبرني، داعيًا إياهم للمحافظة على انتظام صدورها وقيمة وتنوع محتواها.

افتتاحية العدد الثاني
بقلم الفريق حبيب الضيف
مدير عام وكالة الاستخبارات والأمن للدّفاع

أذن السيد وزير الدفاع الوطني بصدور مجلة السلامة المعلوماتية والأمن السيبرني سنويا قصد مزيد الرفع من مستوى اليقظة لدى مختلف مستعملي الأنظمة المعلوماتية بوزارة الدفاع الوطني وتحسيسهم بالمخاطر والتهديدات السيبرنية المستجدة ونشر ثقافة السلامة المعلوماتية والأمن السيبرني داخل الوسط العسكري وخارجه.

وفي ذات السياق، أفرز التطور التكنولوجي في مجال الاتصال والشبكات مفاهيم جديدة ومتغيرة، على غرار أنترنات الأشياء الحوسبة السحابية والجيل الخامس للاتصالات والذكاء الاصطناعي، وهو ما أدّى إلى تنامي الأخطار والتهديدات السيبرنية وتطور طرق وتقنيات قرصنة الأنظمة المعلوماتية.

وفي هذا الإطار، تعمل جميع هياكل وزارة الدفاع الوطني على مواجهة هذه الأخطار والحدّ منها عبر تحسين مستوى النظم المعلوماتية والتجهيزات المستغلة والارتقاء بها مع وضع برامج ومخططات تضمن استمرارية العمل ومجابهة الأخطار، إضافة إلى تكوين ضباط ذوي مؤهلات وكفاءة عالية في المجال بالتعاون مع الوكالة الوطنية للسلامة المعلوماتية، حيث تخرجت سنة 2021 دفعة أولى ماجستير مهني إختصاص "أمن سيبرني عملياتي" وأذن السيد وزير الدفاع الوطني بمواصلة تشريك دفعات أخرى بصفة سنوية.

هذا، ويوجد بوزارة الدفاع الوطني هيكل يشرف على حماية نظمها المعلوماتية، وذلك بالتدقيق على معداتها والتطبيقات المستغلة اعتمادا على دليل إجراءات مطابق للمواصفات العالمية وإعداد المذكرات والمناشير المتعلقة بمجال السلامة المعلوماتية، بالإضافة إلى التنسيق مع مختلف المتداخلين لتقديم التوصيات اللازمة لتلافي النقائص المسجلة. كما يقوم الهيكل المذكور بالكشف المبكّر عن الهجمات التي تستهدف مزود خدمات الأنترنات بالوزارة قصد منعها، ونشر معطيات متعلقة بالثغرات والهجمات السيبرنية المستجدة عبر منصّة خاصة تم تطويرها مؤخّرا للغرض بكفاءات داخلية، على غرار جيوش البلدان المتقدمة للتحذير من خطورة هذه الهجمات وتلافي أضرارها على الأنظمة المعلوماتية.

مقالات متنوعة

السلامة المعلوماتية
درع للإدارة الإلكترونية

العميد لطفي حشانة

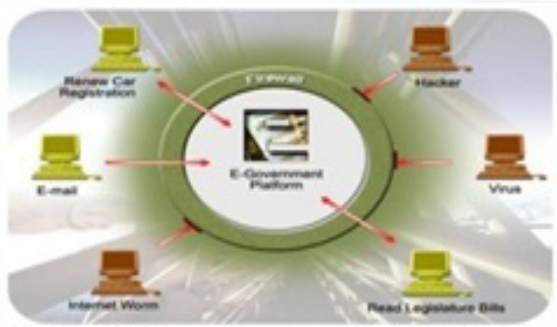
أصبحت الإدارة الإلكترونية مطلبا لضمان الشفافية والمساواة والعدالة بين المواطنين وتفادي المحسوبية والرشوة والبيروقراطية الإدارية التي عطلت مصالح المواطن. كما أنها تعتبر معيارا أساسيا ودوليا في مجال الديمقراطية. لذا، سعت الدول للقيام بالتحول الرقمي في عدة مجالات كالصحة والانتدابات بالوظيفة العمومية والتصرف في الميزانية وحتى الانتخابات التشريعية والرئاسية والبلدية...

إن قرار الدولة توفير خدمات ومعطيات عن بعد يجب أن تكون مؤمنة نظرا لوجود مخاطر وتهديدات سيبرنية خطيرة، حيث تعتبر السلامة المعلوماتية شرطا أساسيا ودرعا واقيا لضمان سرية وصحة المعلومة. ولتوضيح ذلك، سيتم تعريف الإدارة الإلكترونية في مرحلة أولى، ثم عرض المخاطر وكيفية التصرف فيها في مرحلة ثانية، وأخيرا معالجة المخاطر عبر منهجية السلامة المعلوماتية.

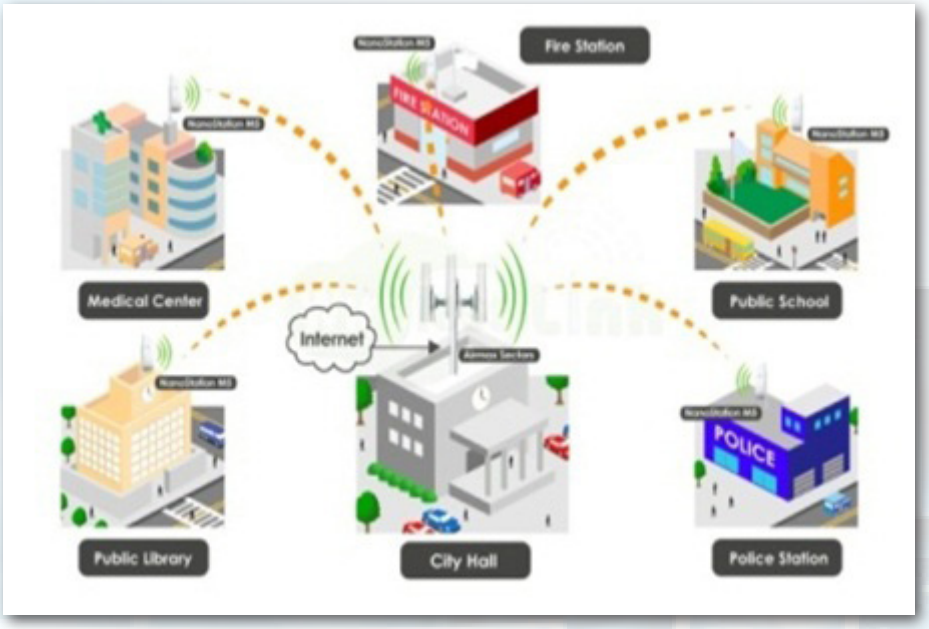
1. الإدارة الإلكترونية مفهوم حديث وأساسي :

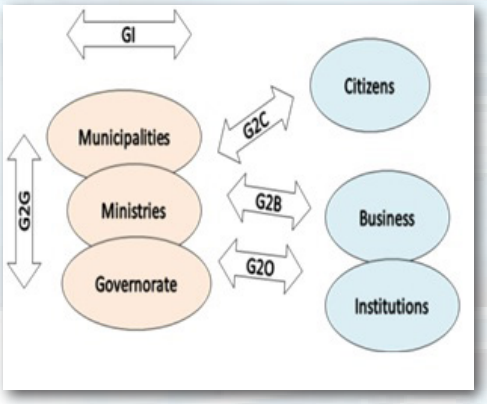
تهدف الإدارة الإلكترونية إلى تقليص الإجراءات بين طالب الخدمة والإدارة وذلك باستعمال تكنولوجيات الاتصال والمعلوماتية. وتمكّن الإدارة الإلكترونية من توفير معلومة سريعة وذات جودة عالية يمكن أن تساعد في اتخاذ القرار بالنسبة للمسؤول واستغلالها بالنسبة للفرد وبصفة عامة لمختلف الفاعلين.

كما يعتبر تطوّر تكنولوجيات الاتصال والمعلوماتية رافدا لتدعيم الإدارة الإلكترونية التي تستعمل بالخصوص شبكة الأنترنات وبعض الشبكات المحلية بالنسبة لتطبيقات معينة. وقد واكبت تونس هذا التطوّر وشرعت في إنجاز مشاريع تطبيقات توفّر للمواطن خدمات عن بعد كخلاص فواتير الكهرباء والماء والهاتف والاطلاع على الحسابات البنكية والتسجيل عن بعد للسنة الدراسية في الجامعات والمعاهد الثانوية والإعدادية والمدارس الإبتدائية...



وتجدر الإشارة إلى أن وزارة الدفاع الوطني بادرت في هذا المجال بتوفير خدمات عن بعد كالانتدابات بصفوف الجيش والنفاذ للمعلومة ومنظومات داخلية بين هياكلها كالتصرف في الميزانية (منظومة إنجاز) والتصرّف في الموارد البشرية (الشبكة المندمجة للتصرف في المعطيات)...





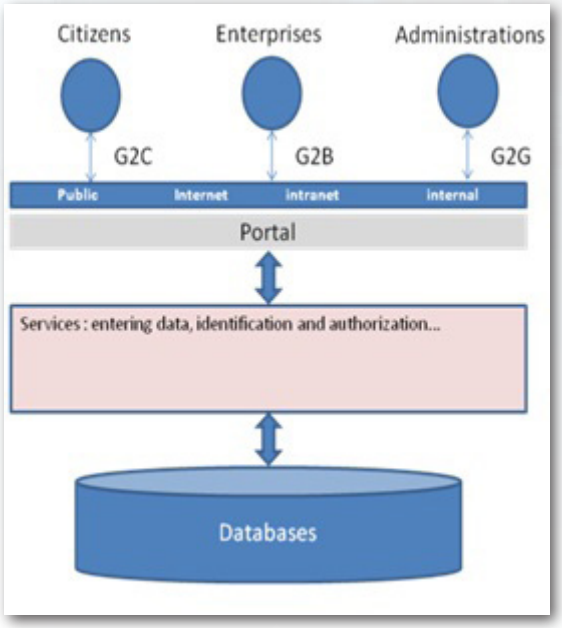
2.1 العلاقة بين مختلف الفاعلين:

- الإدارة داخل الإدارة نفسها (GI)
- الإدارة مع إدارة أخرى (G2G)
- الإدارة مع المواطن (G2C)
- الإدارة مع المتدخلين في الأعمال (G2B)
- الإدارة مع المؤسسات (G2O)

2.1 هيكلة الإدارة الإلكترونية:

تتيح تكنولوجيات الاتصال للإدارة عناصر تقنية تستجيب للمواصفات والتشريعات المعمول بها والتي تمكّن من إسداء خدمات عن بعد. وتكون الهيكلة كما يلي :

- طلب الخدمة يكون عبر قنوات الاتصال شبكات الأنترنات وشبكات محلية.
- استغلال البوابة الإعلامية للإدارة لتوفير النفاذ للمعلومة والولوج لمختلف الخدمات مع ضمان سهولة الدخول ومنح التراخيص اللازمة بعد التعرّف على طالب الخدمة.
- توفير قاعدة بيانات محينة وشاملة

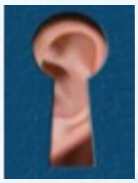


إن فوائد الإدارة الإلكترونية متعددة، فهي تمكّن من فرض الثقة بين المواطن والإدارة وضمان الشفافية وتوفير المعلومة بصفة سريعة، كما تمكّن من تبادل المعلومات بين إدارة الدولة والمؤسسات، ولكن هل أن الإدارة الإلكترونيّة مؤمّنة ضدّ المخاطر السيبرنيّة؟

2. مخاطر الإدارة الإلكترونية :

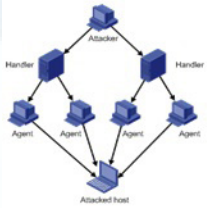
تواجه الإدارة الإكترونية عدة تهديدات ومخاطر سيبرنيّة، لذلك وجب التعرّف عليها وتحليلها والتحكّم في تأثيراتها قدر الإمكان.

1.2 المخاطر :



• اختراق المعطيات (information intercepting) : يتمّ اختراق قواعد بيانات الإدارة أو معطيات طالبي الخدمة.

• العبث بالمعطيات (Information tampring) : يتمّ إدراج أو تغيير معطيات مغلوطة وتقديمها لطالب الخدمة وكأنها معطيات صحيحة أو حذفها تماما.



• منع الولوج إلى الخدمات (Services denying): رفض النظام المعلوماتي الترخيص بالولوج الخدمات أو للشبكات وذلك لوجود هجوم سيبرني أو فيروس أو إمكانية أعطاب مفتعلة للمعدات الإعلامية.

• سرقة موارد النظام المعلوماتي (System resources stealing): سرقة المعطيات من قاعدة البيانات والشبكات وتباع هذه المعطيات في أسواق افتراضيّة على الأنترنات.

• تزييف المعطيات (Information faking): تبديل المعطيات الأصلية بأخرى مزيفة وهذه الأخيرة تكون مضرة للأشخاص والشركات وحتى الدول.

2.2 التصرف في المخاطر:

لمواجهة المخاطر المذكورة آنفا، وجب اتباع إجراءات محددة تحتوي على تحديد وتحليل ثم التحكّم في هذه المخاطر.

• تحديد المخاطر (Risk identifying): تعتبر أول مرحلة في التصرف في المخاطر التي تهدد النظام المعلوماتي للإدارة الإكترونية، ويكون ذلك بتجميع مختلف نقائص النظام المعلوماتي والاختراقات السابقة والمحتملة، ويتمّ تسجيل ذلك بملفات رقمية وسجلات ورقية. ويمكن أن يكون مصدر هذه المخاطر التدخل البشري أو المعدات أو التطبيقات أو الحامل للمعطيات أو مكان العمل والاستغلال.

• تحليل المخاطر (Risk analyzing): يعتمد هذا التحليل على دراسة وتقييم التأثيرات ثم ترتيبها حسب خطورتها على النظام المعلوماتي. وتكون هذه المخاطر إما مقصودة (هجوم سيبرني...) أو غير مقصودة (خطأ بشري من طرف المسؤول أو المستعمل...) أو طبيعية (فيضانات، حريق...). ويتم إنجاز خلاصة حول النتائج المحتملة المباشرة وغير المباشرة على النظام المعلوماتي.

• التحكم في المخاطر (Risk controling): يتم اختيار منهجية التحكّم لتقليص تأثيرات المخاطر على النظام المعلوماتي. وتعتمد هذه المنهجية على تصوّر السيناريوهات المحتملة للمخاطر والحلول التقنية والبشرية لمواجهتها. بعد توضيح المخاطر التي تهدّد الإدارة الإلكترونية والتصرّف فيها وجب أن يطرح السؤال حول كيفية ضمان سلامة نظامها المعلوماتي؟

3. منهجية السلامة المعلوماتية للإدارة الإلكترونية :

تعتبر السلامة المعلوماتية ركيزة أساسية لضمان حماية النظام المعلوماتي للإدارة الإكترونية من مختلف المخاطر سواء كانت بشرية (الحلقة الأضعف) أو تقنية (نظم استغلال وتطبيقات ومعدات إعلامية...) وبنية أساسية (شبكات اتّصال ومحلات غير مؤمنة...) يعتمد نظام السلامة المعلوماتية في الإدارة الإلكترونية على منهجية تصرف في المخاطر في كل المجلات حسب معايير علمية وترتكز على التخطيط (Planning) والفعل أو التدخل (Do) والتقييم (Check) وردّ الفعل (Action) وتتلخص في (PDCA). وفي ما يلي توضيح مبسط لهذه المنهجية :

1.3 التخطيط (Planning) :

إنشاء إستراتيجية حماية نظام الإدارة الإلكترونية حسب مخطط يرتكز على تحقيق أهداف مرتبطة بصد المخاطر وتوفير معلومة صحيحة وحينية. ويكون المخطط حسب أهمية المخاطر مرتبا زمنيا وحسب أولويات الإدارة.

2.3 الفعل أو التدخل (Do) :

تركيز سياسة وقاية وتدخّل وتحكّم ومجابهة المخاطر لنظام الإدارة الإلكترونية. تكون هذه السياسة موثقة وقانونية وذلك بإصدار تراتيب كتابية من طرف رئيس الإدارة.

المسؤول عن السلامة المعلوماتية

3.3 التقييم (Check) :

تقييم داخلي للسياسة المتبعة وملاءمتها مع الأهداف المرسومة لحماية النظام المعلوماتي، ويتم من طرف مسؤول عن السلامة المعلوماتية (كضابط السلامة المعلوماتية بمختلف هياكل وزارة الدفاع الوطني)، ويكون ذلك بالقيام بتجارب وتمارين نظرية وتطبيقية ومحاكاة الهجمات السيبرنية والأعطاب في الشبكات والمعدات للسيطرة والتحكم في المخاطر عند حدوثها، واستقراء التهديدات المستقبلية. يتم إنجاز تقرير بعد عملية التقييم يصادق عليه رئيس الإدارة، كما يستحسن طلب تدقيق معمق

ومتقدم من طرف مختصين في التدقيق الدوري على السلامة المعلوماتية من طرف الهياكل المختصّة يتم على إثرها إنجاز تقرير يبرز النقائص والمخاطر واقتراح حلول عاجلة وآجلة تكون واقعية يسهل تطبيقها مع مراعاة الإمكانيات الحقيقية للإدارة ولا يرتكز على حلول نظرية.

4.3 رد الفعل (Action) :

ويتمّ على ضوء التقارير المنجزة بعد تقييم داخلي أو من طرف مختصين واتخاذ الإجراءات الوقائية والعلاجية على نظام الإدارة الإلكترونية لتحقيق مستوى عال من السلامة المعلوماتية. نتيجة لهذه التقارير، يتم إنجاز الحلول المقترحة للمجابهة والتحكم في المخاطر التي تم تحديدها ويتم استعمالها عند الحاجة. كما يتم تحيين هذه الحلول دوريا حسب التطور التكنولوجي.

إن ضمان حماية النظم المعلوماتية للإدارة الإلكترونية أصبح حتميا لما تحتويه هذه النظم من معطيات هامة يمكن أن تمس الأمن القومي للدولة ذاتها، لذا وجب إعطاء الأولوية القصوى لهذا الموضوع. وينصح في هذا الإطار باتباع معايير الجودة العالمية كمعيار ISO 27001 الذي يعتبر أحد أهم أنظمة التصرّف في السلامة المعلوماتية.

عموما يمكن القول أن الإدارة الإلكترونية تحسن العلاقة بين الإدارة البيروقراطية والمواطن وتوفّر معلومة سريعة تمكّن من رفع نجاعة الإدارة وتحسين أدائها، ويكون ذلك بتحديد المخاطر والتصرف فيها ثم اتباع منهجية لسلامة النظام المعلوماتي للإدارة ضمن إستراتيجية واضحة في إطار مخطط زمني محدد. ولكن مهما كانت المناهج والتقنيات المتبعة لتحقيق سلامة النظام المعلوماتي للإدارة الإلكترونية، لا يمكن ضمان صفر بالمائة من المخاطر (0 %) ولا مائة بالمائة (100 %) من الحماية. لذا وجبت اليقظة دائما ليلا ونهارا مع توفير الإمكانيات البشرية (انتداب وتكوين ورسكلة) والمادية (معدات ونظم استغلال وتطبيقات).

المراجع :

- Information security Management courses, DRESMARA, Brasov, Romania 2015.
- Challenges in E-Government and security information, Information and security journal, vol 15, No 1, 2004 p 9-20.
- Frame / methodology for the information security management in an e-government environment, Ing. Mag. Kristian Tomov, Dr B. Balabanov. ITU Regional Forum on Cybersecurity, October 2012, Sofia, Bulgaria.
- Establishing a Sustainable Information Security Management Policies in Organization: A Guide to Information Security Management Practice (ISMP), International Journal of Computer and Information Technology (ISSN: 2279 - 0764) Volume 04-Issue 01, January 2015.
-Local Government Information Security Risk in the Age of E-Government, Eunjung Shin, Lauren N. Bowman. PhD Students Eric Welch, Associate Professor Department of Public Administration, Science, Technology and Environment Policy Lab, University of Illinois at Chicago,2010.
- United nations : E-government Survey 2014, E-government for the future we want.

تكنولوجيا الجيل السادس

الوكيل إيمان الرياحي

تتقدّم التكنولوجيا دائما للأمام فتجدنا نسير في طريق عالم شبكات الجيل السادس «6G» مع أنّ مجرّد الفكرة تبدو مبكّرة في الوقت الذي ما يزال فيه تركيب واستخدام شبكات اتصالات الجيل الخامس «5G» مستمرًا في جميع أنحاء العالم وعدد مستخدميها لا يزال قليلا. كما أن العديد من مناطق العالم تستخدم شبكات اتصالات الجيل الرابع «4G»، حتى أنّ بعض البلدان لا تزال في طور إستخدام شبكات الجيل الثالث «3G». فهل سيصبح الخيال العلمي واقعا متجسّدا وطبيعيا مع تكنولوجيا الجيل السّادس؟ أم أنّها ستكون مجرّد «شبكات الجيل الخامس المحسّنة» (5G Enhanced)؟

1. تطور شبكات الأنترنات:

شهد الانتقال إلى شبكات الجيل الرابع «4G» في بدايات سنة 2010 زيادة كبيرة في السرعة بعد أن كان يعاني من بطء في تصفّح الأنترنات ومكالمات الفيديو لشبكات الجيل الثالث «3G». بينما توفر شبكة «5G» الآن اتصالاً أكبر للعديد من الأجهزة كما تساعد على بناء نظام عصبي إدراكي يدمج الذّكاء الاصطناعي والإدراك اللّاسلكي بهدف تحسين زمن الاستجابة (يصل إلى 20 جيغابايت في الثانية) مع زمن استجابة أقلّ. أمّا من حيث التنمية الاقتصادية، فقد سبق وأن عزّزت تقنيات الجيل الثالث «3G» التجارة الإلكترونية، بينما عززت تقنيات الجيل الرابع «4G» التجارة الإلكترونية والدفع عبر الهاتف الجوّال. ويمثل بناء وتطبيق البنية التحتية «5G» بداية التصنيع الذكي للشركات العالميّة كالصينيّة والأمريكيّة.

2. شبكات الجيل السادس «6G»:

من المتوقّع أن تعمل تقنية الجيل السادس مع حلول سنة 2030 على تحسين نقاط ضعف الجيل الخامس مع سرعة بأضعاف قد تصل إلى 1 تيرابايت في الثانية بعد توسعة النطاق التردّدي للشبكات (أكثر من 300 جيغاهرتز) مع وقت استجابة أقل من 100 ميكروثانية وهو مستوى غير مسبوق من السرعة ممّا سيؤدي مستقبلا إلى زيادة أداء تطبيقات «5G» بالإضافة إلى تطوير تطبيقات جديدة ومبتكرة. كما ستساعد هذه التكنولوجيا المتقدمة في ربط العالم الحقيقي بالعالم الرقمي الافتراضي ممّا سيجعل تصميم المنتجات والبحث والتطوير أكثر كفاءة وتقلل من تكاليفها بشكل كبير.

أمّا تقنية الإدراك اللاسلكي «la technologie de perception sans fil» المرتبطة بتقنية «6G»، فبمجرد نضوجها ستقوم بتطوير الاقتصاد الرقمي الذي سيصبح قائما على القدرة التنافسية للدول في المستقبل وبالتالي المحرك الرئيسي للاقتصاد الرقمي وذلك من خلال:

- كشف التهديدات (la détection des menaces)
- المراقبة الصحية (la surveillace de la santé)
- الاعتراف بالسمات والوجوه (la reconnaissance des caractéristiques et des visages)
- تحسين التكنولوجيات المتنقّلة مثل المركبات المستقلّة والمدن الذكيّة (Améliorer les technologies mobiles telles que les véhicules autonomes et les villes intelligentes)...

وعلى الرّغم من أنّ شبكات الجيل الخامس قد بدأ العمل بها في بعض الدّول منذ سنة 2019 كالصين وأمريكيا وبعض الدول الأوروبية وأن هذه الدول قد بدأت فعليا في البحث والدعم لمراكز بحوثها وشركاتها الكبرى لتطوير شبكات الجيل السادس، إلّا أنّ تونس لا تزال تعاني من ضعف وبطء شبكات الجيل الرابع مع عدم توفر تام للأنترنات في بعض المناطق الريفية نظرا لضعف البنية التحتية، وحلم شبكات الجيل الخامس لا يزال في طور التجربة من قبل مشغلي الاتصالات على غرار أورنج. فهل سنبدأ برؤية ملامح الجيل السادس في العالم قبل أن نستخدم هاتفا يدعم تقنية «5G» بشكل كامل في تونس؟

المراجع:

- http://mmwave.dei.unipd.it/research/6g/
- https://www.tuitec.com/ar/
- https://www.telenorconnexion.com/technologies/evolution-mobile-technology/
- https://www.journaldugeek.com/2022/02/16/6g-un-nouveau-record-de-vitesse-etabli-a-1-tb-s-grace-a-des-ondes-3d/

مراكز الاستجابة للطوارئ الإعلاميّة

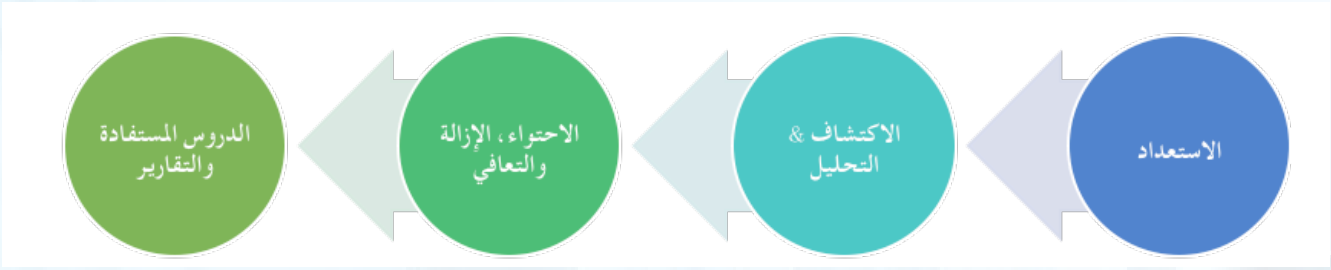
الملازم أول ظافر رويس

لا يخفى على الجميع أهمية الأمن السّيبرني وحماية الأنظمة المعلوماتيّة في الوقت الحالي نظرا لما يشهده العالم من تطور هام في مجال التكنولوجيا وتقنيات الاتصال، حيث أصبح لا يمكن الاستغناء عن استعمالاتها من قبل كل الفئات لما توفّره من سهولة في الاستخدام وإمكانيّة تحقيق أرباح ماديّة.

تشير المواقع والهياكل المختصّة في مجال السلامة المعلوماتيّة والأمن السيبرني من خلال نشر إحصائيّات حول الثغرات والهجمات السّيبرنيّة أن معدّل هذه الحوادث في ارتفاع بشكل ملحوظ حيث أصبحت تشكل خطرا على أمن الدول من خلال تسريب بيانات حسّاسة ونشرها على الواب المظلم وتعطيل خدمات إلكترونية، أو تؤثر على حياة أشخاص في بعض الأحيان من خلال الاستقطاب والتحرش عبر مواقع التواصل الاجتماعي. لذا أصبح من الضروري توفير بيئة سيبرنيّة آمنة وموثوقة لضمان حسن استغلال التكنولوجيا الحديثة في مختلف الخدمات العموميّة.عمدت عدّة دول وشركات كبرى إلى إنشاء مراكز خاصّة بالاستجابة للطوارئ الإعلاميّة تهدف إلى حماية البنى الرقمية الحسّاسة (الحيوية)، ومن أبرز مهام هذه المراكز أنها تعمل على الاستباق في رصد وكشف التهديدات والهجمات السيبرنيّة والتعامل معها بصفة حينيّة حسب طبيعتها ودرجة خطورتها، وتقديم الحلول والمقترحات التقنيّة لتلافي الثغرات وحماية مكوّنات النظام المعلوماتي. كما تعمل هذه المراكز على نشر المعطيات التقنيّة المشبوهة (عناوين ، بصمات رقميّة، مجالات، عناوين بريد إلكتروني) على منصّات ومواقع مختصّة في المجال للاستفادة منها وتطبيقها بالمعدات المستهدفة، إضافة إلى القيام ببرامج تحسيسيّة لتوعيّة الأفراد حول مدى

خطورة الهجمات وما يمكن أن ينجر عنها وذلك من خلال تنظيم محاضرات في الغرض أو تصميم نشريات ومقاطع فيديو مبسطة تحتوي على إجراءات السلامة المعلوماتيّة.

1. منهجية الاستجابة للحوادث السّيبرنية:



تعتمد جميع مراكز الاستجابة للطوارئ الإعلاميّة على منهجيّة للاستجابة للحوادث السّيبرنيّة حسب المعايير العالميّة والتي ترتكز أساسا على 4 مراحل:

1.1 الاستعداد:

تُعتبر هذه المرحلة العمود الفقري لكل مركز حيث يتمّ من خلالها حصر كل المعطيات حول البنية التّحتيّة للأنظمة المعلوماتيّة والشّبكات والتّطبيقات خاصّة الحسّاسة منها والمزمع مراقبتها. ويتم خلالها تركيز برمجيّات خصوصيّة لكشف الهجمات التي تستهدف الموزّعات الرّئيسيّة على غرار موزّع الواب، البريد الإلكتروني والمجالات،... والمراقبة الدّوريّة لحركة البيانات داخل الشبكة وملفّات النّفاذ "fichiers logs" وإعداد خطّة الاستجابة للحوادث السّيبرنيّة عند وقوعها.

2.1 الاكتشاف والتحليل:

تتمثّل هذه المرحلة في تكوين فرق تعمل بنظام 24/7 تقوم بمراقبة الحوادث عبر شاشات مخصّصة للغرض في مرحلة أولى، وتحليلها للتثبّت من صحّة وجودها في مرحلة ثانية، وإعداد تقرير تقني أوّلي في حالة التأكد من وجود حدث مشبوه وتمريره إلى فريق تقني لمزيد التحري والتدقيق في مختلف مراحل الهجمة.

3.1 الاحتواء، الإزالة والتعافي:

وهي المرحلة الأكثر دقّة حيث تقوم فيها الفرق التقنيّة بحصر مصادر الهجمات وتحديد المؤشرات الفنيّة، القيام بنسخ رقميّة للأجهزة المصابة ثمّ تحليلها، التفحّص في البرمجيّات الخبيثة والملفّات القارّة، التأكّد من خلوّ الشبكة وجميع المعدات من مؤشّرات الهجمة، عزل الأنظمة المصابة وإعادة صيانتها وفحصها.

4.1 الدروس المستفادة والتقارير:

تعتبر هذه المرحلة الأخيرة التي يتمّ خلالها تحرير تقرير فني مفصّل حول الحادثة السّيبرنيّة وتحيين البرمجيّات الخصوصيّة وإضافة جميع المؤشّرات والأنشطة التي تمّ اكتشافها ومراقبتها بصفة دوريّة ثم نشرها بالمنصات الخاصّة حتى يتم منعها مستقبلا.

2. تحديد أولويات الاستجابة للحوادث:

يُعتبر الوقت عنصرا مهما في الاستجابة للحوادث السيبرنية لذا كلّما قلّت الفترة الزمنيّة بين بداية الهجمة واكتشافها كلّما تقلّ الأضرار المترتّبة عن الهجمة. يُمكن خلال مرحلة الاكتشاف والتحليل أن يواجه فريق الاستجابة للطّوارئ عدّة تنبيهات سيبرنيّة مختلفة في نفس الوقت ويستحيل تحليلها والاستجابة لها بصفة حينيّة، لذا وفي هذه الحالة يتمّ تصنيفها حسب الأولويّة وترتيبها من الحوادث ذات الخطورة العالية جدّا إلى الأقل خطورة.

ومن أهم العوامل التي يعتمد عليها لتحديد الأولويّات لتحليل الحوادث هي:

- قيمة وحجم البيانات بالجهاز (معطيات حسّاسة بحاسوب مخصّص للعمل، صور وفيديوهات شخصيّة، قاعدة بيانات خاصة بمعطيات الأفراد،...)،
- مكان الجهاز المصاب في الشبكة (موزّع حسّاس، حاسوب مسيّر، حاسوب مستعمل عادي،...)،
- نوع الهجمة وعدد تكرارها على نفس الجهاز.

3. المركز العسكري للطوارئ الإعلاميّة«CERT MIL»:

تماشيا مع التوجه العالمي نحو إنشاء هيئات من قبل الدولة للعمل في مجال الأمن السيبرني، بادر هيكل مختصّ في السّلامة المعلوماتيّة بوزارة الدّفاع الوطني إلى بعث مركز عسكري للاستجابة للطوارئ الإعلاميّة حيث يمكن من متابعة وإدارة الحوادث السّيبرنيّة داخل الوزارة. يهدف هذا المركز إلى الكشف المبكّر، الإنذار والتّصدي للهجمات المستهدفة للأنظمة المعلوماتية التّابعة لوزارة الدّفاع الوطني، تحقيق اليقظة التكنولوجية ومواكبة المستجدات في مجال السّلامة المعلوماتيّة، تنظيم محاضرات تحسيسية وتوعوية لمختلف الأفراد وهياكل الوزارة، والقيام بالتحريات السّيبرنيّة "Cyber Forensics" اللازمة عند حدوث طارئ سيبرني.

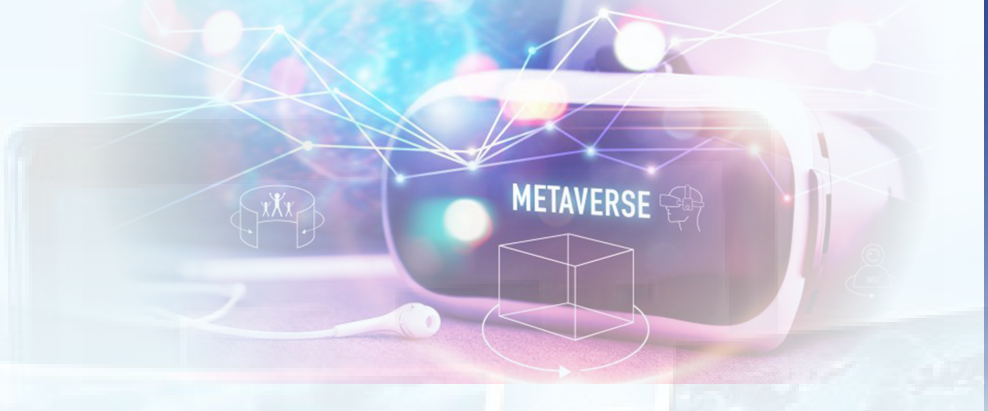
لا شك أن مشهد التهديدات السيبرنية سيتطور في الأيام القادمة، غير أنه من الواضح أن ملخص السنوات السابقة لا يعرض سوى نظرة بسيطة حول مخاطر العام المقبل، إذ يختلف كل عام عن الآخر. في هذا السياق، من الضروري أن يتّسم العام المقبل بسمتين قيميتين: الجاهزيّة والصمود السيبرني.

المراجع:

-https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0_ar.pdf
- https://www.rmg-sa.com
- https://github.com/ThA33/IRGuide

عالم الميتافيرس "Metaverse"

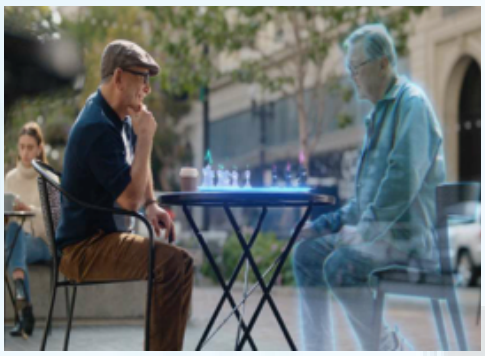
الوكيل أوّل صدّيق بن الطيّب



شهدت الثورة الرقمية في النصف الثاني من القرن العشرين تطورا سريعا فاق جميع تنبؤات وتصورات أغلب الخبراء في العالم التقني، فعلى مدى عمره القصير تطور الفضاء السيبرني في سنوات الثمانينات والتسعينيات من الصفحات النصية ووسائل التواصل البسيطة إلى الأنترنات الملون والسريع والمملوء بالحركية والثريّ بالمعطيات البصرية عالية الدّقة من صور وفيديوهات. مع بداية القرن الحادي والعشرين تسارع التطور التكنولوجي خاصّة بعد الانتشار الواسع لوسائل التواصل الاجتماعي المتنوعة والترقيات المستمرة لأنظمة تصفّح الواب (web3.0) وبزوغ نجم العملات الرقمية وحلم الثراء السريع مع وفرة التطبيقات على مختلف المنصّات من هواتف وساعات وشاشات عرض ذكية ومختلف نظم الاستغلال مفتوحة المصدر. فحسب أغلب الباحثين في المجال فإن هذا العالم لن يدوم طويلا على شكله الحالي مع التطور الكبير الذي تشهده سرعة نقل البيانات على غرار شبكات الجيل الخامس (5G) المنتشرة والتحضير للانتقال إلى شبكات الجيل السادس قريبا، ومع استغلال تكنولوجيا الخدمات السّحابية "Cloud".

1. ثورة الميتافيرس:

في إطار مواكبة التطوّر التكنولوجي واللّحاق بالشركات الكبرى مثل مايكروسوفت، إنفيديا، وولمارت، سناب شات وغيرهم في مجال العوالم الافتراضية قامت شركة «فيسبوك» العملاقة مؤخرا بتغيير إسمها إلى «Meta» والمشتق من مصطلح «Meta Verse»، حيث صرّح رئيسها «مارك زوكربيرغ» بأنّ هذا العالم الافتراضي سيصبح المنصّة التقنية الأهم مستقبلا و«أنّنا سوف نحيا ونعمل من خلاله». كما أعلنت ذات الشركة عن اعتزامها توفير 10 آلاف وظيفة جديدة في الإتحاد الأوروبي لبناء هذا العالم، وحسب توقعاتها سيكون المستخدمون قادرين على التسوق، وعلى مقابلة أصدقائهم، والعمل عن بُعد، وسيتيح مشاركة المساحات الرقمية، والموسيقى، والأعمال الفنية، بالإضافة إلى دمج العناصر الرقمية في العالم الماديّ.



سيساهم دمج العالم المادّي بمعطيات افتراضية في تمكين المستخدمين على سبيل المثال من حضور مباراة لكرة القدم لم يكن بالإمكان فعليّا الذهاب إلى مكان انعقادها وذلك عبر ما يُعرف بتقمص الأفاتار «Avatar» (شخصية رمزية ثلاثية الأبعاد) والتي تمثل الشخص الحقيقي في العالم الافتراضي.

2. مفهوم الميتافيرس:

تشتقّ كلمة «MetaVerse» من شقين الأول «Meta» وهي كلمة لاتينية تعني (ما وراء) والثاني «Verse» مشتق من «univers» «الكون»، تمّ استعمالها لأوّل مرة في رواية (Snow Crash) للكاتب الأمريكي «نيل ستيفنسون» سنة 1992، حيث يتفاعل البشر من خلال تقمّص شخصيات خيالية (ava-tars) مع بعضهم البعض وعبر بعض البرمجيات، في فضاء إفتراضي ثلاثي الأبعاد مشابه للعالم الحقيقي. وقد استخدم المؤلف «ستيفنسون» هذا المصطلح لوصف بديل لما بعد الأنترنات ويعتمد على الواقع الافتراضي. يستخدم المصطلح لوصف «الإصدارات المستقبلية المفترضة» لعالم الأنترنات والمكوّنة من مساحات ثلاثية الأبعاد لامركزية، ومتصلة بشكل دائم ويمكن دخولها عبر نظارات الواقع الإفتراضي أو الواقع المعزّز أو الهواتف الجوالة أو الحواسيب المكتبية ومنصّات الألعاب المختلفة.

3. كيفية عمل الميتافيرس:

العالم الافتراضي في لعبة Roblox

هناك حاليّا عدد من التطبيقات الفعليّة الموجودة ضمن ما يسمّى بالميتافيرس، خاصّة في مجالات الإنتاج السينيمائي والألعاب الإلكترونية على غرار «Mine craft» و «Fortnite» و «Roblox» كما أنه وحسب توقعات الشركات التكنولوجية الكبرى عند الوصول إلى عالم «ميتافيرس مثالي» سيكون بمقدور المستخدم أن يخوض أي تجربة أو نشاط وسيكون بإمكانه التعامل مع أيّ أمر يحتاجه من مكانه دون الحاجة إلى التنقل.

1.3 الواقع المعزّز Augmented Reality (AR):

إجتماعات افتراضية في عالم الميتافيرس

يعتبر الواقع المعزّز نوع من الواقع الافتراضي الذي يهدف إلى نسخ البيئة الحقيقية ونقلها إلى الحاسوب و تعزيزها بمعطيات افتراضية لم تكن جزءا منها، فنظام الواقع المعزّز يولّد عرضا مركّبا للمستخدم يمزج بين المشهد الحقيقي الذي ينظر إليه المستخدم والمشهد الظاهري الذي تم إنشاؤه بواسطة برمجيات الحاسوب والذي يعزّز المشهد الحقيقي بمعلومات إضافية. يهدف المشهد الظاهري «virtual scene» إلى تحسين الإدراك

الحسّي للعالم الحقيقي الذي يراه أو يتفاعل معه المستخدم. ويهدف الواقع المعزّز إلى إنشاء نظام لا يمكن فيه إدراك الفرق بين العالم الحقيقي و ما أضيف عليه. فعند قيام شخص ما باستخدام هذه التقنية للنظر في البيئة المحيطة به فإن الأجسام في هذه البيئة تكون مزوّدة بمعلومات تظهر أو «تسبح» حولها وتتكامل مع الصورة التي يشاهدها المستعمل وتزوده بكافة المعطيات التي يريد رؤيتها. هذا، وتستخدم تقنية الواقع المعزّز حاليا في مجال الترفيه، والتدريب العسكري، والتصميم الهندسي، والروبوتات، والصناعة التحويلية وغيرها من الصناعات، كما يتم إدماجها في التعليم بشكل تدريجي.

2.3 الواقع الافتراضي Virtual reality (VR):

الواقع الإفتراضي (VR) هو محاكاة برمجيات الحاسوب للبيئات التي يمكن محاكاتها ماديّاً في بعض الأماكن في العالم الحقيقي، وذلك في عالم خيالي يصنع بالمؤثرات البصرية، أو عرض على شاشة الحاسوب أو من خلال عرض مجسّم خاص. تتضمّن بعض المحاكاة معلومات حسيّة إضافية مثل الصوت من خلال مكبّرات الصوت أو سمّاعات الرأس. كما يوجد بعض الأنظمة المتقدّمة اللمسيّة (Tou-chable)، وتشمل المعلومات عن طريق اللمس، والمعروفة عموما بإسم قوّة ردود الفعل، في التطبيقات الطبية والألعاب الإلكترونية. كما يتوقع مزيد دمج بعض الحواس الأخرى عبر البيئة الرقمية مستقبلا (كالرائحة والطعم). يشمل الواقع الافتراضي على بيئات الاتصال عن بعد والتي توفر للمستخدمين وجود ظاهري مع مفاهيم التواجد عن بعد إمّا من خلال استخدام أجهزة الإدخال العادية مثل لوحة المفاتيح والفأرة، أو من خلال أجهزة متعددة الوسائط مثل النظارات المتطوّرة والقفازات.

4. التحديات التي ترافق هذا التحول على أمن المعلومات والمعطيات الشخصية والمجتمعات والأشخاص:

يرى بعض المختصين أن عالم الميتافيرس الذي تحاول الشركات الكبرى التسريع في إظهاره على الساحة التجارية يمثل تهديدا على سلامة الأطفال (أكبر مستخدميه في الوقت الحالي) ويتوجب إحداث عوالم خاصة بهم تتيح لأوليائهم مراقبتهم. يمكن أن تسحر عوالم الميتافيرس المستخدمين وتقنعهم بأنها جديرة باستهلاك الوقت والاستثمار المهووس فيها وبأنها يمكن أن تكون مفيدة (بعض المستثمرين دفعوا ما يقارب المليون دولار أمريكي لشراء أراضي على العالم الافتراضي «sandbox» و هناك من اشترى أرض ب 450 ألف دولار ليجاور المغني الشهير SnoopDogg) . فقد يؤدّي عالم الميتافيرس إلى زيادة الضغوطات ومن المرجّح أن تزيد المخاطر المحتملة للإدمان والتعلق الإلكتروني. كذلك، فإن تفاقم الاستغلال الواسع لتقنية التزييف العميق«DeepFake» والتي تتيح صنع محتوى مزيّف عالي الكفاءة يستهدف الأشخاص وذلك بتركيب صورهم على شخصيات افتراضية لتشويههم أو الإساءة إليهم علاوة عن تفاقم ظاهرة التنمر الإلكتروني.

يمثل هذا العالم الافتراضي المبتكر بيئة آمنة وجيدة لبعض المنحرفين لممارسة

تم فعليا بيع هذا اليخت على الميتافيريس بمبلغ 650
ألف دولار من العملة الرقمية المشفرة

الجرائم والإخلالات غير الأخلاقية أو التي يعاقب عليها القانون في الحياة الفعلية على غرار التحرش أو الابتزاز وقد حصلت في شهر فيفري 2022 عملية اغتصاب جماعية لـ(Avatar) خاص بسيدة معروفة منذ مشاركتها لأول مرة في هذه البيئة وهو ما طرح كثير التساؤلات حول التعامل القانوني في الميتافيرس.

هذا، وسيغير هذا العالم الافتراضي طبيعة عمل الإعلانات التي ستعتمدها الشركات الكبرى كمصادر أرباح والتي رافقتها عديد الانتهاكات والتشكيّات. كما أنّ استعمال العملة الرقمية المشفرة في بيع وشراء الممتلكات والعقارات في العالم الافتراضي قد يتيح لبعض المجرمين ضرب القوانين التقليدية عرض الحائط وتفشي المخالفات الضريبية مثل غسيل الأموال والتفصّي من الرقابة المالية والجبائية وغيرها.

عموما، تتسابق الشركات التكنولوجية الكبرى للاستثمار والسيطرة على هذا العالم الافتراضي الجديد مع إقناع المستخدمين بأنّه مستقبل الأنترنات القريب، فهنالك العديد من التساؤلات المتعلقة بهذه التقنيات والعوالم الافتراضية التي يجب طرحها والإجابة عنها قبل الانسياق في المجهول وتحت قيادة هذه الشركات العملاقة. فهل سيكون هذا العالم الافتراضي المفتوح آمنا في المستقبل؟ وما هي انعكاساته على الحياة الطبيعية لمستعمليه؟ و ما مدى تأثيره على التواصل وعلى التعاون وعلى التعلّم للأفراد والمجتمعات؟ وهل ستزيد صعوبة مراقبة المحتوى في هذا العالم الرقمي؟ وماهو مصير المعطيات الشخصية الضخمة التي سيعالجها؟ وهل سيكون الخروج من متاهة هذه العوالم سهلا إن برزت الحاجة لذلك، علما أنها عوالم رقمية متعددة وتدار من قبل شركات عملاقة متنوعة؟

المراجع:

- https:/www.asharq.co/whmn4
- https:/www.youtube.com/watch?v=Uvufun6xer8
- https:/www.Reuters.com/technology/what-is-metaverse-2021-10-18
- https:/www.ar.wikipedia.org/wiki/ميتافيرس
- https:/www.akhbar24news.com/2021/12/09/metaverse-2031-a-day-in-the-life
- https:/www.matthewball.vc/the-metaverse-primer
- https:/www.cbr.com/doomsday-clock-superman-metaverse/
- https://www.mosoah.com/law-and-government/military-and-defense
- https://al-ain.com/article/deep-fake-apps-dangerous-entertainment-absurdity
- https:/www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview
- https:/www.bbc.com/arabic/science-and-tech-59009407
- https:/www.bbc.com/arabic/science-and-tech-59327203

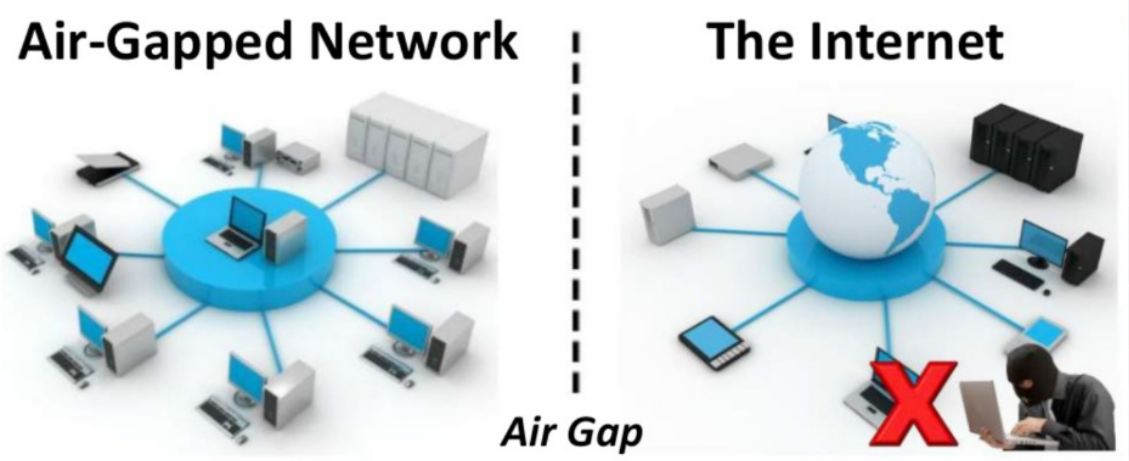
ثغرات الفجوة الهوائية
Air Gab

النقيب خالد الشابي

في ظل تزايد الهجمات والأخطار المهددة للأنظمة المعلوماتية تسعى الشركات والمنظمات ودول العالم إلى حماية أنظمتها المعلوماتية من شبكات وحواسيب، ولعل أحد أنجع الحلول المتبعة في هذا المجال هو عزل الشبكات والحواسيب الخاصة بالنظم الحساسة على غرار الشبكات العسكرية والحكومية وصناعات الطاقة عن باقي الشبكات في ما يسمى الفجوة الهوائية Air Gab. غير أنّ هذا الإجراء لا يحد بصفة قطعية الأخطار والتهديدات نظرا لنجاح بعض الهجمات التي تستغل المكونات المادية للحواسيب مثل الذاكرة وبطاقة الصوت للقيام بهجمات سيبرنية تستهدف فجوة الهواء. سنتطرق ضمن هذا المقال لتعريف الثغرات المتعلقة بفجوة الهواء مبرزين كيفية عمل هذه الثغرات ومخاطرها على الأنظمة المعلوماتية.

1. الفجوة الهوائية Air Gab:

في مجال سلامة وأمن المعلومات تسمى فجوة الهواء، أيضا الجدار الجوي، هو إجراء أمني يمكّن من عزل الأنظمة المعلوماتية عن أي معدّات أو شبكات خارجيّة قصد تأمينها مما يجعل أي محاولة لقرصنتها عن بعد شبه مستحيلة.



2. الثغرات المتعلقة بالفجوة الهوائية:

تستهدف ثغرات الفجوة الهوائية مكوّنات الأنظمة المعلوماتية المعزولة مثل الحواسيب والشّبكات الداخليّة المؤمّنة وذلك باستغلال ترددات قريبة أو خارج حدود السمع البشري المنبعثة من أجزاء الحواسيب من ميكروفونات ومكبّرات صوت أو إدخال معدات من الفروض أن لا تكون ضمن الشبكة وبالتالي قرصنة الشبكة الداخليّة المؤمنة وسرقة المعطيات مثل استعمال قرص قلمي USB يحتوي على برمجية ستوكسنت "Stuxnet" الخبيثة للدخول للفجوة الهوائية في المنشآت

النووية الإيرانية وهو ما أدّى إلى إصابة أجهزة الكمبيوتر وتدميرها، وبالتالي عمل المنشأة النووية.

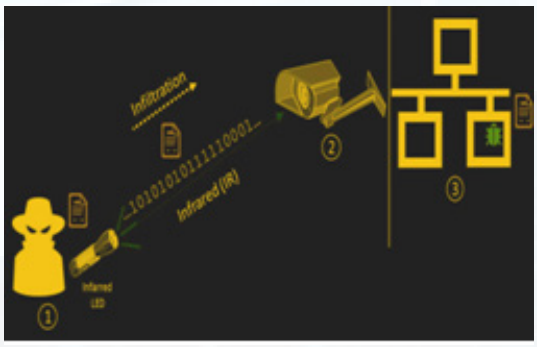
1.2 القنوات المستهدفة لثغرة الفجوة الهوائية:

1.1.2 القنوات الصوتية:

يمكن لمكبرات الصوت والميكروفونات الخاصة بالحواسيب إنتاج الصوت على مستويات غير مسموعة بشريّا حيث يمكن تفعيلها عن بعد، مما يتيح استخدامها من طرف القراصنة كقناة استخدامها واستلام المعطيات.

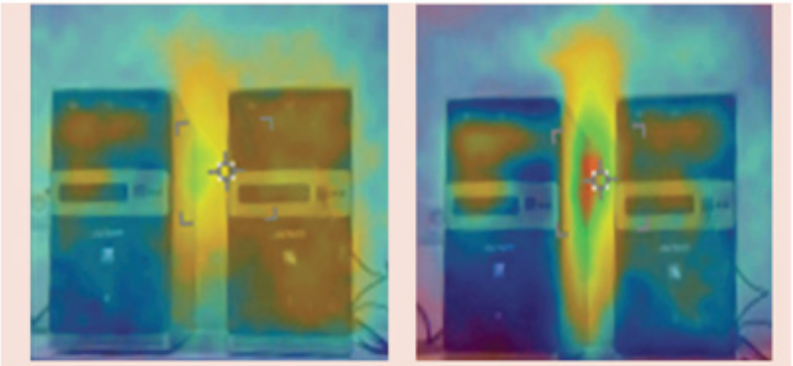
2.1.2. القنوات البصرية:

تستعمل الأجهزة البصرية كطريقة لتسريب البيانات بطريقة لا يمكن الكشف عنها بالعين البشرية المجرّدة، حيث يمكن للمهاجمين تسريب البيانات الحساسة باستغلال الأجهزة الطرفية (مثل لوحة المفاتيح) المجهزة بمؤشرات الضوء، كما يمكن استخدام مستشعر ضوئي أو كاميرا فيديو لاستقبال الإشارات.



3.1.2 القنوات الحرارية:

يمكن للمهاجمين استخدام درجة الحرارة المنبعثة من وحدة المعالجة المركزية (Proc-cesseur) ووحدة معالجة الرسومات (Processeur Graphique)، كقنوات اتصال ذات تردد منخفض جدا، بالإضافة إلى أنظمة تكييف الهواء والتدفئة في قاعة الموزعات.



4.1.2 القنوات الكهرومغناطيسية:

ينتج مرور التيار الكهربائي في الأسلاك مجالا كهرو مغناطسيا، حيث يمكن للمهاجمين ضبط الانبعاثات الكهرومغناطيسية على سبيل المثال إلى النطاق الراديوي FM أو نطاقات تردد GSM و UMTS و LTE واستخدامها كقناة خارجية للإرسال.

3. طرق الوقاية من هجمات الفجوة الهوائية:

إن إدراك التهديدات المذكورة وكيفية عملها هو الخطوة الأولى للوقاية منها. حيث يجب أن يدرك المستعملون أن الهواتف الذكية العادية يمكن تحويلها إلى أدوات هجومية، وعليه يجب اتخاذ التدابير الوقائية وأساليب الحماية والتي من بينها:

- تركيز مضاد فيروسات مع تحيينه بصفة دورية.
- حظر الهواتف النقالة في أي مكان بالقرب من الأنظمة الحساسة.
- الفحص الجيّد ومسح الأقراص القلمية USB.
- عدم تفعيل مكبرات الصوت داخل الحواسيب.
- حفظ نسخ إحتياطية للأنظمة المعلوماتية واستعمال تقنية الحوسبة السحابية.
- تحسيس الأفراد حول خطورة مثل هذه البرمجيات.

المراجع:

- www.rubrik.com/insights/what-is-an-air-gap-and-why-is-it-important
- www.sentinelone.com/blog/air-gapped-networks-a-false-sense-of-securitywww.commvault.com/resources/greater-ransomware-protection-with-data-isolation-and-air-gap-technologies
-www.blog.global.fujitsu.com/fgb/2019-01-29/air-gaps-the-most-effective-defense-against-cyberattacks

حرب المعلومات تعريفها
خصائصها وسبل التوقي منها

العميد رؤوف حفصية

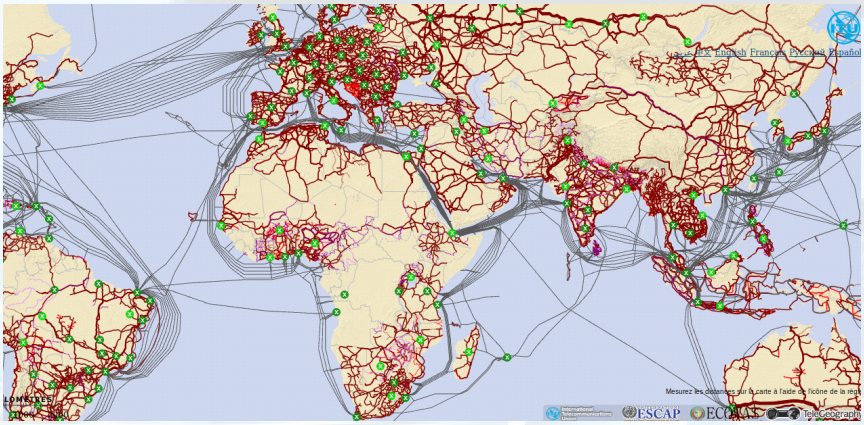
يشهد العالم منذ القرن الماضي وخاصة مع بداية القرن 21 تطورات تكنولوجية سريعة وبالغة الأهمية في مجال أنظمة المعلومات والاتصال، حيث مكنت هذه التطورات من توفير بنية تحتية رقمية قادرة وبصفة ملحوظة على معالجة كم هائل من البيانات في أسرع الأوقات علاوة على توفير شبكة اتصالات مترابطة ومتكاملة سلكية ولاسلكية متكونة من عديد الحوامل (Supports de transmission) ومن أهمها: الأسلاك والألياف البصرية وشبكات الاتصال من الجيل الأول "1G" وصولا إلى شبكات الجيل الخامس "5G" حسب مراحل تطور شبكات الاتصال اللاسلكية المبينة بالجدول التالي:

جدول مراحل تطور شبكات الاتصال اللاسلكية

الجيل	تاريخ الظهور	التطورات	الاستعمال	سعة التدفق
الجيل الأول «1G»	أواخر سنوات 1970	النواة الأولى للاتصالات اللاسلكية مع بعض الصعوبات (حجم ضخم، بطارية كبيرة، فقدان الاتصال بصفة متكررة.	اقتصر الاستعمال على نقل المكالمات الصوتية فقط. لم يتم استخدامه بشكل تجاري إلا في نطاق محدود للغاية.	-
الجيل الثاني «2G»	سنوات1990	الاعتماد على تقنية «GSM» (GlobalSystem for Mobile Communication) والانتقال للعمل من طريقة Analog system إلى Digital Signals ما ساهم في انتشار الهواتف بشكل كبير.	المكالمات الصوتية - الرسائل النصية - رسائل صور أو فيديو، الأنترنات.	64-144kbit/s
الجيل الثالث «3G»	سنوات 2000	ثورة حقيقية في مجال الاتصالات	الأنترنات على الهواتف، تشغيل مقاطع الفيديو والموسيقي، تحميل ملفات كبيرة الحجم، ألعاب الفيديو على الهواتف.	2-14Mbit/s
الجيل الرابع «4G»	2009	الاعتماد على تقنية «: LTE Long Term Evolution»	استخدام الأنترنات على الهواتف واستغلال المحتوي الرقمي بجودة عالية	100Mbit/s
الجيل الخامس«5G»	2019	إدخال تحسينات على تقنية « LTE» مع اعتماد تقنيات رقمية حديثة «- SDN : Sof- tware-Defined Networ- king»	استخدام الأنترنات على الهواتف الذكية بسرعة فائقة، والمنتظر أن يدعم عدد أكبر من الأجهزة وأن يكون نواة لانتشار أنترنات الأشياء«IoT: Internet of Things»	20Gbit/s

هـذا التقـدم الملحـوظ فـي البنيـة التحتيـة الرقميـة للاتصـالات متّـع قرابـة 4.9 مليـار نسـمة مـن سـكان العالـم بشـبكة الانترنـات حسـب الإحصائيـات الأخيـرة لسـنة2021 المقدمـة مـن طـرف الاتحـاد الدولـي للاتصـالات (قرابـة 63 % مـن سـكان العالـم يسـتعملون الانترنـات بتسـجيل17 % إضافيـة مقارنـة بسـنة 2019 حسـب نفـس المصـدر).

جزء من خارطة شبكة الألياف البصرية العالمية



إن التطـورات المسـجلة فـي هـذا المجـال مهـدت الطريـق لتطويـر جملـة مـن التطبيقـات والمنظومـات المعلوماتيـة شـملت جميـع المجـالات منهـا التجـارة الإلكترونيـة والدفـع الإلكترونـي والتدريـس والطـب عـن بعـد والإعـلام والصحـف الإلكترونيـة وتطبيقـات التواصـل الاجتماعـي وغيرهـا مـن الخدمـات الإلكترونيـة التـي أصبحـت ضروريـة ولا يمكـن التخلـي عنهـا مـن طـرف الأشـخاص والمؤسسـات. وقـد أثـرت هـذه المنظومـات بصفـة ملحوظـة علـى مختلـف المجـالات الاقتصاديـة والاجتماعيـة والسياسـية وسـلوكيات الأشـخاص وصـولا إلـى فنـون الحـرب "l'art de la guerre"،مـا أجبـر الـدول علـى اتخـاذ جملـة مـن الإجـراءات وسـن القوانـين ووضـع الوسـائل الماديـة لحمايتهـا، لاعتقادهـا الراسـخ بـأن المسـاس بهـذه الأنظمـة يعتبـر تهديـدا لسـلامتها وأمنهـا وسـيادتها.

1. تعريف حرب المعلومات:

تعـددت مفاهيـم حـرب المعلومـات (Infowar-guerre de l'information-Infoguerre-In-formation Warfare) وتنوعـت معانيهـا ولا يوجـد تعريـف رسـمي لهـا وغالبـا مـا يتـم تعريفهـا بأنهـا اسـتخدام نظـم المعلومـات لاسـتغلال وتخريـب وتدميـر وتعطيـل نظـم معلومـات الخصـم ، وفـي المقابـل العمـل علـى الحمايـة منـه. وعمومـا فـإن هـذه الحـرب تعتمـد علـى وسـائل وأسـاليب تهـدف إلـى التفـوق فـي المعلومـات "Information Superiority" سـواء فـي الهجـوم أو فـي الدفـاع زمـن الحـرب أو السـلم وذلـك لدعـم الإسـتراتيجية العسـكرية للدولـة بالتأثيـر علـى معلومـات الخصـم ونظـم معلوماتـه، وفـي الوقـت نفسـه رفـع مسـتوى فاعليـة معلوماتهـا ونظمهـا الدفاعيـة. ويعتبـر المجـال العسـكري هو أكثـر المجـالات اسـتخداما لهـذا النـوع مـن الحـروب نظـرا للتطـور الحاصـل فـي منظومـات الأسـلحة والاتصـال ووسـائل الإنـذار والاستشـعار والاسـتطلاع والتـي أطلـق عليهـا الكثيـرون إسـم الثـورة التكنولوجيـة فـي الشـؤون العسـكرية " Revolution in Military Affairs"(كتـاب الرؤيـة المشـتركة 2020 الـذي أصدرتـه وزارة الدفـاع الأمـريكيـة).

2. خصائص حرب المعلومات:

من أهم خصائص حرب المعلومات :

• انخفاض التكلفة مقارنة بتكلفة الحرب التقليدية في بعض الحالات (الهجمات السيبرنية، بث الشائعات ونشر الأخبار الزائفة، القرصنة ...).

• عدم التقيد بالحدود الجغرافية، وكذلك عدم وجود خطوط مواجهة محددة.

• إمكانية التسبب في خسائر كبيرة دون خسائر بشرية فهي حرب غير دموية دون قتال.

• التأثير على العناصر الرئيسية والحيوية للدولة في مجالات مختلفة.

• لا يرتبط تنفيذها بالعسكريين ولا تقتصر على الأنظمة العسكرية، بل يمكن أن توجه ضد مؤسسات مدنية أو حتى ضد أفراد.

ومن أهم الوسائل والأدوات المستخدمة في حرب المعلومات:

• الوسائل التقنية :الفيروسات والبرامج الخبيثة،الأبواب الخلفية «Back door» الديدان «Worms» ، حصان طروادة«Cheval de troie»،التشفير «Cryptographie»، القرصنة وسرقة المعلومات، شل شبكات الاتصالات، استخدام الحرب الإلكترونية، استخدام الطائرات دون طيار...

• وسائل أخرى: التضليل والخداع، نشر الأخبار الزائفة باستعمال الوسائل الحديثة للتواصل الاجتماعي للتأثير على الرأي العام ، الحط من المعنويات والتأثير النفسي، نشر الفكر المتطرف والاستقطاب.

3. أنواع حرب المعلومات:

بالنظر إلى ما سبق ذكره بخصوص التطورات الملحوظة في مجال تكنولوجيا المعلومات المعاصرة والاتصالات السلكية واللاسلكية التي ساهمت بشكل فعّال في معالجة، تخزين، وبث المعلومات، واعتبارا لأهمية المعلومة ـ فامتلاكها يُشكل قوة لصاحبها ـ ومدى تأثيرها على مختلف المجالات الاقتصادية والاجتماعية والسياسية والشؤون العسكرية زمن الحرب وزمن السلم، فأنه يمكن تقسيم حرب المعلومات حسب الباحثين والخبراء في المجال إلى الأقسام التالية، والتي تعتبر من أبرز الأشكال التي تظهر بها هذه الحرب:

• حرب القيادة والسيطرة «Command and Control Warfare».

• الحرب الاستخبارية «Intelligence-basedWarefare».

• الحرب الإلكترونية «ElectronicWarefare».

• حرب العمليات النفسية «PsycologicalOperation».

• حرب المعلومات الاقتصادية «Information EconomicWarefare».

• حرب المعلومات الافتراضية «Cyberwar».

وفي ما يلي سيتم التطرق إلى بعض من أنواع حرب المعلومات المذكورة أعلاه والتي لها علاقة بالشأن العسكري.

1.3 حرب القيادة والسيطرة:

مع زيادة الاعتماد على الأنظمة المعلوماتية والتكنولوجيا الحديثة، وتقليل دور

العامل البشري، تطور مفهوم القيادة والسيطرة C5ISR (Command, Control, Com-puters, Communications, Cyber, Intelligence, Surveillance, andReconnaissance) وأصبح الوسيلة الرئيسية للجيوش لإدارة عملياتها،إذ تضطلع هذه الأنظمة بدور ربط أجهزة الاستشعار وأنظمة الأسلحة وأنظمة المعلومات العسكرية ضمن شبكة واحدة متكاملة ومتجانسة تمكن من قيادة المعركة بتبادل المعطيات بسرعة فعالة.وبالتالي، تهدف حرب القيادة والسيطرة إلى شل أنظمة العدو شبكاته ووسائل نيرانه، وكذلك أنظمة التوجيه والإنذار والمراقبة والاستطلاع، وتعتبر من الأشكال الرئيسية لحرب المعلومات في الصراعات المسلحة.

2.3 الحرب الإلكترونية:

هي أحد أشكال حرب المعلومات، بشكل عالي التقنية وخاصة في العمليات العسكرية، تهدف إلى السيطرة على المجال الكهرومغناطيسي اللازم لعمل نظم التسليح والرادار والتوجيه والإنذار في منطقة العمليات (التشويش على أنظمة تحديد المواقع «GPS» والرادارات والاتصالات العسكرية وأنظمة التحكم في الطائرات دون طيار والاتصالات عبر الأقمار الصناعية وغيرها من عمليات التنصت). هذه السيطرة تكون إما في شكل دعم إلكتروني أو هجوم أو حماية إلكترونية. ولا تتم منفصلة عن الأشكال الأخرى لحرب المعلومات وخاصة حرب القيادة والسيطرة.

3.3 حرب العمليات النفسية:

تهتم بالجانب البشري لحرب المعلومات، وتهدف لمهاجمة عقل الخصم بشكل مباشر ليصل لحالة من اليأس والاستسلام والاقتناع بعدم جدوى المواجهة، كما قال رومل «إن القائد الناجح يسيطر على عقول أعدائه قبل أبدانهم» وقال تشرشل «كثيرا ما غيرت الحرب النفسية وجه التاريخ». ومن أهم أساليب حرب العمليات النفسية،استخدام وسائل الإعلام المرئية والمسموعة والوسائط الحديثة كمنصات التواصل الاجتماعي على شبكة الانترنات لإطلاق الشائعات التي من شأنها زعزعة ثقة الخصم في قدراته وبث الفرقة بين صفوفه.

4.3 حرب المعلومات الافتراضية:

تتّخذ حرب المعلومات الافتراضية من شبكة الأنترنات حلبة صراع لها، وتهدف هذه الحرب لاختراق وقرصنة أنظمة حواسيب الخصم وشبكاته والتحكم فيها عن بعد ومعرفة محتواها دون وجه حق، وسرقة البيانات السرية وتخريبها وطلب الفديات، على غرار الهجوم الإلكتروني «WANNACRY ransomware attack» الذي جد سنة 2017 والذي أطاح بأكثر من 230 ألف جهاز إلكتروني في 99 دولة حول العالم حسب وكالة تطبيق القانون الأوروبية «Europol». وتهدف هذه الحرب إلى إلحاق الضرر بالخصم وتعطيل أنظمة معلوماته والخدمات الحيوية والأساسية له.

4. سبل الوقاية والحماية من حرب المعلومات:

بالرجوع إلى ما تم ذكره، وبالنظر لأهمية المعلومة والمنظومات المعلوماتية في شتّى المجالات الاقتصادية والاجتماعية وخاصة العسكرية وإمكانية المساس بها وتعطيل أنظمة المعلومات والخدمات الحيوية والأساسية، فإنه من الضروري توفير قدرا من الحماية يتناسب مع مستوى أهمية المعلومات بهدف ضمان سلامتها واستمرارية خدمة مختلف المنظومات، وذلك باعتماد جملة من الإجراءات كضبط سياسة واضحة لحماية الأنظمة المعلوماتية «Politique de Sécurité» ووضع الوسائل والطرق والتقنيات (مضاد الفيروسات، جدار نار، مخططات استمرارية الخدمات، مخططات إرجاع الخدمات، مخططات لحفظ المعطيات، مراقبة النفاذ، وسائل الحماية من الحرب الإلكترونية في العمليات العسكرية...) وتحيينها كلما اقتضت الحاجة والحرص على تطبيقها، مع الإشارة كذلك إلى أهمية العنصر البشري ودوره الفعّال في حماية المعلومة وذلك بالتزامه بتطبيق الإجراءات واجتناب الأخطاء مع ضرورة إرساء إستراتيجية لنشر الثقافة الرقمية لدى أفراد المجتمع وتحسيسهم بمخاطر الوسائل الحديثة للتواصل الاجتماعي وعدم الانسياب وراء ما يتم تداوله من أخبار زائفة للتضليل والتأثير على الرأي العام.

في ظل تطور تكنولوجيا المعلومات والاتصالات وما توفره من قدرات عالية على معالجة وتخزين وتحليل وبث كميات هائلة من المعلومات شملت المجالات الاقتصادية والاجتماعية والسياسية والعسكرية والأمنية والثقافية، ومساهمة شبكة الأنترنات في تداولها بين مختلف المنصات وإيصالها إلى نسبة كبيرة من سكان العالم، فإنه من المتضح أن البيئة الرقمية الجديدة إذ وفرت خدمات مفيدة لجميع المستخدمين فإنها مثلت تهديدا واضحا لأمن وسلامة المنظومات والمعطيات الخصوصية للأفراد والمؤسسات وصولا إلى المساس بالأمن القومي للدول.

إن المنظومات المعلوماتية عامة والمعلومة بالخصوص أصبحت في عصرنا هذا ذات أهمية بالغة وامتلاكها أصبح يُشكل قوة وسبقا لصاحبها حتى أنها مثلت صراعا يطلق عليه "حرب المعلومات"، وبالتالي فان البناء الأمني للدولة وسيادتها الرقمية يتم عبر تحديد وبكل دقة، التهديدات والمخاطر التي يمكن أن تنتج عن استخدامات حرب المعلومات لهدف صياغة سياسات لحماية المنظومات المعلوماتية وتحقيق أهداف الأمن القومي في هذا المجال.

المراجع:

- https://www.ege.fr/infoguerre/2001/11/les-principes-de-la-guerre-de-l-information
- https://arabhardware.net/articles/the-evolutuion-from-1g-to-5g
- https://www.itu.int/itu-d/tnd-map-public/fr/
- https://www.institut-ega.org/l/la-guerre-electronique-dans-les-conflits-aujourd-hui
- https://www.accronline.com/article_detail.aspx?id=25605
- https://www.lahaonline.com/articles/views/38362.htm
- https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/chronicles/borden.pdf

الذكاء الاصطناعي
Artificial Intelligence

الرائد بالبحرية بشير سليماني

يعتبر الذكاء الاصطناعي من أهم مجالات التطور التكنولوجي الذي اجتاح الحياة اليومية للإنسان، إذ يتميز بالقدرة على تحليل ودراسة كميات كبيرة من المعطيات والبيانات للمساعدة على أخذ القرار في وقت قصير نسبياً مقارنة بالوقت الذي يستغرقه الإنسان. إذ أصبح الذكاء الاصطناعي مندمجا صلب جميع المجالات كالطب، التعليم وعلوم الفضاء حتى بات من الصعب تجاهل تأثير الذكاء الاصطناعي على حياتنا اليومية.

1. مفهوم الذكاء الاصطناعي:

يعتبر الذكاء الاصطناعي«Artificial Intelligence» من أبرز علوم تكنولوجيا المعلومات والتي اكتسحت عدة مجالات في حياتنا اليومية، على غرار الصناعة، البحث العلمي،علوم الفضاء، الطب والخدمات الذكية للشركات.

ويقصد بالذكاء الاصطناعي قدرة الأجهزة الرقمية والأنظمة المتخصصة في تحليل وتصميم الخوارزميات على أداء الوظائف التي تؤديها عادة الكائنات الذكية، ومثال على ذلك المهام التي يقوم بها الإنسان كالتفكير، التحليل والاستنتاج.

ويتميز الذكاء الاصطناعي بقدرته على المساعدة في اتخاذ القرار بشكل ملائم وجيد، وذلك بالاعتماد على دراسة جميع الاحتمالات وحسن انتقاء نتائجها، وثم اختيار أفضل القرارات التي تؤدي إلى النتائج المطلوبة، ومثال على ذلك الرد الآلي في الروبوتات الذكية وعملية تحديد خصائص الكائنات في الصور من خلال مراجعة البيانات المخزنة في الأجهزة الذكية.

2. أنواع الذكاء الاصطناعي:

يمكن تصنيف انواع الذكاء الاصطناعي حسب القدرات والوظائف الخاصة به كالآتي:

1.2 انواع الذكاء الاصطناعي حسب القدرات:

• الذكاء الاصطناعي الضيق

الذكاء الاصطناعي الضيق«Artificial Narrow Intelligence»ويسمى أيضا الذكاء الاصطناعي المحدود، فهو يركز على مهمة واحدة ومبرمجة سابقا عبر امكانيات تحاكي القدرات البشرية ولا يمتلك أي قدرة على التحليل أو الاستنتاج، وأبرز مثال على ذلك نجد «google translate»،وتعتبر هذه الامثلة ذكاء آلي يستخدم لمعالجة اللغة الطبيعية«Natural LanguageProcessing».

• الذكاء الاصطناعي العام

الذكاء الاصطناعي العام«Artificial General Intelligence» ويسمى أيضا الذكاء الاصطناعي القوي. ومن خلال هذا النوع من الذكاء الاصطناعي تقوم وحدات البحث في المجال بتطوير الآلات الذكية وجعلها تعمل كالذات البشرية من خلال التفكير، التحليل والاستنتاج.

• الذكاء الاصطناعي الخارق

يعتبر الذكاء الاصطناعي الخارق«Artificial Super Intel-ligence» خطوة هامة نحو المستقبل والمبني على التطور التكنولوجي، فهو يقوم على التعويض الكلي للذات البشرية من خلال التفكير، التحليل، الاستنتاج وأخذ القرار. ولنصل إلى هذه المرحلة الهامة يجب علينا الاعتماد تدريجيا وكليا على الذكاء الاصطناعي في كافة المجالات.

2.2 انواع الذكاء الاصطناعي حسب الوظائف:

• **الآلات التفاعلية "Reactive Machines"**

تعتبر الآلات التفاعلية من ابسط أنواع الذكاء الاصطناعي فهي تقوم بردة فعل او حركة اعتمادا على المنطق ودون استغلال البيانات المخزنة سابقا.وأبرز مثال على ذلك الحاسوب نوع «DeepBlue» والتابع لشركة « IBM » والذي تغلب على بطل العالم في لعبة الشطرنج.وذلك من خلال تقييم جميع الحركات الممكنة لأخذ القرار المناسب.

• **الذاكرة المحدودة "Limited Memory"**

يعتبر هذا النوع من الذكاء الاصطناعي تطورا جزئيا في المجال وذلك من خلال قدرته في الاعتماد على البيانات المخزنة سابقا لأخذ القرار المناسب، وأبرز مثال لهذا النوع من الذكاء الاصطناعي نذكر السيارات ذاتية القيادة، والتي تعتمد على البيانات المخزنة والمتعلقة بحالة الطريق وعدة عوامل اخرى لاتخاذ الطريق المناسب الذي ستسلكه.

• **نظرية العقل "Theory of Mind"**

يعتمد هذا النوع من الذكاء الاصطناعي على نظرية العقل وذلك لإدراكه الذات البشرية إدراكا حسيا وتحليل سلوك الانسان بغاية التفاعل معه إضافة إلى القدرة على توقع تصرفاته من خلال اعتماد التحاليل السابقة. وتعتبر نظرية العقل المرحلة المستقبلية من أنظمة الذكاء الاصطناعي والتي تعمل وحدات البحث على تطويرها.

• **الوعي الذاتي "Self Aware"**

يعتبر هذا النوع من الذكاء الاصطناعي الأكثر تطور وإمتدادا لنظرية العقل والتي تقوم على إدراك مشاعر الذات البشرية، بينما الوعي الذاتي يقوم على إدراك الآلة لمشاعرها. وقد يشكل هذا النوع من الذكاء الاصطناعي خطرا على الوجود الإنساني مستقبلا.

3. مجالات استعمال الذكاء الاصطناعي:

يكتسح الذكاء الاصطناعي عدة مجالات نذكر منها:

• **الذكاء الاصطناعي في المجال الطبي:**

يتم استخدام تقنيات الذكاء الاصطناعي في المجال الطبي من خلال استغلال التقارير الطبية وسجلات المرضى وبيانات التجارب السريرية المتعددة والمتنوعة لتطوير صناعة الأدوية وتعزيز البحوث الطبية وطرق العلاج والمساعدة على أخذ القرار في تشخيص المرضى. ومثال على ذلك، قامت منظمة» CambioHealth Care» بتطوير نظام دعم سريري للوقاية من السكتة الدماغية والذي يرسل تنبيهات تحذيرية حينما يكون هناك مريض معرض لخطر الإصابة بسكتة قلبية.

• **الذكاء الاصطناعي في مجال علوم الفضاء**

يعتبر الذكاء الاصطناعي ركيزة في مجال البحث العلمي الخاص بالفضاء وذلك من خلال عمليات بناء وإدارة الأقمار الاصطناعية والتي تعتبر عمليات معقدة. كما تستخدم تقنيات الذكاء الاصطناعي في التطبيقات الفضائية الخاصة بعمليات تحليل كميات كبيرة من بيانات ومعطيات رصد الأرض أو بيانات القيس عن بعد من المركبات الفضائية.ومثال على ذلك، إشارت «Victoria Da Poian» رئيسة الفريق البحثي التابع لوكالة الفضاء الأمريكية «NASA» أن تقنيات الذكاء الاصطناعي تساعد على التحليل الفوري للعينات التي يتم جمعها من الكواكب وهو ما يمكن من ربح المال والوقت لنقل تلك العينات مرة أخرى إلى الأرض بغرض تحليلها.

• **الذكاء الاصطناعي في مجال التعليم**

يهدف الذكاء الاصطناعي في مجال التعليم إلى تطوير القدرات البشرية وأساليب وطرق العمل، وذلك من خلال اعتماد تقنيات تكنولوجية تقوم بتحديد مجالات الاهتمام الخاصة بالمدرسين والتلامذة استنادا إلى بيانات ومعطيات مخزنة سابقا.كما يمكن الذكاء الاصطناعي في مجال التعليم من التقييم الآلي والدقيق للمستوى الدراسي والعمل على تطويره عبر مراجعة المناهج وتبسيط طرق العمل وخاصة تكييف البرامج التعليمية الجامعية مع متطلبات سوق الشغل.

4. دور الذكاء الاصطناعي في مجال الأمن السيبرني:

تعتبر السلامة المعلوماتية من أهم العناصر الأساسية في مجال التطور التكنولوجي،لذلك تعتمد الشركات الكبرى تدابير تنظيمية تتمثل خاصة في عمليات الرقابة وتحديد طرق العمل والمسؤوليات في استغلال مكونات الأنظمة المعلوماتية، وتدابير تقنية تتمثل في اعتماد تطبيقات وبرمجيات تقوم على مراقبة حسن عمل المعدات والأجهزة الرقمية. وتهدف كل هذه التدابير والإجراءات الى حماية المعطيات والبيانات من الهجمات والأحداث السّيبرنية والتي يمكن أن تحدث شلل تام في عمل الأنظمة المعلوماتية وخاصة منها الحساسة. وفي هذا المجال، يصعب على الانسان وحده إدارة وتسيير كل التقنيات المتجددة والتفطن وتحليل كافة الهجمات في أسرع وقت ممكن، لذلك يمكن الاعتماد على خوارزميات الذكاء الاصطناعي في مجال الأمن السّيبرني والذي يتميز بالتحليل، معالجة الكميات الكبيرة للبيانات والاستنتاج الآلي للمساعدة على أخذ القرار والاستباق لصد الهجمات السيبرنية. كما يساعد

الـذكاء الاصطناعـي علـى الكشـف المبكـر للهجمـات وتطويـر القـدرات علـى التأقلـم مـع التطـورات التكـنولوجيـة للمعلومـات وذلـك مـن خـلال:

- دمج الذكاء الاصطناعي في كافة المعدات المكونة للأنظمة المعلوماتية.
- دمج الذكاء الاصطناعي في الأنظمة الخاصة بكشف الاختراقات «IDS».
- دمج الذكاء الاصطناعي في مراكز الاستجابة للحوادث السيبرنية «CERT».

المراجع:

- https://www.actuia.com/contribution/thomas-gayet/ia-et-cybersecurite-8-cas-dusage-principaux/
- https://ar.unesco.org/themes/ict-education/action/ai-in-education
- https://www.ibm.com/ae-ar/watson-health/learn/artificial-intelligence-medicine
- https://www.itproportal.com/features/the-4-types-of-ai-and-where-you-encounter-them/

أهم 5 إشهادات في مجال الأمن السّيبرني

Top 5 Cyber Security Certifications

الملازم أوّل صبرين العايدي

أصبح الاستعمال المتزايد لتكنولوجيات المعلومات والاتصالات خطرا على سلامة الأنظمة المعلوماتية خاصة في ظلّ الاستخدام السيئ وغير المسؤول لهذه التكنولوجيات. في هذا السياق، وسعيا لتأمين المعطيات والمنظومات وتعزيز جانب الأمن السيبرني لمختلف الهياكل الحكومية والخاصة، شهد الطلب على الموظفين المختصين تزايدا هاما في السنوات الأخيرة وخاصة منهم المتحصلين على إشهادات معترف بها في المجال. في ما يلي لمحة عن أهم الإشهادات المطلوبة على الصعيد العالمي.

1. Certified Ethical Hacker (CEH)

هو إشهاد في مجال تكنولوجيا المعلومات موجه خاصة إلى مسؤولي السلامة المعلوماتية وإلى المدققين. يُمنح الإشهاد المذكور من قبل المجلس الدولي لمستشاري التجارة الإلكترونية المعروف بإسم EC-Council.

يُمكّن إشهاد CEH من توفير فهم عميق لمراحل القرصنة الأخلاقية (دون إلحاق الضرر فعليا بالأنظمة)، وطرق الهجمات السيبرنية المختلفة والإجراءات الوقائية المضادة. حيث يتّم تدريب المتلقي على كيفية البحث عن مواطن الضعف والثغرات في الأنظمة المستهدفة باستخدام نفس الأدوات التي يستخدمها المخترق لكن بطريقة شرعية وقانونية بهدف تقييم الوضع الأمني لهذه الأنظمة وتقوية ضوابط الأمان الخاصة بها قصد تقليل مخاطر الهجمات الضارة.

2. Certified Information Security Manager (CISM)

هو إشهاد موجه لمديري أمن المعلومات ولمستشاري تكنولوجيا المعلومات الذين يديرون برنامج أمن المعلومات في المؤسسات. ويُقدم الإشهاد المذكور من طرف جمعية تدقيق ومراقبة نظم المعلومات المعروفة بإسمها المختصر ISACA.

يُمكّن إشهاد CISM من اكتساب الخبرة في مجالات عدة من بينها إدارة أمن المعلومات، وتطوير البرامج وإدارتها، وإدارة الحوادث وإدارة المخاطر السيبرنية.

3. Certified Information Systems Security Professional (CISSP)

هو إشهاد موجه للأشخاص الذين يمتلكون خبرة في مجالات إدارة أمن المعلومات والمخاطر وحماية الشبكات وأنظمة الاتصالات وهندسة الأنظمة وحمايتها وغيرها. ويُمنح هذا الإشهاد من طرف المعهد الدولي لشهادات نظم أمن المعلومات المعروف بإسمه المختصر ISC².

يُمكّن إشهادCISSP من اكتساب الخبرة في مجالات متعددة تتمثل أساسا في ثمانية مجالات وهي :

- إدارة الأمن والمخاطر (Security and Risk Management)
- أمن الأصول (Asset Security)
- الهندسة والمعمارية الأمنية (Security Architecture and Engineering)
- أمن الاتصالات والشبكات (Communication and Network Security)
- إدارة الهوية والوصول (Identity and Access Management)
- التقييم والاختبار الأمني (Security Assessment and Testing)
- العمليات الأمنية (Security Operations)
- أمن تطوير البرمجيات (Software Development Security)

4. CompTIA Security+

هو إشهاد موجه للأشخاص المبتدئين في أي مجال متعلق بالأمن السيبرني من حماية شبكات واختراق أخلاقي، وغيرها من التخصصات ذات الصلة، حيث أن محتوى التحضير للإشهاد يغطي أغلب المصطلحات والمسميات المتعارف عليها، والمفاهيم الأساسية، في مجال الأمن السيبرني. كما يعتبر هذا الإشهاد فني، وليس إداري. ولكنه لا يغطي جميع النواحي التقنية بشكل تفصيلي ودقيق، بل إنه يغطي وبشكل سطحي عدد من المفاهيم والمصلحات دون تعمق. يُمنح الإشهاد المذكور من طرف جمعية صناعة تكنولوجيا الحوسبة أو ما يسمى بـ CompTIA.

5. Certified Information Systems Auditor (CISA)

هو إشهاد يهم العديد من الفئات العاملة في مجال نظم المعلومات الذين لديهم خبرة لا تقل عن خمس سنوات نذكر من بينهم مدققي نظم المعلومات ومديري ومسؤولي تطوير النظم الآلية ومديري ومسؤولي شبكات المعلومات وغيرهم.

يحتوي إشهاد CISA على معارف متنوعة ومن أبرزها:

- التدقيق على نظم المعلومات (IS Audit Process).
- حوكمة نظم المعلومات (IT Governance).
- النظم وإدارة دورة حياة البنية التحتية (Systems & Infrastructure Lifecycle Management).
- تقديم خدمات ودعم نظم المعلومات (IT Service Delivery & Support).
- حماية الأصول المعلوماتية (Protection of Information Assets).
- استمرار العمل و علاج الكوارث (Business Continuity & Disaster Recovery).

يتطلب الحصول على أي إشهاد في مجال السلامة المعلوماتية والأمن السيبرني عادة تحضيرا معمقا مع هيكل مختص يمكّن من اكتساب المبادئ الأساسية وتقنيات الاختبار فيه. إلا أن الراغب في الحصول على الإشهاد مطالب بالتحضير الفردي لمدة تتراوح من 6 أشهر إلى سنة على الأقل حسب صعوبة الإشهاد المطلوب.

المراجع:

- https://www.eccouncil.org/programs/certified-ethical-hacker-ceh-fr
- https://www.comptia.org/certifications/security
- https://www.isc2.org/Certifications/CISSP
- https://www.isaca.org/credentialing/cism
- https://www.isaca.org/credentialing/cisa

حماية المعطيات الشخصية

العريف نضال المنصوري

مع التطور التكنولوجي ومستجدات العالم الرقمي في الإدارات وفي المؤسسات العامة والخاصة، أصبحت حماية المعطيات الشخصية من أهم الأولويات الإستراتيجية للدول، فهي تتوفر في كل مكان ولها مصادر مختلفة كالمؤسسات والأفراد أو السلطات العمومية أو من الأجهزة الإلكترونية، فالمعطيات تنتقل ويعاد إنتاجها وتخزينها لتصبح مادة أولية تستعمل لعدّة أغراض ما بين الممنوع والمشروع.

1. واقع حماية المعطيات الشخصية في تونس:

بظهور وتنوّع التجاوزات في علاقة بمعالجة المعطيات الشخصية مثل الجرائم الإلكترونية والإتجار بها وبيعها في الشبكات المظلمة، أصبحت حمايتها رهان دولي حيث ذهبت العديد من التشريعات إلى تكييف منظومتها القانونية مع التطوّرات التكنولوجية والرقمية لاسيما في الجوانب المعلوماتية والاتصالات للاهتمام بمجال حماية الخصوصية لتأمين معالجة المعطيات الشخصية وتوضيح الجزاءات المترتبة عند التعرض لها.

تعتبر تونس الدولة الثانية والثلاثين في العالم التي قامت بتضمين حماية المعطيات الشخصية في دستورها وكان ذلك إثر الاستفتاء الدستوري سنة 2002، حيث ينص الفصل 24 منه على أن الدولة تحمي الحياة الخاصة وحرية المسكن وسرية المراسلات والاتصالات والمعطيات الشخصية، وتطبيقا لهذا النص الجديد صدر القانون الأساسي عدد 63 لسنة 2004 المؤرخ في 27 جويلية 2007 يتعلّق بحماية المعطيات الشخصية وكان بابه السادس يتعلّق ببعث وتنظيم الهيئة الوطنية لحماية المعطيات الشخصية وأهم أعمالها، حيث تتولى حماية هاته المعطيات وتوعية الأفراد بأهميتها وضرورة تأمينها وإيضاح العقوبات المترتبة عن التلاعب بها.

الهيئة الوطنية لحماية المعطيات الشخصية
Instance Nationale de Protection des Données Personnelles

INPDP

2. مفهوم المعطيات الشخصية ومعالجتها:

تعتبر «المعطيات الشخصية» ـ من وجهة نظر قانونية ـ كل معلومة تسمح بالتعرّف على الهوية والخصائص الذاتية للشخص الطبيعي بطريقة مباشرة أو غير مباشرة بالصورة أو من خلال العديد من المعلومات والرموز مثل رقم بطاقة التعريف الوطنية والوضعية العائلية والبصمة ورقم الهاتف و عنوان السكن والملف الطبي وغيرها. ويقصد بمعالجة المعطيات الشخصية كل العمليات المنجزة بطريقة آلية أو يدوية لجمع هذه المعطيات أو الاطلاع عليها أو تسجيلها أو نسخها أو حفظها أو تخزينها أو تنظيمها أو تنقيحها أو استغلالها أو استعمالها أو إرسالها أو توزيعها أو نشرها أو ربطها بمعطيات أخرى أو إحالتها أو تحويلها أو نقلها بأي شكل من الأشكال أو إخفاء هويتها أو تشفيرها أو فسخها أو إتلافها. تضمّ عملية المعالجة عادة ثلاثة متداخلين وهم: المعني بالأمر، وهو كل شخص تكون معطياته الشخصية موضوع معالجة، المسؤول عن المعالجة وهو كل شخص أو هيكل يحدد أهداف معالجة المعطيات وطرقها، وأخيرا المناول، وهو كل شخص أو هيكل يقوم بمعالجة المعطيات لحساب المسؤول عن المعالجة وتعتبر هذه الأطراف المسؤولة أمام القانون عن المعطيات المتداولة بينها.

3. ضوابط معالجة المعطيات الشخصية:

تقيدا بالقانون المذكور سابقا فإن أي شخص أو مؤسسة أو إدارة تتصرف في المعطيات الشخصية يجب أن تحترم الالتزامات القانونية الستّة (06) التي توضع على كاهل المعالج وهي:

- أولا: الإجراءات الاستباقية، أي قبل التصرف في المعطيات الشخصية يجب الحصول على تصريح مسبق يودع لدى الهيئة الوطنيّة لحماية المعطيات الشخصية وتتعدد التصاريح بتعدد الغايات من المعالجة.
- ثانيا: الموافقة، لا يمكن معالجة معطيات شخصية دون الحصول على موافقة أصحابها إلا في الحالات التي يفرضها القانون أو وجود التزام تعاقدي.
- ثالثا: الغاية المشروعة، يجب أن تكون الغاية من معالجة المعطيات الشخصية محددة وواضحة.
- رابعا: سلامة المعطيات، لا يجب التصرف في المعطى الشخصي قبل ضمان أمنه وسلامته.
- خامسا: التحيين، لا بد من تحيين المعطيات الشخصية بصفة مستمرة.
- سادسا وأخيرا: عند إحالة المعطى الشخصي داخل تونس أو خارجها بعد الحصول على موافقة صاحبه يجب ضمان أمنه وسلامته .

وتعتبر هاته الالتزامات أهم القواعد التي يجب احترامها من قبل الجهات المسؤولة عن معالجة المعطيات الشخصية لتضمن سلامة تداولها وحسن معالجتها وحتى لا يكون المواطن ضحية تلاعب أو يتم الزج به ليكون طرف في تنفيذ جرائم إلكترونية دون علمه باعتباره مسؤول أيضا أمام القانون.

4. حق المواطن تجاه معطياته الشخصية:

لضمان جودة معالجة المعطيات الشخصية على كل شخص معرفة حقوقه تجاه معطياته موضوع المعالجة والمتمثلة في أربع نقاط أساسية وهي:

- الحق في النفاذ إلى معطياته الشخصية (الحصول على نسخة منها).
- الحق في الاعتراض على معالجة معطياته الشخصية.
- الحق في تحيين أو فسخ معطياته الشخصية.
- الحق في النسيان بانتهاء الغاية من المعالجة (النسخ أو إخفاء الهوية).

يجب على كل مواطن رفض أي إجبار بإدلاء معطى شخصي كرقم الهاتف أو رقم بطاقة التعريف الوطنية. كما يجب عليه أن يحرص على حماية معطياته الشخصية بالفضاء الافتراضي بمختلف أشكاله وذلك بعدم تنزيلها على مواقع التواصل الاجتماعي الفايسبوك أو الأنستغرام وغيرها .... حتى لا يتم استغلالها في الجرائم الإلكترونية والتحيّل والتصيد الإلكتروني. هذا ويضمن القانون حق المواطن في تقديم شكاية في الغرض لدى الهيئة الوطنيّة لحماية المعطيات الشخصية عند حصول تلاعب باستعمال معطياته الشخصية وأيضا في حالة تعنت المؤسسات ورفض تقديم نسخة من هذه المعطيات.

إن ضرورة التكيف مع التطور التكنولوجي في مختلف المجالات لاسيما في الجوانب المعلوماتية فرض خلق بيئة تشريعية واجتماعية يجتمع فيها عديد المتداخلين لتأطير معالجة وحماية مختلف المعطيات الشخصية داخليا وخارجيا نظرا لما تتسم به من حساسية قد تساهم بطريقة أو بأخرى في المساس بالأمن القومي، الأمر الذي يقتضي توفير مختلف الضمانات لخلق بيئة آمنة تضمن فيها خصوصية الأفراد وحسن التعامل ومعالجة معطياتهم الشخصية باعتبار حمايتها حق يضمنه الدستور التونسي.

المراجع:

- https://www.cdp.sn/sites/default/files/doc/Recueil_INPDP.pdf
- http://www.inpdp.nat.tn
- https://www.youtube.com/channel/UCEwCeSiM0pszPm_xrpJXCIA/videos
- https://www.facebook.com/INPDP.TN/

الهجمات السيبرنية المتقدمة الموجّهة: الواقع والتحديات المطروحة

العقيد حسن الكشوطي

يشهد العالم اليوم تطورا سريعا للرقمنة في عدة مجالات، اقتصادية، اجتماعية وخدماتية حول الفضاء السيبرني، حيث أصبحنا نتحدث عن الاقتصاد الرقمي، المجتمع الرقمي، الخدمات عبر الأنترنات، عن تطبيقات متعددة ومتنوعة على الخوادم وخاصة الهواتف المحمولة والأشياء المتصلة بالأنترنات. هنالك تحول في استعمال الأنترنات والرقمنة وخير دليل على ذلك أزمة كوفيد - 19 والدور الذي لعبته الرقمنة وتطبيقاتها في الحدّ من تداعيات هذا الوباء على الأفراد، العائلات المجتمع، المؤسسات والدول. بالتوازي صاحب هذا التحول في استعمال الأنترنات والرقمنة تهديدات ومخاطر تتطور بسرعة كبيرة منها هجمات على أجهزة الحواسيب ومحطات العمل، اختراق شبكات، تعطيل عمل خوادم، سرقة بيانات وغيرها من الأضرار. لقد بلغت الهجمات السيبرنية مستوى عالي من الحرفية حيث ظهر ما يسمى بالهجمات السيبرنية المتقدمة الموجّهة وهي هجمات تستهدف النظم المعلوماتية والبنى التحتية الرقمية الحيوية والتي تتسبّب في أضرار عميقة شبيهة بالكوارث الطبيعية. من هنا تطرح إشكالية رئيسية لهذا المقال: انطلاقا من أمثلة وحقائق لهجمات سيبرنية متقدّمة في العالم، فماهي التحديات المطروحة وماهي أبرز المقاربات التي يمكن اعتمادها في مجال الأمن والدفاع السيبرني لمجابهة هذا النوع من الهجمات والحدّ منها؟.

1. الهجمات السيبرنية المتقدمة:

أصبح الفضاء السيبرني مساحة تنفّذ فيه أو بواسطته هجمات سيبرنية متقدمة وموجهة ذات حرفية عالية لها انعكاسات وخيمة على النظم المعلوماتية والبنى التحتية الحيوية حيث وجب حماية هذه النظم والبنى في إطار رؤية واضحة ومقاربة متكاملة في مجال الأمن والدفاع السيبرني.

إن الهجمات السيبرنية المتقدمة الموجهة هي هجمات مختلفة عن الهجمات السيبرنية التقليدية حيث أنها تستعمل تقنيات متطوّرة وتستهدف مؤسسات قطاعية إستراتجية كالشركات الكبرى، والدول والحكومات، مما يتسبب في أضرار عميقة كالتوقّف عن العمل أو تدّمير للبنى التحتية التي تعتمد تكنولوجيات المعلومات والاتصال، أنظمة التحكّم الآلي، والخدمات على الخط. يمكّن هذا النوع من الهجمات من الولوج داخل النظم والتواجد دون التفطن إلى ذلك بصفة مبكرة (في حالة ركود وانتظار).

2. أمثلة لهجمات سيبرنية متقدمة موجّهة وقعت في العالم:

1.2 هجمة سيبرنية واسعة على إستونيا:

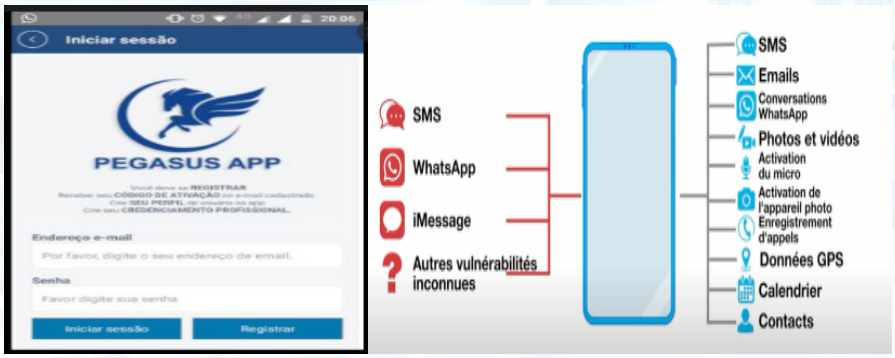
أبرز مثال لنوعية هذه الهجمات هو ما وقع في إستونيا سنة 2007 حيث تعرّض هذا البلد إلى هجمة سيبرنية متقدمة موسّعة على مواقع مرقمنة للحكومة والرئاسة والوزارات والبنوك ومؤسسات إعلامية كبرى عن طريق ضخّ كمية هائلة من البيانات الوهميّة وإرسالها في نفس الوقت إلى الخوادم مما تسبّب في تعطيلها وتوقّف عديد الخدمات المؤسساتية العمومية والمصرفية لعدة أيام وشلل شبه كلي للعديد من الخدمات الحيوية. للتذكير فإنّ أستونيا بلد رائد في استخدام الأنترنات (تحصلت على استقلالها من روسيا سنة 1991)، قرابة 99% من خدماتها الإدارية هي خدمات على الخط، معرّف وحيد لكل مواطن ومكتبية محوسبة بالكامل(صفر ورق). اعتبرت إستونيا هذه الهجمة عملا حربيا باعتماد مواصفات الهجمة، المدّة والهياكل المستهدفة والأضرار التي خلّفتها.

2.2 هجمة سيبرنية متقدمة على مؤسسات أمريكية حسّاسة:

مثال آخر لهجمة سيبرنية متقدمة وقعت سنة 2020 وشملت مؤسسات أمريكية حسّاسة حيث نجح متسلّلون في إخفاء شفرة خبيثة داخل نسخة تحديث برمجية (SolarWinds Orion) صدرت بين مارس وجوان 2020. وهي برمجية مشابهة لنظام تشغيل تسهّل استعمال الشبكات ومستعملة بكثرة في الولايات المتحدة الأمريكية. تسمح الشفرة الخبيثة للمهاجم بتنفيذ تعليمات عن بعد واستخراج بيانات. من بين الهياكل المستهدفة وزارة الخزينة والطاقة والتجارة، الإدارة المركزية للاتصالات، البحرية، البيت الأبيض وقائمة كبيرة من الحرفاء (18 ألف).

3.2 برمجية اختراق الهواتف المحمولة:

لا يفوتنا في هذا الصدد، ذكر نوع من البرمجيات المستعملة لاختراق الهواتف المحمولة على غرار برمجية (Pegasus) وهي مصنعة من طرف شركة إسرائيلية (NSO Group) والتي تمكّن مستخدميها من النفاذ إلى الملفات والبيانات، الصّور، كلمات المرور، التنصّت، التسجيل بالصوت والصورة والتي يمكن توظيفها في مرحلة مهّدة لعملية سيبرنية متقدمة موجّهة.



4.2 هجمات سيبرنية ذات حرفية عالية على منشآت وبنى تحتية إيرانية:

يغطي هذا المثال هجمة سيبرنية متقدمة حدثت في أكتوبر 2021 وكانت موجهة نحو البنى التحتية للتزود بالبنزين في إيران حيث تسببت في شلل تامّ لعديد محطات التوزيع وعدم تمكّن حوالي 60 مليون إيراني من شراء البنزين المدعّم. تتجه أصابع الاتهام إلى مجموعة معارضة مدعومة من دول كبرى. ولا يفوتنا في هذا الصدد، التذكير بما يعرف بهجمة ستوكسنات (Stuxnet) على المفاعل النووي الإيراني التي وقعت سنة 2010 والتي اعتمدت على إدخال برمجيّة خبيثة (malware) باستعمال طرق الهندسة الاجتماعية (Social Engineering) للتحكم عن بعد في أجهزة ونظم آلية. أسفرت الهجمة عن تلف في أجهزة الطرد المركزي لتخصيب الأورانيوم وتأخير في تنفيذ البرنامج النووي الإيراني.

3. الهجمات السيبرنية المتقدمة الموجّهة، واقع ومجال إستراتيجي:

لقد فرضت مثل هذه الهجمات السيبرنية المتقدمة الموجهة واقعا وتحديات جديدة في علاقة بالفضاء السيبرني. أول تحدّي يكمن في الميزة الجيوسياسية التي اكتسبها الفضاء السيبرني، فهو فضاء يمهّد للعلاقات والصراعات ويحوي عديد المتدخلين على مستوى فردي، جماعي، محلي، إقليمي ودولي. نشأت مجموعات مدعومة من الحكومات وأجهزة الاستخبارات مع تواجد المشغّلين العمالقة للتكنولوجيات الحديثة الخواص مثل شركات قوقل، فايسبوك، أمزون وميكروسوفت. في البداية اقتصرت الرقمنة على نظم المعلومات والاتصالات ثم امتدت إلى النظم الآلية الصناعية (SCADA) وفي مجال الدفاع إلى الأنظمة والأسلحة الحديثة. يمكن اعتبار أي هجمة سيبرنية متقدمة موجهة على البنى التحتية الحيوية تمثل تهديدا بالغ الأهمية للحكومات والبلدان. وطبقا لذلك بات الفضاء السيبرني يمثل أهمية بالغة للدول والتحالفات، ولعل أبرز مثال للاهتمام الدولي بالفضاء السيبرني هو منظمة حلف الشمال الأطلسي أو ما يعرف بالناتو (OTAN). ففي سنة 2008 تمّ إحداث أول إستراتجية دفاع سيبرني اعتمدتها هذه المنظمة، وفي سنة 2014 اعترف أعضاء هذا الحلف بالدفاع السيبرني كجزء من الدفاع الجماعي وفي سنة 2016 اعترف أعضاء هذا الهيكل بالفضاء السيبرني كمجال مدمج للعمليات العسكرية. إن أي هجوم سيبرني كبير وحسب الضرر الجسيم الذي يسبّبه، يمكن أن يشكل عدوانا مسلحا بالمعنى المقصود في المادة 51 من ميثاق الأمم المتحدة، وبالتالي يبرّر الاحتجاج بالدفاع عن النفس. من جهة أخرى وفي سياق نزاع مسلّح، يخضع تخطيط وتنفيذ العمليات السيبرنية التي يمكن اعتبارها هجمات إلى موجب القانون الدولي الإنساني. بالفعل، فهنالك تفاعلات متعددة بين الفضاء السيبرني والفضاءات الأخرى (الأرض،الجو،البحر) فهو يمثل مساحة عرضية بين كل الفضاءات مما يسمح بالوصول إليها جميعا باستعمال التكنولوجيا الرقمية الجدّ متطورة. على سبيل المثال إن فرقاطة بحرية حديثة يمكن أن تحوي 2000 تطبيقه حاسوب، 300 جهاز حوسبة و25 مليون سطر من التعليمات البرمجية لتشغيل أنظمة قتالية. وفي مجال الطيران نظمت وزارة الدفاع الأمركية مسابقة (hackaton) في أوت 2019، سمح فيها لمجموعة من القراصنة السيبرنيين القيام بمحاولة اختراق أمن طائرة مقاتلة من نوع (F15). لم يمض يومين فقط للتوصل لاكتشاف ثغرة في نظام التحكم في الطائرة من طرف القراصنة. بالتوازي في الحياة المدنية، العالم آخذ في التحضّر. فبحلول سنة 2050، من المتوقع أن أكثر من ثلثي سكان العالم سيتواجدون في المدن. 40 مدينة كبيرة ستستوعب أكثر من 20 مليون نسمة، أكثر من مليون كائن متّصل لكل متر مربع و38 عنصر ذكي لكل ساكن. إنّه تحدّي حقيقي للسلط والحكومات وأجهزة الأمن والدفاع الشامل. إن تواجد الرقمنة في بنى تحتية حساسة كالخدمات على الخط وأنظمة صناعية لتوزيع الكهرباء والماء والأنظمة الصحية، والنقل وأنظمة الدفاع

البري والجوي والبحري وغيرها يرتقي بمثل هذه النظم إلى مستوى نقاط حساسة يجب حمايتها والدفاع عنها لأنها قد تصبح أهدافا أمنية أوعسكرية عند نشوب حرب أو صراعات داخلية أو استغلالها من طرف الإرهابيين. فاكتساح الرقمنة للمجالات الحياتية للمواطن والحكومات وزيادة إدماجها في الأجهزة العملياتية والصناعية كالطيران والمعدات العسكرية بصفة عامة فرض واقعا جديدا وجب التفكير فيه والإعداد له بجدية. إن التعامل مع الهجمات السيبرنية المتقدّمة الموجّهة يمرّ حتما عبر مقاربة أو إستراتجية واقعية واضحة المعالم في مستوى أول في مجال الأمن السيبرني وفي مستوى ثاني في مجال الدفاع السيبرني. تضبط هذه الإستراتجيات الأهداف المرسومة، السياسات الأمنية الممكن اتباعها لتحقيق الأهداف، الهيكلة، الأدوار والمهام التي توكل إلى جميع المتدخلين.

المراجع

- Connaissance de la menace avancée et du cyber espionnage
- European Security and défense 4/2019
- Qualité et gouvernance des systèmes d'informations
- La gestion des risques pour les systèmes d'informations
- Revue de cyber défense « RAIDS N°386 »
- Des sites sur Internet :
- https://www.senat.fr/rap/r11-681/r11-681_mono.html
- https://www.developpez.com/actu/21459/Le-tres-complexe-virus-Stuxnet-attaque-les-infrastructures-industrielles-de-l-Iran-qui-evoque-une-guerre-electronique/
- https://www.ege.fr/infoguerre/la-cyber-attaque-solarwinds-contre-les-etats-unis
-https://www.france24.com/fr/am%C3%A9riques/20211103-cyberespionnage-washington-place-le-logiciel-isra%C3%A9lien-pegasus-sur-liste-noire
-https://www.cnews.fr/vie-numerique/2019-08-21/des-hackers-piratent-un-avion-de-chasse-f-15-et-en-prennent-le-controle
-https://www.usinenouvelle.com/article/les-navires-de-guerre-nouvelles-cibles-des-cyber-pirates.N581808

مشروع الإدارة الإلكترونية والتحول الرقمي

الوكيل أعلى بالبحرية الصحبي السبري

تماشيًا مع الثورة الصناعية الرابعة وما تقدّمه من تقنيات حديثة وفعّالة في تحسين الأداء وجودة العمل، توجّهت أغلب الدّول إلى تطويع هذه التقنيات واستخدامها بما يتناسب واحتياجاتها المتعدّدة. ومن أبرز ما جاءت به هذه الثورة، هي الحوسبة السحابية وتقنية البلوك تشين Blockchain والذكاء الاصطناعي وإنترنت الأشياء، وأهم ما يميّزها هو إمكانية استخدامها في كافة المجالات والقطاعات.

لم يقتصر استخدام هذه التقنيات على الشركات أو المؤسسات الخاصة، وإنما بادر القطاع الحكومي ومؤسساته باستخدامها في تحويل خدماتها التقليدية إلى خدمات إلكترونية متطورة، وهو ما ساهم في مرونة الخدمات الإدارية حيث أصبحت الرقمنة أو الإدارة الرقمية أمرا حتميا على الوزارات و المؤسسات العمومية.

تتسابق أغلب الدول نحو الرقمنة الإدارية لدعم الاستثمار ومواكبة الطرق العصرية التي تقدم تسهيلات إدارية للمستثمرين في جميع القطاعات الحيوية، حيث انطلقت الدولة التونسية كسائر الدول في مشروع التحول الرقمي أو "الحكومة الذكية Smart Gov 2020" لتحديث وعصرنة الإدارة بهدف توفير مناخ رقمي مرن يعمل على تحقيق خدمات أفضل للمواطنين والمؤسسات. فما هو مفهوم وأهداف هذه الإدارة الرقمية؟ وماهي تحديات مشروع التحول الرقمي؟

1. مفهوم وخصائص الإدارة الرقمية:

يعرّف بعض الباحثين الإدارة الرقمية (أو الإلكترونية) على أنها العملية الإدارية القائمة على استخدام تكنولوجيا المعلومات والاتصال ضمن منظومات للقيام بوظائفها إلكترونيا قصد تطوير الأداء وتحقيق أهداف المؤسسة. كما يتم تعريفها على أنها عملية تحويل كافة الأعمال والخدمات الإدارية التقليدية إلى خدمات إلكترونية تنفّذ بدقّة وسرعة عالية ودون استخدام الأوراق والطرق البيروقراطية القديمة.

الفرق بين الإدارة التقليدية والإدارة الإلكترونية

المعيار	الإدارة التقليدية	الإدارة الإلكترونية
الوسيلة المستخدمة	الاتصالات المباشرة والمراسلات الورقية	شبكات الاتصال الإلكترونية
الوثائق	أوراق	لا أوراق
الحفظ	ملف ورقي	ملف إلكتروني
الوصول للبيانات	صعوبة البحث في الأرشيف الورقي	سهولة البحث في قواعد البيانات
الحماية	حماية أقل، لا توجد نظم حماية	حماية عالية عن طريق نظم أمن المعلومات
الاستجابة	بطيئة وروتينية	سريعة
التكلفة	مكلفة على المدى البعيد	اقتصادية على المدى البعيد
نوع التنظيم	هرمي جامد	شبكي مرن
مدة الخدمة	ساعات العمل	24/7 إلى حد ما
الجودة	أقل	عالية

1.1 مراحل تطور الإدارة الرقمية:

شهد تحويل ورقمنة الخدمات الإدارية التقليدية إلى خدمات إلكترونية حديثة عدّة مراحل، حيث كان الإنسان هو العامل الأساسي في الإنتاج لما يمتلكه من حرفية في الآداء الإداري. ومع مرور الوقت تم في مرحلة أولى تألية بعض الأعمال التي كان ينجزها الإنسان، ثم بعد التطور الملحوظ في البرمجيات ومنظومات الإعلاميّة أصبحت الآلة في خطوة ثانية تقوم بكل الأعمال المرتبطة بالتخطيط والمراقبة والتنظيم.
في مرحلة ثالثة، ساهم الذكاء الاصطناعي في تنمية قدرات الأنظمة المعلوماتية حتى أصبح النظام المعلوماتي يحاكي الذكاء والسلوك الإنساني في التعامل مع المسائل الإداريّة.
وكمرحلة أخيرة وقصد توفير الخدمات للمواطن والمؤسسات مثّلت الأنترنات بوابة الوصول إلى الخدمات الإدارية عن بعد وساهم تشبيكها العنكبوتي في نقل ومعالجة وتخزين البيانات رقميا.

2.1 خصائص الإدارة الرقمية:

تتميز الإدارة الرقمية عن الإدارة التقليدية بعديد الخصائص التي جعلت منها مستقبل الإدارة والأعمال والاستثمار في أغلب الدول المتقدمة وذلك من خلال :
1. **السرعة والوضوح**: الكفاءة والفاعلية في تسيير العمل الافتراضي والقدرة على تحقيق أعلى درجات السرعة في الأداء بتوفير الوقت ووضوح مراحل المعالجة.
2. **المرونة**: توفير مرونة عالية جدا لأن العمل يعتمد على أنظمة معلومات واتصال رقمي يمكّن من التنسيق وتبادل البيانات بين مختلف الأطراف المساهمة في اتخاذ

القرار وأصبح غير حكر على بعض الأشخاص أو الهياكل.

3. **مكان عمل افتراضي**: يستطيع الموظفون الدخول إلى النظم المعلوماتية عن بعد و إنجاز العمل دون حدود زمانية أو مكانية.

4. **تبادل وتشارك المعطيات**: إدارة متشابكة تتيح التعامل البيني والتبادل الإلكتروني.

5. **أمن المعلومات**: القدرة على توفير مستوى عالي من الحماية إضافة إلى القدرة على تحديد صلاحيات الموظفين في الاطلاع على ما هو مخول لهم من البيانات.

6. **إدارة المعلومات بدلا من حفظها**: ليس الهدف تكديس الملفات بل معالجتها ثمّ حفظها على شبكة المعلومات.

7. **الرقابة المباشرة**: القدرة على متابعة العمل في كل المواقع عن بعد.

8. **الشفافية**: تتمّ معالجة الملفات بصفة آلية أي دون محسوبية أو تدخل بشري للتأثير على القرار علاوة على القدرة على الرقابة الدورية. حيث تمثل على سبيل المثال منظومة الشراءات العمومية على الخط TUNEPS خطوة حاسمة في مسار إضفاء الشفافية على الصفقات العمومية.

2. أهمية وتحديات مشروع التحول الرقمي:

تسعى الدولة التونسية بكل هياكلها إلى إنجاح مشروع التحول الرقمي وذلك لما له من أهمية على مستوى المجتمع (المواطن) والمؤسسات:

- **أهمية الإدارة الرقمية على مستوى المجتمع:**

تساهم رقمنة الإدارة في توفير معلومات دقيقة وموثوقة ومتاحة على مدار الساعة إضافة إلى الحد قدر الإمكان من تأثير العلاقة الشخصية في تنفيذ أو إنجاز المصلحة أو الخدمة الإدارية.

تساهم الإدارة الرقمية في إيجاد فرص جديدة للعمل وذلك من خلال قدرة الأشخاص على التواصل مع المؤسسات الوطنية والعالمية بكل سهولة وتجنب عناء التنقل.

- **أهمية الإدارة الرقمية على مستوى المؤسسات:**

ساهمت رقمنة الإدارة في تحسين أداء الإدارات وتقديم الخدمات وتسهيل الإجراءات للحصول على الخدمات وذلك بتقليل التعقيدات الإدارية من خلال إلغاء المستويات الإدارية والانتقال من التنظيم الهرمي إلى التنظيم الشبكي.

تعتبر الإدارة الرقمية سببا في إتساع نطاق الأسواق والأعمال والانفتاح على أسواق عالمية وكسب ثقة العملاء أو المواطنين وذلك من خلال تغيير صورة المؤسسة من الشكل التقليدي إلى الرقمي الذي يواكب عصر التكنولوجيا.

من أهم التأثيرات الإيجابية للإدارة الرقمية على المؤسسات هي تخفيض التكاليف والتقليل من حجم المصاريف التي يتم إهدارها على النظام الورقي علاوة على التقليل بشكل كبير في نسبة الأخطاء البشرية

بسبب وجود قواعد بيانات يتم الاعتماد عليها في التخطيط واتخاذ القرار، حيث أن الإدارة الحديثة تقوم على توفير المعلومات بشكل مستمر لجميع الأقسام والمصالح داخل المؤسسة وهو ما يتجاوز عوائق النظام الإداري المركزي.

• **تحديات مشروع التحول الرقمي أو رقمنة الإدارة:**

هناك مجموعة من الصعوبات والعوائق التي تؤخر تنفيذ مشروع التحول الرقمي في الإدارات التونسية والمؤسسات الخاصة ومن ذلك نذكر :

• صعوبة تأقلم الموظفين مع التغيرات الإلكترونية الجديدة.

• عدم توفر الموارد المالية اللازمة لتنفيذ مشروع الإدارة الرقمية.

• عدم توفر إطار قانوني يغطي أو ينظم الإدارة الإلكترونية ويضمن حق المواطنين أو العملاء.

• ضعف البنية التحتيّة للاتصال وتكنولوجيا المعلومات للإدارات أو لمزودي خدمات الأنترنات في بعض المناطق.

• مقاومة هائلة من الموظفين الذين يخشون على عملهم المستقبلي جراء تبسيط الإجراءات، إضافة إلى الحد من نفوذهم الذي يتحكمون به في الإدارة التقليدية.

هذا، وفي صورة النجاح في تنفيذ مشروع التحول الرقمي، فإن الإدارة الإلكترونية لا تخلو من بعض التحديات على غرار تأمين البيانات التي يمكن أن تتعرض إلى عمليات اختراق، حيث أن الأنظمة المعلوماتيّة ستصبح هي العمود الفقري والحيوي لكل مؤسسة أو إدارة مما يجعل تعطيلها سبب في انقطاع العمل وعدم توفر الخدمات، علاوة على أن أي عملية سرقة للبيانات قد تعرض الإدارة أو الشركة إلى أضرار مادية جسيمة وتتبعات قانونية متعلّقة بحماية المعطيات الشخصية للعملاء والشركاء. علاوة على ذلك ستتكبد الإدارات والمؤسسات تكاليف إضافية خاصة بصيانة المعدات الإلكترونية والبرمجيات وتأمين السلامة المعلوماتيّة لهذه الأنظمة.

لقد بدأت تونس مرحلتها الرقمية بشكل جيد ولكنها لا تزال بعيدة عن الرقمنة الكاملة التي تكون فيها الخدمات بسيطة ومتجانسة وشفافة وغير مادية تمامًا. وعلى الرغم من أن برنامج الحكومة الإلكترونية "e-GOV" في تونس يشهد تقدمًا كبيرًا من عام إلى آخر، إلا أنه يجب بذل جهود إضافية لتحسين وتطوير الخدمات الإدارية المتاحة للمواطن عبر شبكة الإنترنت.

TUNISIA DIGITAL SUMMIT

المراجع:

-الإدارة-الإلكترونيّة-في-تونس

- http://www.itceq.tn/files/innovation-Tic/2021/le-gov-a-l-ere-du-digital.pdf

-https://www.mtc.gov.tn/index.php?id=119&tx_ttnews%5Btt_news%5D=4090&cHash=b-7be34580a7295318a6441a913575cc3

- http://www.pm.gov.tn/pm/actualites/actualite.php?id=13214&lang=ar

- http://www.tunisie.gov.tn/117

التعدين الخفي «CryptoJacking»

الوكيل أحمد القاسمي

تشهد العملات الرقمية منذ سنة 2013 ارتفاعا كبيرا في قيمتها المالية على رأسها عملة «Bitcoin» التي تجاوزت 180 مليونا بالدينار التونسي سنة 2021 وفي المقابل تضاعفت تكلفة إنتاجها وتعدينها بإعتبار الطاقة الكهربائية الكبيرة التي تستهلكها الحواسيب والأجهزة الإلكترونية في التعدين. كل هذه العوامل أدت إلى ارتفاع معدل الهجمات الإلكترونية على الأجهزة المرتبطة بشبكة الأنترنات (الحواسيب، الهواتف الذكية، الخوادم والموزعات) واستغلال مواردها بصفة خفية في تعدين العملات الرقمية المشفرة بغاية الربح المادي.

1. مفهوم التعدين الخفي:

يعتبر التعدين الخفي (CryptoJacking) نوع من الجرائم الإلكترونية التي تهدف إلى الاستغلال غير المشروع لموارد أجهزة الضحايا (وحدة المعالجة المركزية CPU، الذاكرة العشوائية RAM، معالج بطاقة الغرافيك) في تعدين العملات الرقمية دون علمهم من خلال حقن الأجهزة المرتبطة بالأنترنات ببرامج خبيثة تعمل تلقائيا أثناء استخدام الضحية لجهازه وتقوم بعمليات حسابية معقدة وإرسالها على شبكات Blockchain.

2. طريقة عمل CryptoJacking:

يمكن استهداف حاسوب الضحيّة وحقنه ببرامج التعدين الخفي باتباع إحدى التقنيات التالية:

• تفخيخ موقع إلكتروني أو إعلانات (Adds) ببرامج جافا سكريبت الذي يقوم باختراق جهاز الضحية (دون حاجة إلى تحميله) ثم يقوم بالتعدين تلقائيا على متصفح الأنترنات (Navigateur).

• تصيد الضحايا وخداعهم عبر إرسال بريد إلكتروني يحمل روابط خبيثة تحتوي شفرة تعدين تعمل كذلك تلقائيا على متصفح الأنترنات.

هذا، وتتواصل عملية التعدين الخفي طوال فترة تواجد البرنامج الخبيث على متصفح الأنترنات.

3. الأضرار التي تقع على الجهاز عند استغلاله في التعدين:

يستنزف قراصنة العملات الرقمية موارد أجهزة الضحايا باعتبار أن عملية التعدين تتطلب زيادة في استخدام معالج (Processeur) جهاز الضحية مما يؤدي إلى:

• إرتفاع درجة حرارة الجهاز مما يسرّع في إتلافه.

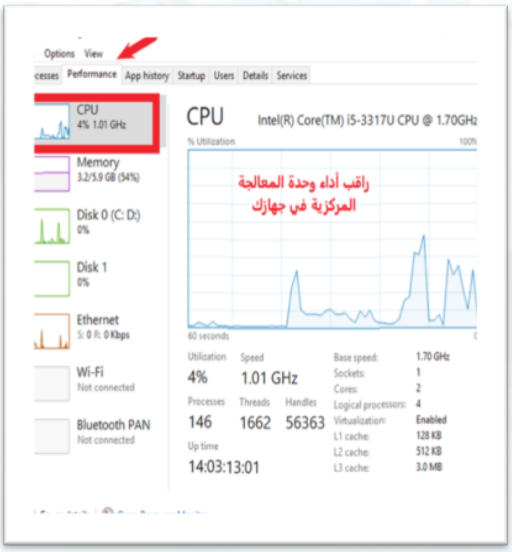
- تباطؤ ملحوظ في أداء الجهاز.
- إمكانية حرق المعالج الخاص بجهاز الضحية.
- توقف متكرر للجهاز بسبب نقص قوة المعالج المتاحة.
- الاستهلاك الكبير للطاقة الكهربائية.

4. طرق حماية الأجهزة من CryptoJacking:

نظرا لصعوبة اكتشاف هجمات التعدين الخفي من قبل الضحايا يجب عليهم الالتزام بـ :

- تثبيت أدوات منع الإعلانات (AdBlock Plus) على متصفح الأنترنات التي تعمل على كشف ومنع عمل برامج التعدين.
- تنزيل إضافات على متصفحات الواب لمنع التعدين على غرار «No-MinerBlock»، «No-Miner» و«NoCoin».
- تجنب الولوج إلى المواقع المشبوهة وفتح الروابط المفخخة.
- المراقبة الدورية لنشاط وحدة المعالجة المركزية عبر «Manager Task».
- تثبيت أخر تحديثات البرامج وتصحيحات نظام التشغيل والتطبيقات المستغلة.

عموما، تعتبر هجمات التعدين الخفي (CryptoJacking) من أخطر هجمات الأنترنات لأنها تستغل جهاز الضحية دون موافقته أو علمه بالإضافة إلى سهولة التفصي من المراقبة. كما تشهد هذه الظاهرة إرتفاعا كبيرا مع كل سنة جديدة ارتباطا بإرتفاع القيمة المالية للعملات الرقمية ولاعتبارها طريقة سهلة وغير مكلفة لمجرمي الأنترنات لكسب المال.



المراجع:

- interpol.int/Crimes/Cybercrime/Cryptojacking
- kaspersky.com/resource-center/definitions/what-is-cryptojacking
- fr.malwarebytes.com/cryptojacking/
- avast.com/c-protect-yourself-from-cryptojacking
- hp.com/us-en/shop/tech-takes/what-is-cryptojacking

النقيب خالد الرحال

تكنولوجيا NFC (Smart Ring)

يشهد العالم اليوم تطورا على عديد الأصعدة والمجالات وخاصة منها مجال الصناعات والابتكارات في مجال تكنولوجيا المعلومات والاتصالات ونذكر منها الخاتم الذكي (Ring Smart) الذي يستخدم تقنية NFC (Near Field Communication) ويعتبر مستقبل التكنولوجيا المحمولة على غرار الساعات الذكية نظرًا لتصميمه المبتكر وتوفيره للعديد من الخدمات. سنتطرق في هذا المقال إلى تعريف تقنية NFC ومختلف مجالات استخدام الخاتم الذكي والتحديات المرتبطة بمجال سلامة أمن المعلومات باستخدام هذه التقنيات.

1. ما هي تقنية NFC؟

تمثل تقنية الاتصال قريب المدى، تقنية لاسلكيّة تمكّن من الاتصال بأي محطة دون الحاجة إلى تطبيقات أو برمجيات وهي مشتقة من تقنية (Radio Frequency Identification) RFID.

2. تعريف الخاتم الذكي (Smart Ring):

الخاتم الذكي هو عبارة عن جهاز إلكتروني يتم ارتداؤه في أصابع اليد عادة ما يكون بحجم الحلقات التقليدية أو أكبر قليلا. يوفّر الخاتم الذكي عدة خدمات مثل القدرة على تخزين المعلومات والدفع الإلكتروني ومتابعة الأنشطة الرياضية. كما تتمتع معظم الخواتم الذكية بقدرات تسمح بالتحكّم في الهاتف الذكي والأجهزة الأخرى مثل ضبط التنبيهات أو تلقي إشعارات الرسائل أو المكالمات أو التحكم في الموسيقى.

3. مجالات استخدام الخاتم الذكي:

يمكن استخدام الخاتم الذكي في مجموعة من المجالات نذكر منها:

1.3 مراقبة النفاذ:

يمكن استخدام الخاتم الذكي كوسيلة تعرّف للنفاذ إلى المكاتب والمنازل والسيارة التي تعتمد تقنية مراقبة النفاذ (Access Control)، بدلاً من استخدام مفتاح مادي تقليدي أو بطاقة وصول، حيث يتمّ استعمال مستشعر بصري يمكّن من عملية التعارف بين جهاز مراقبة النفاذ والخاتم الذكي.

2.3 متابعة اللياقة البدنية:

يمكّن الخاتم الذكي من مراقبة الأنشطة اليومية، بما في ذلك عدد الخطوات والمسافات المقطوعة أثناء المشي أو العدو والسعرات الحرارية المحروقة ومعدل دقات القلب ومستويات الأكسجين في الدم وغيرها.

3.3 خدمة الدفع الإلكتروني:

تعتبر خدمة الدفع الإلكتروني من أهم الخدمات الخاصة التي توفرها الخواتم الذكية من ناحية الاستعمال. تمكّن الخدمة المذكورة مستعمل الخاتم الذكي من القيام بعمليات الدفع وتحويل الأموال دون الحاجة إلى تطبيق معين أو بطاقات الدفع البنكية. اتجهت البنوك والمؤسسات المالية في بعض الدول على غرار المملكة المتحدة واليابان وفرنسا إلى اعتماد هذه الخدمة خاصة في ظل تنامي جائحة كورونا قصد ترسيخ مبدأ التباعد الاجتماعي في عمليات الدفع.

4.3 مراقبة النوم:

يرصد الخاتم الذكي معدل نبضات القلب والتنفس ودرجة حرارة الجسم وحركته حيث يتمّ إرسال وتخزين البيانات المذكورة إلى تطبيق على الهاتف الذكي يقوم فيما بعد بتحليل ودراسة البيانات المرسلة وتقديم نصائح للحصول على نوم أفضل.

4. مخاطر تكنولوجيا الخاتم الذكي:

كغيرها من التكنولوجيات الحديثة تحتوي الخواتم الذكية على العديد من الثغرات كما أنها عرضة للاختراقات والمخاطر السيبرنيّة خاصة في ما يتعلّق بسرقة المعطيات الشخصية.

تكمن الهجمات المستهدفة لهذه التكنولوجيا بالأساس في إمكانية استغلال المخترقين لبرمجيات قرصنة يتمّ ارسالها إلى الخواتم الذكية قصد سرقة معطيات نفاذ (الأبواب، دفع إلكتروني...) وسرقة المعطيات الشخصية واختراق أنظمة الدفع الإلكتروني لهذه الخواتم.

وعليه يجب اتخاذ عدة تدابير وقائية نذكر منها:

- عدم مشاركة معطيات التعارف،
- تغيير معطيات التعارف والولوج دوريا،
- التحيين الدوري والمستمر لجميع الأنظمة المشغلة،
- استعمال تقنية التعارف المزدوج «two-factor Authentification».

Smart ring

المراجع:

- https://www.unitag.io/fr/nfc/what-is-nfc
- https://smartringnews.com/posts/

الأمن السيبرني في تونس

الرائد نادية الفزعي

أصبح العالم اليوم يعيش سباق تسلح سيبرني غير مسبوق حيث ساهم تطور تكنولوجيات المعلومات والاتصال وانتشار أجهزة أنترنات الأشياء وشبكات الجيل الخامس المتطورة في تنامي التهديدات السيبرنية وهو ما أدى إلى تزايد مساعي الدول لتعزيز إمكانياتها لحماية فضاءها السيبرني. في ذات السياق عملت الدولة التونسية جاهدة إلى تطوير قدراتها بهدف تدعيم مناعة مؤسساتها الحساسة والحيوية من هذه التهديدات من خلال هياكل وطنية تعنى بحماية الفضاء السيبرني تقنيا وقانونيا.

لتقييم مدى جاهزية الدول أصدر الإتّحاد الدّولي للاتّصالات التّابع للأمم المتّحدة مؤشّر الأمن السّيبرني العالمي «Global Cybersecurity Index» الذي يعرض مستوى التزام الدّول الأعضاء فيه في مجال الأمن السّيبرني من خلال مجموعة من معايير التّقييم على غرار التّدابير القانونيّة والتّنظيميّة والتّقنيّة وتنمية القدرات والتّعاون الدّولي وقد احتلت تونس المرتبة 45 عالميا لسنة 2020 ضمن ترتيب المؤشر الخاص بالأمن السيبرني العالمي «Global Cyber Security Index» من أصل 192 دولة، بحسب التقرير الذّي نشره الاتحاد الدولي للاتصالات، علما وان تصنيف تونس كان ضمن المرتبة 76 في سنة 2018. كما احتلت المرتبة الخامسة إفريقيا والسادسة عربيا. ويرتكز المؤشر على خمسة ركائز للأمن السيبرني في كل بلد وهي التدابير القانونية،الفنية،التنظيمية،تدابير بناء القدرات وتدابير التعاون.

ورغم هذا التحسن على مستوى التصنيف،لا تزال تونس تواجه جملة من التحديات أساسًا في العديد من المؤسسات البنكية والمصرفية والشّركات في القطاعين العام والخاص في ظل تطور الهجمات الإلكترونية وقرصنة مواقع العديد من المؤسسات العمومية. وهو ما دعى رئاسة الحكومة مؤخرًا إلى التأكيد على ضرورة تعيين مسؤولين عن السلامة المعلوماتية بالوزارات والوكالات والهيئات الوطنيّة توكل لهم مهمة السهر على سلامة الأنظمة المعلوماتية بالتنسيق مع الهياكل المسؤولة على السّلامة المعلوماتيّة في تونس والتي من أهمها الوكالة الوطنية للسلامة المعلوماتية والوكالة الفنية للاتصالات والوكالة الوطنية للمصادقة الإلكترونية.

1. الهياكل المسؤولة على السّلامة المعلوماتيّة في تونس:

تضم تونس عدّة هياكل تنشط في مجال السلامة المعلوماتية، على غرار الوكالة الوطنية للسلامة المعلوماتية والوكالة الفنية للاتصالات والوكالة الوطنية للمصادقة

الإلكترونية والوكالة الوطنية للترددات والوكالة التونسية للأنترنات والهيئة الوطنية للاتصالات والهيئة الوطنية لحماية المعطيات الشخصية. وفي ما يلي لمحة على الوكالات المسؤولة على السلامة المعلوماتية:

1.1 الوكالة الوطنية للسلامة المعلوماتية:

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

تعمل هذه الوكالة منذ إحداثها على وضع مقاييس خاصة بالسلامة المعلوماتية وإعداد أدلة فنيّة في الغرض والعمل على نشرها كما تعمل على تشجيع تطوير حلول وطنيّة في مجال السلامة المعلوماتيّة وإبرازها وذلك وفق الآليات والبرامج التي تقوم بتجديدها. كما تقوم على مراقبة عامة للنظم المعلوماتيّة وشبكات مختلف الهياكل العمومية والخاصة.

2.1 الوكالة الفنية للاتصالات:

الوكالة الفنية للاتصالات
AGENCE TECHNIQUE DES TELECOMMUNICATIONS

توفر الدعم الفني للأبحاث العدلية في جرائم أنظمة المعلومات والاتصال وتتكفّل بتلقي ومعالجة أذون البحث ومعاينة جرائم أنظمة المعلومات والاتصال الصادرة عن السلطة القضائية طبقا للتشريع الجاري به العمل وذلك بالتنسيق مع مختلف مشغلي الشبكات العمومية للاتصالات ومشغلي شبكات النفاذ ومزودي خدمات الأنترنات كما أنها تقوم بأشغال المنظومات الوطنية لمراقبة حركة الاتصالات في إطار احترام المواثيق الدولية المتعلقة بحقوق الإنسان والأطر القانونيّة المتعلّقة بحماية المعطيات الشخصيّة.

3.1 الوكالة الوطنية للمصادقة الإلكترونية:

الوكالة الوطنية للمصادقة الإلكترونية
Agence Nationale de Certification Electronique
ANCE National Digital Certification Agency

تقوم بمنح ترخيص تعاطي نشاط مزود خدمات المصادقة الإلكترونيّة على كامل تراب الجمهورية. وتسهر على مراقبة احترام مزودي خدمات المصادقة الإلكترونية لأحكام القوانين الجاري بها العمل. كما تعمل على تحديد مواصفات منظومة إحداث الإمضاء الإلكتروني. وإبرام اتفاقيات الإشراف فيما يخص المصادقة الإلكترونية وإصدار وتسليم وحفظ شهادات المصادقة الإلكترونية الخاصة بالأعوان العموميين المؤهلين للقيام بالمبادلات الإلكترونية وذلك مباشرة أو عبر مزودي خدمات إلكترونية عموميين.

2. آليات الاستجابة للطوارئ والهجمات على المستوى الوطني:

tunCERT
Tunisian Computer Emergency ResponseTeam

تقوم الوكالة الوطنية للسلامة المعلوماتية بوضع المقاييس الخاصة بالسلامة المعلوماتية ومراقبة النظم المعلوماتية وشبكات مختلف الهياكل العمومية والخاصة عن طريق مركز الاستجابة للطوارئ المعلوماتية TunCERT.

يعمل هذا المركز على تعزيز سلامة المنظومات المعلوماتية والبنية التحتية للاتصالات والمعلومات بالجمهورية التونسية وذلك من خلال اعتماد إجراءات استباقية وجمع وتحليل المعلومات الخاصة بالحوادث السيبرنية والتنسيق بين الاطراف المعنية في معالجتها وفي صورة عدم قدرة الجهة المستهدفة على تجاوز الهجمة.

تكلف الوكالة الوطنية للسلامة المعلوماتية فريق من المختصين بالتوجه على عين المكان لجمع المعطيات اللازمة والمساندة التقنية قصد تجاوز الهجمة مع إمكانية نقل هذه المعطيات على معدات خزن لتحليل الهجمة وفهم طريقة عملها لتجنبها لاحقا.

تأتي هذه الهجمات إثر تحذير الوكالة الوطنية للسّلامة المعلوماتية خلال سنة 2022 من عمليات قرصنة عبر هجمات حجب الخدمة الموزعة كما أنّ هذه الهجمات تتم دون فّك كلمات السر أو سرقة البيانات السرية. وإنما من خلال إطلاق المهاجم لأحد البرامج التي تُحدث صعوبة في الإبحار على الموقع وتمنع بالتالي أي مستخدم آخر من الوصول إليه.

تثير عمليات القرصنة الأخيرة العديد من التساؤلات حول السلامة السيبرنية في تونس وأمن المعطيات الشخصية التي يتم تداولها في العديد من المواقع. خاصة وأنّ الوكالة الوطنية للسلامة المعلوماتية باتت تصدر بلاغات أسبوعية لتحذير التونسيين حول عمليات اختراق إلكتروني وقرصنة. لا سيّما مع تواتر عمليات إرسال روابط تدعو مستعملي الأنترنات إلى دخولها ليتسنى الاستيلاء على بياناتهم الشخصية إضافة إلى محاولة مقايضتها بمبالغ مالية تدفع للقراصنة ولذات الأسباب طالبت الوكالة الوطنية للسلامة المعلوماتية الأشخاص والمؤسسات بتحصين نظمهم المعلوماتية وعدم فتح رسائل مجهولة المصدر حتى لا يتحولوا إلى ضحايا لعمليات قرصنة.

كما دعت الوكالة إلى التأكد في كل مرّة من صحة ومصداقية الروابط الإلكترونية ومواقع الواب قبل الولوج إليها، مشددة على ضرورة اجتناب الإدلاء بأي معطى خاص أو شخصي على مواقع التواصل الاجتماعي والإنترنت.

هذا، وشهدت محاولات الاختراق والهجمات السيبرنية ارتفاعًا خلال سنوات 2019 و2020 وبداية 2021 وذلك بنسبة تتجاوز 30 بالمائة، حيث تم تسجيل ارتفاع هام في محاولات الاختراق باستعمال تقنيتي التصيد «Phishing» والبرمجيات الخبيثة «Ran-somware».

التصيد "Phishing": يقوم المخترق بإرسال رسائل إلكترونية تحتوي على روابط وملفات مصاحبة تتضمن برمجيات خبيثة عبر البريد الإلكتروني، وبمجرد أن يقوم المتلقي بفتح الرابط أو الملف المصاحب الذي يحتوي على البرمجيات الضارة، يصاب الجهاز وتنتشر عبرها الفيروسات على الشبكات الداخلية.

برمجيات الفدية الخبيثة "Ransomware": يقوم المخترق أولًا بتشفير جميع المعطيات الموجودة بالجهاز سواء كان حاسوبًا أو غيره ثم في مرحلة لاحقة يحاول الاتصال بالضحية ويطلب فدية عادة ما تكون مبالغ مالية كبيرة بالعملة الافتراضية الـ"Bitcoin" أو الدولار ويزعم أنه بتلقي الفدية المطلوبة سيقوم بموافاة الضحية برمز التشفير ويسترجع معطياته.

تبقى توصيات الوكالة المتمثلة في ضرورة توفير مخططات إستمرارية العمل ومخططات استئناف العمل بالنسبة لجميع المؤسسات لضمان الاستمرارية في حال وقوع حادث أو اختراق سيبرني طبقا للمنشور عدد23 في 5 نوفمبر 2020 (حول إحكام التصرف في الصفحات والحسابات الرسمية بشبكات التواصل الاجتماعي) والمنشور عدد 24 المؤرخ في 5 نوفمبر 2020 (حول تدعيم إجراءات السلامة المعلوماتية بالهياكل العمومية) إجراءات من الأفضل تطبيقها.

الهجمات الإلكترونية وتداعياتها

جمعية قدماء ضباط الجيش الوطني

الهجوم السيبرني (أو الإلكتروني أو هجوم الأنترنات) هو نوع من المناورة الهجومية التي تستهدف أنظمة المعلومات أو البنية التحتية أو شبكات وأجهزة الكمبيوتر. ويمكن أن تكون الهجمات السيبرنية جزءًا من الحرب السيبرنية أو الإرهاب السيبرني، كما يمكن استخدامها من قِبل دول أو مجموعات أو منظمات أو أفراد. منذ أواخر الثمانينات من القرن الماضي، تطورت الهجمات السيبرنية باستخدام الابتكارات في تكنولوجيا المعلومات كأدوات لارتكاب جرائم الأنترنات. و قد لاحظ المنتدى الاقتصادي العالمي في تقريره لعام 2018 أن القدرات السيبرنية الهجومية تتطور بسرعة أكبر من القدرة على التعامل مع الحوادث العدائية.

1. التهديدات السيبرنية:

تختلف التهديدات السيبرنية من حيث أشكالها ومصادرها ودرجة خطورتها وتتراوح ما بين تهديدات بسيطة ومتوسطة ومعقدة. تتمثل التهديدات البسيطة في تلك الهجمات التي يستطيع أي فرد يمتلك قدرات تحليلية وتقنية بدائية القيام بها. فالقدرات التحليلية تمكنه من تحديد الهدف المراد مهاجمته وتحليل نقاط الضعف الموجودة فيه والتي يمكن مهاجمتها. أما القدرات التقنية فهي امتلاك الآليات السيبرنية من برامج وشبكات للقيام بالهجوم. فأي فرد يستطيع أن يقوم بتحميل البرامج الخاصة بالقرصنة من الأنترنات وتحديد هدف ما لمهاجمته، دون الحاجة إلى وجود موارد خاصة أو هياكل مؤسساتية للقيام بالهجوم. ولقد أصبح هذا النوع من الهجمات شائعًا بشكل كبير في الفضاء السيبرني. وهناك نوع آخر من التهديدات أكثر تقدمًا، يمتلك فيه المهاجم معرفة واسعة بالهدف وأنظمة السلامة المعلوماتية التي يطبقها والأنظمة المشغلة للأجهزة السيبرنية الخاصة به، ويستطيع وضع سيناريوهات مختلفة للقيام بهجمات أكثر تعقيدًا من الهجمات البسيطة المشار إليها. غير أن هذه التهديدات، وعلى الرغم من خطورتها، لا ترقى إلى مستوى التهديدات المركبة أو المعقدة التي تمثل الخطر الأكبر على أمن الدول. فهذا النوع من الهجمات لا يمكن القيام به من قبل فرد أو مجموعة صغيرة من الخبراء لوحدهم، وإنما يتطلب مجموعات كبيرة وفرق مكونة من عدد كبير ممن يمتلكون قدرات ومعرفة بكافة الجوانب التقنية، كالمعرفة الكاملة بطبيعة الشبكات، وأنظمة التشغيل، وأنظمة التحكم، وكيفية جمع المعلومات الاستخباراتية والتقنية وتحليلها. وبالتالي فهي

تحتاج إلى تدريب شديد التعقيد والقيام بتجارب وتدريبات على القيام بالهجوم، وهو ما يتطلب كمًّا كبيرًا من الأموال والموارد والمعرفة التقنية والتحليلية. من البديهي أن يتضمن أي نظام إلكتروني بعض نقاط الضعف التي يمكن استغلالها في شن الهجمات السيبرنية. ولهذا السبب تقوم معظم المؤسسات بمحاولة وضع أنظمة للتأمين يكون الهدف منها هو محاولة معالجة نقاط الضعف والتخفيف منها. ففي حالة التهديدات البسيطة، يتم استغلال نقاط الضعف الواضحة الموجودة في الأنظمة السيبرنية الرئيسية التي لا ينصب اهتمام الدول والمنظمات على معالجتها. أما بالنسبة للهجمات المتقدمة فيتم استغلال نقاط الضعف الظاهرة في الأنظمة السيبرنية، إضافة إلى إمكانية الوصول إلى نقاط الضعف الأقل بروزا في نظام ما عن طريق استخدام التقنيات الحديثة. بالنسبة للتهديدات المركبة يتم التوصل خلالها إلى نقاط الضعف غير الواضحة داخل الأنظمة، سواء في مؤسسة واحدة أو أكثر، ويمكن في هذه الحالة شن هجوم متزامن على كافة تلك المؤسسات.

وتزيد نقاط الضعف في الأنظمة المعلوماتية المختلفة من قابلية وقوع الهجمات السيبرنية. فالبرامج الخاصة بالحاسب الآلي يتم تطويرها من خلال لغة برمجية معينة. ومع زيادة سرعة الحواسيب أصبحت البرامج المشغلة أكثر تعقيدًا، ولذا يحتوي البرنامج على ملايين السطور من "شفرات المصدر" والتي قد تتضمن بعض الأخطاء أثناء تطويرها من قبل المبرمجين. هذه الأخطاء لا يمكن اكتشافها بسهولة حتى من قبل تلك البرامج المصممة خصيصًا لمراجعتها. كما أن عديد الأجهزة وأنظمة الاتصال وغيرها يتم تصنيعها وتجميعها في أكثر من دولة، فهي إذا عرضة للهجمات السيبرنية. فقد يتم تغيير أحد أجزائها سرًّا حتى لا تعمل بشكل مغاير أو لا تعمل بالشكل المطلوب أو أن تفسح المجال للبرامج الخبيثة، وقد يتم مهاجمة البرامج المشغلة لها لتحقيق ضرر مادي بالجهاز والمستعمل ذاته. تؤدي الطبيعة غير المركزية للأنترنات وغياب قواعد منظمة له إلى زيادة احتمالات تعرض الأنظمة السيبرنية للهجمات. وكلما زاد اعتماد الدول على الفضاء السيبرني في إدارة شؤونها كلما زادت نقاط الضعف في أنظمتها المعلوماتية وبالتالي زيادة فرص

التعرض للهجمات السيبرنية. مع تزايد استخدام الأنترنات سواء من قبل الشعوب أو الحكومات، باتت كثيرٌ من الدول تواجه عديدًا من التهديدات السيبرنية الجدية مما دفعها لتطوير أنظمتها الدفاعية لتحسين قدرتها على مواجهة تلك المخاطر والتهديدات.

2. الهجمات السيبرنية وحرب المعلومات:

تعيش الشركات المختصة في الأمن السيبرني والتي تحلل هجمات القراصنة، وضعا استثنائيا، حيث تنشر المعلومات لدى جهات ستتكتّم حتما عن الأمر على غرار الشركات المُخترقة، التي تخشى المساس بسمعتها، والدول المُخترقة التي تخشى أن يعلم مواطنوها ما حدث، فضلا عن القراصنة الذين يرغبون في العمل لصالح الأجهزة الاستخباراتية بشكل سري.

1.2 القرصنة أداة للتجسس الرقمي:

تُعتبر قرصنة أنظمة المعلومات أحد أهم الأدوات التي تستخدمها الدول للتجسس. وعموما، تصل هذه الدول إلى المعلومات من خلال الثغرات الرقمية المتوفرة بالأنظمة المستهدفة. تجدر الإشارة إلى أن ذلك يحمل في طياته أمرا إيجابيا، حيث لن تحتاج الدول لتجنيد مخبرين فعليين وإقناعهم بسرقة وثائق حساسة، ولن يتجاوز الأمر مجرد إسداء أوامر لأحد البرمجيات عن طريق لوحة المفاتيح (على غرار برمجيات "أحصنة طروادة") والتي ستتكفل بالاستيلاء على الوثائق بشكل سري. في المقابل، يحمل التجسس الرقمي بعدا سلبيا يتمثل في ترك آثار على شبكات الشركات والدول. لذلك، يمكن للجهات المختصة في الأمن السيبرني، على غرار "فاير آي"، تتبع منفذي الهجمات. وعلى الرغم من أن التقارير حول الهجمات السيبرنية يمكن أن تؤدي إلى اندلاع أزمات سياسية، إلا أنها تتسم بالشفافية. وفي الحقيقة، بفضل هذه التقارير، يتمكن الرأي العام من الاطلاع على طريقة عمل القراصنة.

2.2 الشركات تستفيد من هذه التقارير في مجال العلاقات العامة:

بالطبع لا تقوم الشركات بهذه الأبحاث والتقارير بشكل مجاني، أو بهدف جعل العالم أكثر أمانا، حيث يقول أحد خبراء أمن تكنولوجيا المعلومات: "الجميع يستخدمون هذه التقارير كأسلوب للتسويق". كما أوضح هذا الخبير، الذي اشترط مثل غيره الحفاظ على سرية هويته، أن "كل الشركات تريد أن تظهر ما لديها من مهارات ومعلومات، وهذا جزء من اللعبة، ويعتبر أمرا شرعيا". ويقول خبير آخر أنه لا يهتم بشكل شخصي بمن يقف وراء الهجمات بل المهم هو تحقيق الأمن. ويؤكد: "بالنسبة لنا لا معنى ولا فائدة من تحديد مصدر الهجوم، ولا فرق لدينا إذا كان المخترقون من الصين أو روسيا أو الولايات المتحدة، مهمتنا هي

إيقاف هذا الهجوم وإنقاذ الضحية. وأحيانا حتى المسؤول في الشركة التي تعرضت للاختراق يعمد إلى إخفاء الوقائع عن مديريه، لأنه سيكون في موقف محرج ويتعرض للتوبيخ، وبعضهم يسألوننا بكل سذاجة حول ما إذا كنا نستطيع الاتصال بسفارة الدولة التي جاء منها الهجوم، ليساعدوننا على إيقافه".

لكن بالنسبة لشركات الأمن السيبرني، فإن مسألة مصدر الهجوم والأطراف التي تقف وراءه تعد في غاية الأهمية في إعداد التقرير، حيث يقول شخص متخصص في كتابة هذه التقارير: "إن البعد السياسي لا يمكن إنكاره، فنحن نريد أن نعرف ما هو الدافع وراء المجموعة التي قامت بالاعتداء".

3.2 تأجيج الخلافات الدبلوماسية و الصراعات السياسية:

عمل "جو سلوفيك" في مجال الهجمات السيبرنية لفائدة البحرية الأمريكية، ثم انتقل للعمل كمسؤول على أمن تكنولوجيا المعلومات في شركة "دراغوس" لحماية منشآت البنية التحتية، وهي تقوم على سبيل المثال بتأمين شبكات الكهرباء. وهو يحذر من مغبة التقليل من خطورة التبعات السياسية لهذه التقارير و يقول: "إن الشركات الخاصة نادرا ما تقوم هي بتحديد من يقف وراء الهجمات السيبرنية، لأن مثل هذه القرارات يمكن أن تصب الزيت على النار المشتعلة أصلا في العلاقات الدبلوماسية".

عبر العديد من الباحثين في مجال أمن تكنولوجيا المعلومات عن شكوكهم في أن الحكومات تتأثر سياسيا بمحتوى التقارير، حيث يقول أحد الموظفين السابقين في المخابرات الأمريكية: "إن موظفي الشركات ليسوا خبراء سياسيين، وعندما يقدمون تقاريرهم فإن الحكومة الأمريكية لا تعلق عليها، بل تستمع إليها وتقول لهم حظا موفقا وإلى اللقاء". ومن المؤكد أن العديد من الشركات مستعدة لفعل أي شيء لمعرفة التفاصيل التي تمتلكها الحكومة الأمريكية حول مجموعات القراصنة في العالم، ولذلك فإن الموظفين الحكوميين يكتفون بتسلم تقارير الشركات دون التعقيب عليها.

3. هل أصبحت الهجمات السيبرنية بديلا عن الحروب التقليدية ؟

سباق تسلح جديد ينطلق في العالم عبر هجمات إلكترونية متطورة تستهدف الوصول لمعلومات حساسة جدا وتغييرها، أو تدمير البنية التحتية لموقع أو دولة، وربما التسبب في انفجارات ودمار هائل للدول. أخذت الحروب في العالم أشكالا مختلفة وتطورت على مدى القرون بدءا من الحروب التقليدية بالسلاح الأبيض إلى البندقية البدائية وصولا للأسلحة المتطورة فالأسلحة الكيماوية والنووية والجرثومية. أما اليوم، مع تطور الأسلحة السيبرنية وتكنولوجيا المعلومات، حيث يشهد العالم ظهور نوع جديد ومتقدم من الحروب أشد خطورة ودقة من أي سلاح آخر، بما في ذلك السلاح النووي، ألا وهي الحروب السيبرنية لكونها غير محدودة بالمكان أو الزمان ويمكن شنها بسرعة خيالية، والأضرار التي يمكن أن تتسبب بها قد تنتشر على مساحات واسعة جدا. و ليس لأضرار الهجمات السيبرنية حدود، فبإمكانها التسبب بانفجارات في مخازن الوقود والمحطات النووية وكافة المراكز الحيوية، أو تعطيل وسائل النقل برا وبحرا وجوا،

أو تغيير مسار الرحلات، إضافة لتعطيل أنظمة الطاقة وقطع الكهرباء عن مدن بأكملها. أما معلوماتيا فالهجوم السيبرني يمكنه تعطيل أنظمة التحكم في الصواريخ والطائرات، و التشويش عليها وتغيير مسارها، أو تعطيل أنظمة الدفاع و حواسيب أمن المعلومات. وتصل قدراتها إلى تعطيل أجهزة الاتصالات بكل أنواعها، إضافة إلى اختراق البنوك وسرقة الحسابات والتلاعب بالتحويلات.

1.3 أمثلة عن الهجمات السيبرنية:

منذ عام 2003 بدأت الدول والأجهزة الأمنية فعليا في شن الهجمات السيبرنية والتصدي للهجمات المعاكسة، وهنا كانت بداية استخدام السلاح الرقمي كأداة للصراعات السياسية والأمنية. وقد شهد العقد الثاني من القرن 21 عدة هجمات أدت لأضرار بليغة، كان أبرزها في أميركا حيث تسببت إحدى الهجمات في تعطيل منظومات شبكات الطاقة الكهربائية وانقطاع التيار الكهربائي عن عدة مدن في مناطق متعددة. وفي أوكرانيا بدأت سلسلة من الهجمات السيبرنية القوية في جويلية 2017، استهدفت مواقع المؤسسات الأوكرانية، منها البنوك والوزارات والصحف وشركات الكهرباء، وسبب ذلك أضرار وخسائر جسيمة. كما واجهت روسيا سلسلة من الهجمات السيبرنية قُدرت بحوالي 25 مليون هجوم على البنية التحتية خلال كأس العالم 2018. وتعرضت استونيا وكوريا الشمالية لهجمات شديدة كذلك. يشير الخبراء في هذا المجال إلى أن الحروب القادمة ستكون حصة الأسد فيها للهجمات السيبرنية. فعلى سبيل المثال لم يعد هناك حاجة لإرسال الطائرات الحديثة لتدمير أنظمة الدفاع الجوي لبلد ما، وإنما يستطيع هجوم سيبرني دقيق تعطيل تلك الأنظمة أو التشويش عليها، إضافة لقدرتها على تعطيل المنشآت الأمنية والعسكرية دون الحاجة لصواريخ. ما يعني عدم الحاجة مستقبلا لصرف الأموال لصناعة طائرة متطورة أو صاروخ بعيد المدى، وإنما ستتحول الحروب إلى " نوايا" يمكن الانتصار فيها بتكاليف وجهد أقل مع تحقيق نتائج أكبر وأدق.

2.3 كيف يوظف الذكاء الاصطناعي في توقع الهجمات السبرنية ومواجهتها؟

بدأ خبراء الأمن السيبرني منذ مدة بالتحذير من تهديدات وشيكة، يتطلب بعضها أعوامًا من الخبرة لفهم اتجاهات الجهات الفاعلة ومسارات البرامج الضارة. و يرجع سبب نجاح المخترقين إلى قدرتهم على الاستغلال الناجح لتوسع المساحة المعرضة للهجمات، وللثغرات الأمنية الناتجة عن التحول الرقمي. ويصعب التنبؤ بأفعال المخترقين، الذين يتمتعون بالقدرة على الاستباق، وغالبًا ما تكون مبادراتهم محاطة بدرجة يقين كبيرة، في حين تهمل المنظمات المستهدفة التدابير الأمنية المناسبة، خلال بحثها الدؤوب عن اكتساب قيمة تنافسية وزيادة تطور شبكاتها. وتشير تقارير إلى أن الاقتصاد العالمي تعرض لخسائر وصلت إلى نحو 1.5 تريليون دولار في العام 2019، ومن المرجح استمرار معدل نمو الجرائم السيبرنية لفترة

طويلة، ما لم تتخذ المنظمات المستهدفة خطوات لتحول نموذجي فيما يتعلق بكيفية تفكيرها في المقاربة الأمنية السيبرنية وتطبيق التراتيب الخاصة بها.

3.3 المواجهة:

تحتاج المنظومات الدفاعية إلى استخدام التقنيات والإستراتيجيات ذاتها التي يستخدمها المخترقون أو "الهاكرز"، والخروج من الدائرة التقليدية المتمثلة في شراء حلول الأمن السيبرني المستحدثة التي تجاري التهديدات. فقد أشار تقرير أمريكي إلى احتمال تطور أعمال " الهاكرز" خلال الأعوام القليلة المقبلة، مما يتطلب وضع إستراتيجية تهدف إلى تطوير نظام مناعة للفضاء السيبرني متكيف يشبه نظام مناعة جسم الإنسان. إذ أن الذكاء الاصطناعي يمكنه أن يؤدي مهمة الكريات البيضاء في جسم الإنسان للتصدي للفيروسات الضارة في الشبكة، من خلال تحديد التهديدات وبدء وتنسيق الاستجابة المناسبة.

4.3 توقع الهجمات:

قال «ديريك مانكي»، رئيس الرؤى الأمنية والتحالفات العالمية للتهديدات في شركة «فورتينت»: «إن الجيل الأول من الذكاء الاصطناعي يوجد فعليًا في بعض القطاعات، وبإمكان الأنظمة المستخدِمة للتعلم العميق للآلات غربلة جبال من البيانات بسرعة، لإيجاد تحليل وتحديد مسار العمل المناسب، من خلال الاستفادة من الشبكات العصبية الاصطناعية وقواعد البيانات الضخمة، وكل ذلك بناءً على سرعة الشبكات.»

وأضاف «الجيل الثاني من الذكاء الاصطناعي قادرا على اكتشاف الأنماط بشكل أفضل من خلال توزيع عقد التعلم على بيئة معينة. ويعمل هذا الجيل حاليًا في المختبرات وبعض بيئات الإنتاج. ويعزز ذلك تأثيره على أشياء مثل التحكم في الوصول. و يمكن لبعض أنظمة الذكاء الاصطناعي الآن تحديد الأفراد باستخدام بصمات حيوية معقدة - مثل أنماط الكتابة أو إيقاعات ضربات القلب- مع قدرتها على اكتشاف أكثر الانحرافات دقةً لتحديد الجهات الفاعلة الخبيثة والبرامج الضارة. وستتضمن أيضًا توافق الحماية والضوابط المركزية مع المتطلبات والتغيرات المحلية.»

5.3 مرونة الحركة:

لن يكون أي إجراءٍ مما سبق مهمًا إذا لم يتوفر الأمن السيبرني حيث يضرب المخترقون. وتوجد اليوم شرائح مختلفةً من الشبكات لا يمكنها التواصل فيما بينها، وغالباً ما تبقى المعلومات المتوفرة عن التهديدات في عزلة. والنتيجة هي تأمين مجزأ للأنظمة يحرص مجرمو الأنترنات على استغلاله.

يؤكد الانتقال من الوضع الحالي لمعظم المنظومات الحاجة إلى نوع من التأمين المتكامل مستقبلًا، والحاجةَ كذلك إلى اتباع منهجيات جديدة. حيث تحتاج المؤسسات إلى التركيز على الترابط والتكامل العميق بين أجهزتها الأمنية، ولا تحتاج المنظومات، كي تنجح، إلى الوصول لمعلومات الأمان المهمة فقط ، بل يجب عليها مشاركة هذه البيانات بسلاسة وعلى الفور من خلال الشبكة، حتى تتكيف مع التكوين الفريد لكل بيئة شبكة خاصة بها. مع التأكد من أن جميع الشبكات وأنظمة الأمن والأجهزة يمكن التحكم فيها باستمرار من أي مكان في الشبكة. ويرى "مانكي" أن قدرة التعلم العميق للآلات وأنظمة الذكاء الاصطناعي ستُغطي على تولي مهام عديدة كانت توكل سابقًا للموارد البشرية وموجهة للتفاصيل. وستغطي كذلك جزءًا كبيرًا من فجوة مهارات الأمن السيبراني المتزايدة. وسيُتاح لمحترفي الأمن السيبراني ذوي الأهمية تركيز مهاراتهم على التخطيط العالي المستوى والإستراتيجيات. وسيكون هذا الانتقال حاسمًا، مع تحرك المؤسسات لاعتماد إستراتيجيات آمنة ومتقدمة للمساعدة على نجاح الأعمال في السوق الرقمية مستقبلًا.

الخلاصة:

تعد الهجمات السيبرنية حروبا غير معلنة، تخوضها بعض الدول ضد بعض آخر من خلال مجموعات ممولة ومدعومة من الحكومات، تقوم بهجمات وحروب سيبرنية صامتة. وتعتبر الهجمات السيبرنية والقرصنة إحدى الطرق الفعالة والمدمرة التي يتم استغلالها لإلحاق الضرر بدولة أو مؤسسة دون عناء، مقارنة بالهجمات المسلحة التي تتطلب مجهودات ومعدات ووقت أكبر. ورغم أن الحرب السيبرنية لا يمكن أن تحل محل الحرب التقليدية، فهي ربما تكون مقدمة تحضيرية لها حين تستهدف إفشال منظومة تبادل المعلومات، وكذلك الاضرار بمنظومات استراتيجية تتعلق بالبنية التحتية والدفاع وغيرها، وربما تمثل مفاتيح أولية لتحضير الانتصار. لذلك أصبح الأمن السيبراني من أهم هواجس الدول لضمان أمن وسلامة منشآتها الرقمية الحيوية. وينبغي توخي إستراتيجية قوية خاصة بالأمن السيبراني، و تأمين عمليات تسجيل الدخول للتطبيقات التي يتم الوصول إليها من خارج الشبكات باستخدام أساليب مصادقة قوية، وفحص وتصفية حركة مرور البيانات على الأنترنات، والاحتفاظ بنسخ احتياطية لجميع الأنظمة والبيانات الهامة، وبذل المزيد من الجهد للانتباه لهجمات طلب الفدية، و تحسين تبادل المعلومات وتخطيط المهام وقيادتها فيما يتعلق بالشؤون السيبرنية.

أنشطة وزارة الدفاع الوطني
في مجال الأمن السيبرني

تغطية لملتقى الأمن السيبرني بالمدرسة الحربية العليا يومي 25 و26 جانفي 2022

العقيد حسني السعداوي

الأمن السيبرني هو مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستغلال غير المصرح به، سوء الاستعمال، استعادة المعلومات الإلكترونية، إضافة إلى نظم الاتصالات والمعلومات التي تحتويها، وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية،قصد اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستعملين من المخاطر المتواترة في الفضاء السيبرني. والأمن السيبرني هو سلاح إستراتيجي بيد الحكومات والأفراد لاسيما الحرب السيبرنية التي أصبحت جزءًا لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول.

وفي عصر التطورالتكنولوجي أصبح لأمن المعلومات الدور الأهم لصد ومنع أي هجوم إلكتروني، قد تتعرض له أنظمة ومؤسسات الدولة، وأيضا حماية الأنظمة التشغيلية من أي محاولات للولوج بشكل غير مسموح به لأهداف غير سليمة، وفي هذا السياق نظمت المدرسة الحربية العليا بالاشتراك مع وكالة الاستخبارات والأمن للدفاع يومي 25 و 26 جانفي 2022 ، الملتقى السنوي للأمن السيبرني تحت عنوان "التحول الرقمي مصدر لفرص قد تولد مخاطر جديدة :الهجمات السيبرنية".

" La transformation numérique source d'opportunité qui génère de nouveaux risques : les Cyberattaques "

افتتح السيد العميد زهير الجديدي آمر المدرسة الحربية العليا، فعاليات الملتقى بكلمة نوه فيها بمجهودات كافة المحاضرين وكذلك المساهمين في إعداد هذا الملتقى، كما أوضح أن تطور الاستعمالات الرقمية اعتمادا على التكنوليجيات الحديثة وانفتاح بلادنا على المحيط الخارجي يطرح جملة من التحديات والرهانات فيما يخص الأمن السيبرني، وهو ما يحتم وضع الأسس الكفيلة لحماية مؤسساتنا العسكرية والمدنية الحيوية من كل التهديدات الممكنة من خلال تكريس الثقة الرقمية وتوفير مناخ الاستثمار في اقتصاد المعرفة والابتكار، وفي ذات السياق بين أن الهدف من الملتقى هو الرفع من مستوى وعي الضباط الدارسين التابعين للدورة 26، بالمخاطر المرتبطة باستعمالات التكنولوجيات الحديثة والأنترنات سواء في المحيط العسكري أو خارجه، وأهمية دورهم كقادة ومسؤولين في حسن إدارة المجال الرقمي في وحداتهم وإدراج السلامة الرقمية ضمن أوكد أولوياتهم. واختتم السيد العميد آمر المدرسة

كلمته معربا عن أمله في أن يحقق الملتقى الأهداف المرسومة والمتمثلة في فتح آفاق المعرفة حول مجالات الأمن السيبرني والاطلاع على مستجدات هذا الفضاء بما يمكن كل من الضباط الإطار والدارسين من إثراء معارفهم والاستعداد الجيد لمواجهة التهديدات السيبرنية المستقبلية، بما أن هذا المجال أصبح ميدانا جديدا للحرب لا يقل أهمية عن الحروب البرية والبحرية والجوية والفضائية.

شارك في هذا الملتقى ثلة من الخبراء والكفاءات الوطنية المدنية والعسكرية المختصة في مجال الأمن السيبرني والتكنولوجيا الرقمية، وفي مايلي حوصلة لأهم ما ورد في مداخلاتهم:

قدم السيد نوفل فريخة، مدير عام الوكالة الوطنية للسلامة المعلوماتية، مداخلة بعنوان «الأمن السيبرني بين الحقيقة والخيال، الحاضر والمستقبل» ، ذكر فيها التحديات الجديدة للأمن السيبرني من خلال تحديد أنواع التهديدات، وأبرز الحاجة الأكيدة لضمان السيادة الرقمية مبينا الفرق بين مفهومي الدفاع السيبرني ومكافحة الجريمة السيبرنية واختتم بتقديم لمحة عامة عن المجهودات المبذولة من قبل الوكالة الوطنية للسلامة المعلوماتية في تعزيز الأمن السيبرني على الصعيد الوطني قبل تقديم الإستراتيجية الوطنية للأمن السيبرني 2020-2025، والتي تهدف إلى إنشاء نظام لحماية المنشآت الحساسة وتطوير الاقتصاد الرقمي وتشجيع الاستثمارات في هذا المجال.

تحدث المقدم نضال الماجري خلال مداخلاته عن تنظيم المجال السيبرني على المستوى الوطني عموما وعلى مستوى وزارة الدفاع الوطني خصوصا، حيث استعرض المؤسسات والهياكل الوطنية التي تُعنى بتنظيم الفضاء السيبرني الوطني ودورها، كما تحدث عن دور وكالة الاستخبارات والأمن للدفاع في تنظيم الفضاء السيبرني، وأكد على ما يجب أن يعرفه المسؤولين بمختلف مستوياتهم عن سلامة النظم المعلوماتية الرقمية والنصائح القيادية الضرورية لضمان حماية الأنظمة المعلوماتية الموضوعة تحت إمرتهم.

وفي مستهل حديثه عن حماية البنى الرقمية الحيوية، أبرز عبر عديد الأمثلة الهامة مخاطر تعرض البنى الرقمية إلى الهجمات السيبرنية، ليؤكد على أن المساس بهذه النظم من شأنه التسبب في أضرار جسيمة، بحيث أصبحت عديد الدول تعتبر تعرضها لمثل هذه الهجمات مساسا من سيادتها الرقمية واعتداء على أمنها القومي. وفي مداخلته الأخيرة حول التخطيط العملياتي للحروب السيبرنية، قدم المقدم نضال الماجري الخطوط العريضة للتحضير للعمليات السيبرنية الدفاعية والهجومية وقارنها مع مرحلة الإعداد للعمليات مع العدو التقليدي مستندا في ذلك لمقطع فيديو يجسد تمرين عالمي في مجال الحرب السيبرنية بعنوان:

«LockedShield».

وتحدث الرائد عثمان القتلاني عن استغلال الفضاء الإلكتروني من قبل المجموعات الإرهابية على غرار تنظيم الدولة الإسلامية بالعراق والشام أو ما بات يعرف بتنظيم داعش الإرهابي لترويج الإيديولوجيات المتطرفة والأفكار التكفيرية الهدامة، وذلك من خلال بث مقاطع فيديو دعائية على منصات التواصل الاجتماعي، الغرض منها التواصل مع منتسبيها واستقطاب وتجنيد عناصر جديدة، مع إمكانية تنفيذ هجمات إلكترونية.

هذا، وأشار الرائد عثمان القتلاني إلى أنه بات من الضروري مجابهة استخدام الفضاء الإلكتروني من قبل التنظيمات الإرهابية بالاعتماد على مقاربة شاملة ومتكاملة تأخذ بعين الاعتبار الجانب التشريعي والتقني إضافة إلى التحسيس المتواصل بمخاطر هذه التنظيمات خاصة وتأثيرها على فئة الشباب، مع دعوتهم إلى اجتناب الإبحار على المواقع المشبوهة.

تطرق الرائد حسام البدوي إلى مفاهيم وأهداف الأمن السيبرني من خلال تعريف نظام المعلومات الذي اعتبره مجموعة من الموارد التي تمكن من تجميع المعطيات وتصنيفها وتخزينها ومعالجتها وتوزيعها بشكل عام عن طريق الحاسوب، وتولى تعريف أمن وتكنولوجيات المعلومات المتمثل في تقليل المخاطر والحد من تأثيرها على العمليات والأنشطة التجارية للمؤسسات باستعمال مختلف الوسائل التقنية والتنظيمية والقانونية والبشرية، ليخوض لاحقا في موضوع الإجراءات الأمنية في المجال وذلك من خلال تطبيق بعض القواعد التي تتمثل أساسا في السرية والنزاهة والجاهزية وإثبات المصدر.

أما الأستاذ نبيل الساحلي، مدير التعليم الجامعي بالأكاديمية البحرية، فقد تطرق إلى موضوع الأمن السيبرني، باعتباره مجالا تكنولوجيا ناشئا يعالج مسألة تأمين الفضاء الإلكتروني. وبما أن معظم الناس اليوم يستخدمون الفضاء الإلكتروني للعمل والتفاعلات الاجتماعية، فقد أصبح عالمنا على نحو متزايد، عالما افتراضيا بديلا، حيث يمكن تنفيذ العديد من الهجمات السيبرنية بطرق مختلفة تحددها طبيعة الأهداف المستهدفة ومدى قدرتها على الصمود، كما أبرز كيفية التصدي لضعف الأنظمة المتصلة بالفضاء الإلكتروني والهجمات الإلكترونية. وأوضح المتحدث المعايير المختلفة التي تدخل حيز التنفيذ مثل طاقة الشبكة، أمن جدار الحماية، أمن الهاتف المحمول إلى غير ذلك.... وهي بدورها تحدد مستوى التعرض للمخاطر السيبرنية وكيفية معالجتها.

هذا وتناول العقيد هشام الدغري الحديث عن الإطار القانوني للفضاء السيبرني حيث وضح بعض المفاهيم الجديدة لتعريف هذا الفضاء على أنه » فضاء رقمي يربط منظومات المعالجة الإلكترونية للمعطيات بشبكات المعلومات والاتصال، ويشمل الحواسيب والشبكات والمنصات والمحتوى والعمليات التي تُجرى باستعمال هذه الشبكات«،كما قدم بعض الحلول العملية التي تتماشى مع مقتضيات الدفاع في مجال الأمن السيبرني وأكد ضرورة تحسين الإطار القانوني للفضاء الإلكتروني لحماية حقوق الدولة وسيادتها وكذلك ضمان حقوق المواطن وحرياته وسلامته، كما شدد على وجوب الدفاع عن مناهجنا وقيمنا المجتمعية لأن الفضاء الإلكتروني أصبح أداة للتأثير والربح وتضارب المصالح لفائدة الجهات الفاعلة في الاقتصاد السيبرني الجديد والذي أصبح أقوى من الدولة، وفي الختام أشار إلى ضرورة تأقلم قواتنا العسكرية مع هذا المجال لمجابهة تحديات ومخاطر جديدة، لأن الحرب القادمة هي حرب إلكترونية بالأساس.

وعلى غرار الملتقى السابق، لاقت المداخلات المقدمة استحسان الضباط الدارسين وإطارات التعليم بالمدرسة الحربية العليا، حيث مكنتهم من فهم أهمية الفضاء السيبرني كمجال جديد للحرب وأطلعتهم على طرق استخدام الهجمات الإلكترونية كما عرفتهم على المخاطر التي تهدد الفضاء السيبرني والتي ترتبط ارتباطا وثيقا بالأمن القومي للدولة والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية، وهو ما يمهد لحسن تعاملهم مع آليات الذكاء الاصطناعي وتحولات الثورة الصناعية الرابعة.

SÉMINAIRE CYBERSÉCURITÉ

25 ET 26 JANVIER 2022

Sous l'autorité du Colonel Major Zouheir JEDIDI

Dirigé par le Colonel Hosni SAADAOUI

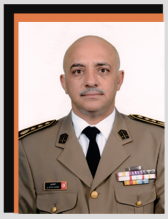
Thème:

La transformation numérique, source d'opportunité qui génère de nouveaux risques : les cyberattaques.

-- Honorables Intervenants --

Mr. Nabil Sahli

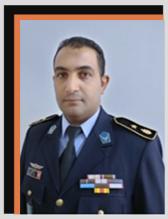
Mr. Naoufel FRIKHA



Col. Hichem Doghri

Lt Col Med Nidhal Mejri

Cdt Houssem BEDOUI



Cdt Othmen GATLENI

-- Programme --

	Mardi 25 janvier 2022						
Horaire	08h à 8h15	08h15 à 10h	10h05 à 11h	11h10 à 12h10	Pause déjeuner	13h à 14h20	14h30 à 16h
Thème	Mot d'ouverture	Cyber sécurité : entre réalité & fiction, Présent et future	Les fondamentaux de la cybersécurité	Organisation du cyberespace : niveau national et au niveau du MDN		Vecteurs de Risques	L'usage terroriste du cyberespace
Intervenant	CM Zouheir JEDIDI	M. Naoufel FRIKHA	Cdt Houssem BEDOUI	Lt Col Med Nidhal MEJRI		M. Nabil SAHLI	Cdt Othmen GATLENI
Mercredi 26 janvier 2022							
Horaire	08h à 10h		10h à 12h		Pause déjeuner	13h à 15h	15h à 16h
Thème	Les infrastructures numériques critiques		Cadre juridique du cyberespace			Planification opérationnelle de cyberguerres	Mot de Clôture
Intervenant	Lt Col Med Nidhal MEJRI		Col Hichem DOGHRI			Lt Col Med Nidhal MEJRI	CM Zouheir JEDIDI

المقدم محمد نضال الماجري

ملتقى التهديدات السيبرنية

12 و14 أفريل 2022

معهد الدفاع الوطني

الدورة الوطنية التاسعة والثلاثون

في إطار سلسة ملتقيات معهد الدفاع الوطني، انتظم يومي 12 و14 أفريل 2022 ملتقى حول "التوقي من التهديدات السيبرنية". وقد تمّ إقرار موضوع هذه السنة لأول مرة بناء على توصيات السيد وزير الدفاع الوطني في هذا المجال، في ظل تنامي التهديدات السيبرنية عبر العالم ضد المنشآت الرقمية الحيوية وضد الأفراد وخاصة منهم كبار المسؤولين، وما تتضمنه هذه التهديدات من مخاطر على السيادة الوطنية وعلى الأنشطة والقطاعات الحيوية والمنشآت الحساسة، وما يقتضيه من مزيد العمل على حماية الأفراد ومعطياتهم الشخصية وحماية الفضاء السيبرني الوطني.

لبلوغ الأهداف المرسومة، اشتمل هذا الملتقى على المحاور التالية:

• مبادئ السلامة المعلوماتية والأمن السيبرني والتعريف بمختلف الجوانب المتعلقة بهما، مع الاطلاع على آخر المستجدات في المجال.

• الجوانب التشريعية المتعلقة بحماية المعطيات الشخصية في الفضاء السيبرني.

• الإجراءات الوقائية والعملية للتوقي من الهجمات السيبرنية وحماية المعطيات في ظلّ ارتفاع مخاطر البرمجيات الخبيثة وتقنيات التصيّد في الفضاء السيبرني والتي تستهدف كبار المسؤولين في أعلى مواقع القرار.

وقد تمّ التطّرق للمحاور المشار إليها ضمن المحاضرات التالية:

- "Cybersecurity trends in Africa"، التي تولّى تقديمها السيد نزار بن ناجي وزير تكنولوجيات الاتصال.

- "حماية المعطيات الشخصية في الفضاء السيبرني: النصوص والتشريعات"، للسيّد شوقي قدّاس رئيس الهيئة الوطنية لحماية المعطيات الشخصية ودارس بالدورة الوطنية 37.

كما تولّى السّيد المقدم محمد نضال الماجري، مدير السلامة المعلوماتية والأمن السيبرني بالنيابة بوكالة الاستخبارات والأمن للدفاع إلقاء محاضرة حول "الأمن السيبرني لكبار المسؤولين" (Cyber Security For Leaders).

تطّرق السيد نزار بن ناجي، وزير تكنولوجيات الاتصال ضمن مداخلته "Cybersecurity trends in Africa" إلى جملة من الأرقام والإحصائيات التي تعبّر عن واقع مجال الأمن السيبرني في إفريقيا وترتيب الدول طبقا لعدة مؤشرات، مع إبراز ترتيب تونس في القارة الإفريقية في هذا المجال. في نفس السياق أوضح السيّد نزار بن ناجي كذلك ضرورة حماية المنظومات الوطنية الهامة وخاصة منها العمومية الموضوعة تحت إشراف المركز الوطني للإعلامية باعتبارها تمثل أهم مصادر قواعد البيانات الوطنية.

تعرض السيّد شوقي قداس ضمن مداخلته "حماية المعطيات الشخصية في الفضاء السيبرني: النصوص والتشريعات" إلى مفهوم المعطيات الشخصية من خلال عديد الأمثلة المستمدة من الاستخدامات اليومية لهذا المصطلح، مؤكدا على ضرورة حماية هذه المعطيات لضمان حسن استغلالها ولحماية خصوصيات الأفراد. كما تطرق السيد شوقي قداس للجوانب القانونية المنّظمة لمجال حماية المعطيات الشخصية في العالم وفي تونس، مؤكدا على ضرورة تطوير التشريعات الوطنية

لتتلاءم مع التطورات التكنولوجية في هذا المجال. واختتمت المداخلة بإبراز علاقة المعطيات الشخصية بالجرائم السيبرنية الحديثة والتي يتعلق معظمها بالاستيلاء على المعطيات الشخصية وسوء توظيفها.

ضمن مداخلته "الأمن السيبرني لكبار المسؤولين Cyber Security For Leaders" أبرز المقدم محمد نضال الماجري مختلف المخاطر المتأتية من الفضاء السيبرني والمستهدفة أساسا للأفراد وللبنى الرقمية الحيوية الحساسة. كما ذكّر بما يجب أن يعرفه كبار المسؤولين والمسيرين في مختلف مواقع القرار عن سلامة النظم المعلوماتية والنصائح القيادية الضرورية لضمان حماية أنفسهم وحماية المؤسسات الموضوعة تحت إشرافهم. تطرق المقدم محمد نضال الماجري كذلك خلال مداخلته، ومن خلال عديد الأمثلة المتنوعة، لمخاطر تعّرض البنى الرقمية إلى هجمات سيبرنية وأبرز أن إلحاق الأضرار بهذه النظم من شأنه التسبب في تداعيات جسيمة تضاهي وتتجاوز أحيانا مخلفات الحروب التقليدية، حيث أصبحت عديد الدول تعتبر تعرض منشآتها الحيوية الحساسة لهجمات سيبرنية بمثابة المساس من أمنها القومي وسيادتها الرقمية.

متفرقات

الملازم أول باسم بنعيسى

أهم التوصيات والاحتياطات للحماية من الاختراقات السيبرنية

1 -اِستخدم أحدث برامج الحماية من الاختراق والفيروسات وقم بعملية مسح دوري وشامل على جهازك في فترات متقاربة خصوصاً إذا كنت ممن يستخدمون الإنترنت بشكل يومي.

2 - تأكد من تحديث مضاد الفيروسات كل أسبوع على الأقل.

3 - ضع مضاد فيروسات فعّال على حاسوبك الشخصي.

4 - تأكد من أن جدار النار"Firewall" على وضعية تفعيل "Activer".

5 - لا تفتح أي رسالة إلكترونية من مصدر مجهول لأن المخترقين يستخدمون رسائل البريد الإلكتروني لإرسال ملفات التجسس إلى الضحايا.

6 - عدم استقبال أية ملفات (أثناء الدردشة) من أشخاص غير موثوق بهم خاصة إذا كانت هذه الملفات تحمل امتداد ".exe" أو أن تكون ملفات من ذوي الامتدادات مثل ".pif" أو".jpg" أو ".bat" أو".dll" أو " com. " وتكون مثل هذه الملفات عبارة عن برامج

تـزرع ملفـات التجسـس فـي جهـازك يسـتطيع مـن خلالهـا المخـترق الولـوج إلـى ملفاتـك الشـخصية.

7 - لا تقـم باسـتلام أي ملـف وتحميلـه علـى القـرص الصلـب فـي جهـازك الشـخصي إن لـم تكـن متأكـدا مـن مصـدره.

8 - عـدم الاحتفـاظ بمعلومـات شـخصية أو عسـكرية داخـل جهـازك (رسـائل خاصـة أو صـور فوتوغرافيـة أو ملفـات أومعلومـات مهمـة مثـل أرقـام الحسـابات البنكيـة أو البطاقـات الإئتمانيـة....).

9 - قمْ بتشفير ملفاتك المهمة حيث لا تفتح إلا بكلمة المرور.

10 - حـاول قـدر الإمـكان أن يكـون لـك عـدد معيـن مـن الأصدقـاء المقربـين عبـر مواقـع التواصـل الاجتماعـي وعـدم إضافـة أشـخاص مجهولـين.

11 - قـم بمسـح ملفـات تعريـف الارتبـاط بالأنترنـات "cookies" مـن جهـازك فهـي عبـارة عـن ملفـات يرسـلها الموقـع لمتصفحـك ولا يسـتطيع أي موقـع قراءتهـا وقـد تكـون بهـا كلمـات سـر موقـع أو اشـتراك... ، فتصبـح مزعجـة فـي بعـض الأحيـان حيـث أنها تسـجل كل المواقـع التـي دخلتهـا و كل الصفحـات التـي شـاهدتها و مـدة مشـاهدة كل صفحـة.

12 - لا تخـزن كلمـات المـرور أو كلمـات سـر علـى جهـازك مثـل كلمـة المـرور لاشـتراكك فـي الإنترنـت أو البريـد الإكترونـي.

13 - إذا لاحظـت حـدوث اي شـيء غريـب مثـل خلـل فـي البرامـج أو خـروج و دخـول CD اِقطـع الاتصـال بالإنترنـت فـورا وتأكـد مـن خلـو الجهـاز مـن الفيروسـات.

14 - لا تفتـح بريـدك أو أيّ مـن معلوماتـك الخاصـة وأنـت متواجـد بمقاهي مغطـاة بالأنترنات، نظـرا لوجـود برامـج تعمـل بشـكل مخفـي تحفـظ جميـع النمـاذج التـي تقـوم بتعبئتهـا دون أن تشـعر.

15 - حـاول دائمـاً تغييـر كلمـة السـر بصـورة دوريـة ويفضـل أن تتكـون كلمـة السـر مـن أرقـام وحـروف ورمـوز يصعـب تخمينهـا، لأن هنـاك برامـج تقـوم بتجريـب الآلاف مـن كلمات

المـرور وتقـوم بمسـح علـى مـدار السـاعة فيُدْخِـلُ المخـترق اسـم المسـتخدم للبرنامـج ويطلـب منـه تخمـين كلمـة المـرور.

16 - لا تسـتخدم كلمـة مـرور موحّـدة بـل اِجعـل كلمـة مـرور بريـدك تختلف عـن معرفك فـي المنتديـات الأخـرى وحـاول أن تجعـل لـكل منتـدى أو بريـد كلمـة مـرور مختلفة.

17 - اِحذر من المواقع المشبوهة مثل مواقع الكراكات "Crack" والسيريالات والمواقع غير الموثوقة، ففيها برامج يتم تحميلها في الخلفية أثناء تصفح الموقع وهي تحدث

بشكل مستمر وأحيانا تفشل برامج "Spyware" في مقاومتها أو القضاء عليها وكذلك عند تركيب كراك لبرنامج فكثير من هذه الكراكات يحتوي على باتش يمكن أن يشكّل عند تشغيله ثغرة خطيرة في جهازك.

18 - عدم الولوج إلى مواقع مشبوهة تمّ تحذيرك منها من طرف مضاد الفيروسات أو متصفح الأنترنات، لأنها غالبا ما تكون مواقع تحتوي على برمجيات خبيثة يمكن أن تلحق الضرر بجهازك.

19 - تجنب المواقع الموجودة في رسائل الإشهارات، لإمكانية احتوائها على برمجيات خبيثة.

20 - جميع الأجهزة المتصلة بالشبكة عرضة للإصابة بالفيروسات في حالة مشاركة الملفات فيما بينها، وفي حالة مشاركة الاتصال بالإنترنت يجب تعطيل وظيفة

تبادل الملفات والطابعات وتفعيل الدخول إلى الجهاز بكلمة سر حتى يتم تجنب المخاطر إلى حد كبير.

21 - الحرص على التنزيل والتحيين الدوري لمتصفح الأنترنات من المواقع الرسمية.

https://www.zdnet.fr/pratique/cybersecurite-le-guide-pour-proteger-votre-vie-privee-contre-les-pirates les-espions-et-le-gouvernement-39910323.htm

رمز الاستجابة السريعة (QR code)
المخاطر وطرق الحماية

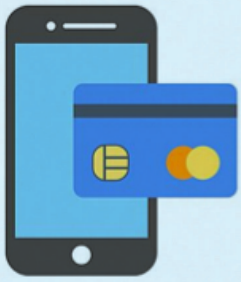
الملازم أول صبرين العايدي

رمز الاستجابة السريعة (Quick Response code أو QR code): هو نوع من الرموز الشريطية ثنائية الأبعاد (الباركود). يتكون الرمز من وحدات سوداء مرتبة على شكل مربع على خلفية بيضاء تحتوي على عديد المعلومات (نص، رابط ،...). ويمكن مسحه ضوئيًا واستغلاله ببرمجيات قراءة على الهواتف الذكية.

1. مخاطر استعمال رمز الاستجابة السريعة:

قد يحتوي رمز الاستجابة السريعة «الملوث» على رابط لصفحة احتيالية أو رابط تنزيل لبرنامج ضار يمّكن من :

بعث رسائل بريد إلكتروني ورسائل قصيرة إلى جهات الاتصال المحفوظة على الهواتف الذكية.



إجراء عمليات شراء ومعاملات مالية باستخدام معطيات البطاقات المصرفية المسجلة على مستوى الهاتف الذكي.

اختراق حسابات على مواقع التواصل الاجتماعي المسجلة على الهاتف الذكي.

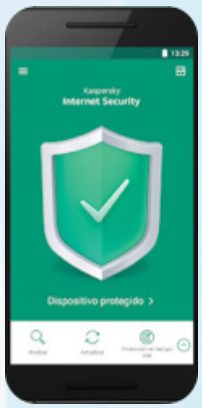
تغيير قائمة جهات الاتصال وإجراء مكالمات هاتفية

2. طرق الحماية من مخاطر استعمال رمز الاستجابة السريعة:

عدم القيام بمسح رمز الاستجابة السريعة ضوئيًا دون التأكد من صحة مصدره.

عند مسح رمز الاستجابة السريعة ضوئيًا، ضرورة التحقق من توافق المعلومات المعروضة مع الخدمة المراد تحقيقها.

التثبت من التطبيقات المراد تحميلها مباشرة عن طريق رمز الاستجابة السريعة الخاص بها وذلك بالتحقق من المعلومات المتعلّقة بها (التقييمات، التحقق من الأمان، المصدر والمطور) بمتجر التطبيقات.



الحرص على تثبيت مضاد فيروسات على الأجهزة المحمولةّ (الهواتف الذكية والأجهزة اللوحية) للتقليل قدر الإمكان من المخاطر المرتبطة بالبرامج الضارة.

الملازم أول ظافر رويس

مقتطفات من بعض المنتجات الرقمية لسنة2022

الحواسيب المحمولة

Station de travail Mobile

يحتوي الجهاز على معالج i7-11850H من الجيل الحادي عشر والتابع لشركة " Intel "، وذاكرة حية GB32، وذاكرة تخزين SSD بسعة TB 1 . كما يتميز هذا الحاسوب المحمول بشاشة مميزة وبدقة عالية جدا"UHD" ومجهز بقارئ بصمات الأصابع. يحتوي هذا الجهاز على نظام التشغيل "Windows 11 PRO".

Station GAMER

يعتبر هذا الجهاز من أفضل الحواسيب المحمولة الخاصة بألعاب الفيديو. ويحتوي علي هارد من نوع SSD بحجم 2TB ويأتي بذاكرة حية بحجم 32GB يحتوي الجهاز أيضا علي معالج i9-10885H بسرعة 5.3GHz كما يحتوي علي كارت شاشة, GTX 1650Ti 4 Go

الهواتف الذكية

iPhone 13, PRO, PRO MAX

اختارت بعض المواقع المتخصّصة في المجال التقني "iPhone 13" كأفضل الهواتف الذكية لعام 2021؛ يتميز iPhone 13 بشاشة OLED قياس 7.6 بوصة بدقة 1170 × 2532ومعالج Bionic A15 Apple وكاميرا 12 + 12، فائقة السرعة وكاميرا أمامية 12 ، وبطارية 3240Mah

GALAXY Z FLIP 3

مثّل الهاتف المحمول "Z FLIP 3" والتابع لشركة "SAMSUNG" ثورة في عالم التكنولوجيا كونه هاتف قابل للطي، كما يعمل بتقنية الجيل الخامس يحتوي على ذاكرة حية8 GB وبطارية بسعة 3300Mah ويدعم تصوير الفيديوهات بجودة 4K بدقة 2160 بكسل

الساعات الذكية

GALAXY WATCH 4

تمكّن هذه الساعة الذكية من تتبع صحتك أثناء التمارين الرياضية من معصم يدك. تحتوي على مستشعر لمعدل نبضات القلب البصري، كما يمكن لها قياس ضغط الدم وتتبع نبضات القلب غير المنتظمة، وقياس الأكسجين في الدم...

SERIE 7

صممت هذه الساعة خصيصا لمستعملي بنظام "iOS" ولا يمكن استعمالها مع الأجهزة التي تعمل بنظام "Android".

السماعات اللاسلكية

Fit Pro

تتميز هذه السماعات بتقنية عزل الضوضاء النشط "ANC" ومقاومة للماء والعرق حسب المعيار "IPX4" والتي تساعد على ممارسة الرياضة دون قلق.

wf 1000xm4

صممت هذه السماعات خصيصا لملاءمة مختلف أشكال تجويف الأذن. كما تمتاز هذه السماعات بجودة صوت استثنائية وتقنية تقليل تشويش الرياح خاصة عند ممارسة الرياضة. وتشحن هذه السماعات بتقنية "Qi" أو الشحن اللاسلكي.

منتجات المنزل الذكي

Robot Vacuum

تتميز المكنسة الذكية بقدرة هائلة في تنظيف المساحات. إضافة إلى تنقلها السريع والدقيق في مختلف الأشكال، وتحتوي على بطارية ذات خاصيات عالية. ويتم ربطها بتطبيقة خاصة على هاتف ذكي.

lampe intelligente

تمكن المصابيح الذكية من الاقتصاد في استعمال الطاقة وذلك من خلال التصرف فيها عن بعد (تشغيلها وغلقها) عن طريق ربطها بتطبيقة مركزة على هاتف ذكي. كما تمكن هذه التطبيقات من مزامنة الضواء أو تغيير اللون.

MI 360° 2K Pro

تمكن هذه الكاميرا الذكية من مراقبة وحماية المنازل والشركات والمحلات التجارية من السرقة. وتتميز خاصّة بسهولة تركيزها وربطها بالشبكة البعدية. تحتوي على بطاقة ذاكرة 32GB ودقّة 1296Px . وتعمل على نظامي التشغيل "Android" و"iOS".

أبرز 5 فأرات لألعاب الفيديو

تعتبر الفأرة أحد المكونات الأساسية لجهاز الحاسوب المكتبي أو المحمول، كما تعد أحد أهم العناصر لممارسة ألعاب الكمبيوتر، لذا يجب أن يكون موثوق ومريح.وتزداد أهميته في ألعاب الكمبيوتر التنافسية،إذ قد يرجع الفرق بين النصر والهزيمة غالبا إلى دقة حركات الفأرة.

فيما يلي قائمة بأفضل فأرات ألعاب يمكنك استعمالها:

DeathAdder V2

لاقت الفأرة " DeathAdder V2" إستحسان مستعميلي ألعاب الفيديو في مختلف أنحاء العالم؛ إذ تتوفر 8 أزرار قابلة للبرمجة والتعديل حتى يتم دمج التصميم الخافت مع الدقة ، للحصول على تجربة سهلة ومريحة، كما تسمح هذه الأزرار بالوصول السهل إلى الخاصيات الخفية أثناء لحظات اللعب الحرجة.

Basilisk V3

على عكس تصميم فأرة DeathAdder المبسط، تقدم فأرة Ba-silisk شكل مميز أكثر.
وتعد الميزة البارزة في Basilisk، عجلة التمرير التي تدور تلقائيا بين التمرير السريع والدوران الحر .

Hero G502

تعتبر الفأرة"Hero G502" من أفضل خيارات فأرات الألعاب غير باهضة الثمن حيث تتضمن 5 أزرار قابلة للبرمجة حول مسند الإبهام وزر النقر الأيسر، تتيح النفاذ السريع لجميع الخصائص الأكثر أهمية في أي لعبة. تعتبر الأزرار اليسرى واليمنى مثيرة؛ إذ يتيح تصميمها سهولة في الاستعمال.

Dark Core

توفر الفأرة "Core Dark" مزايا قوية ومتعددة، مع سعر مناسب وتوفر تجربة مريحة ودقيقة مع أزرار قابلة للبرمجة والإضاءة، هي فأرة لاسلكية، يمكن استعمالها من خلال ربطها بخاصية Bluetooth، مع إمكانية تشغيلها باستخدام الشحن اللاسلكي Qi أو USB-C؛ وهو ما يجعل Core Dark أحد أسهل أجهزة الألعاب اللاسلكية في السوق.

MM720

مقارنة بمعظم أجهزة الفأرات المخصصة للألعاب، تبدو "MM720" غريبة بعض الشيء؛ من خلال تصميمها الفريد من نوعه وشكلها الدائري ولكن مقصود؛ إذ توفر إحساس مريح مع خفة الوزن؛ ما يجعلها مناسبة للألعاب والاستعمال العادي.

نصائح حول كلمات المرور

تعتبر كلمات المرور من أول وأهم الإجراءات الواجب تفعيلها لحماية الحواسيب والحسابات على شبكة الأنترنات. في ما يلي بعض النصائح المقترحة لإنشاء كلمات المرور والحفاظ عليها وتجنب الهجمات السيبرنية:

كلمات المرور معقدة

تأكد دائما من استعمال كلمة مرور معقدّة وقوية لتفادي التعرض لهجمة سيبرنيّة من نوع التخمين أو "BruteForce".
تتكون كلمة المرور المعقّدة على الأقل من 10 حروف وأرقام ورموز

تحيين كلمات المرور

يجب اعتماد منهجية خاصة بتحيين كلمة المرور الخاصة بك بصفة دورية لحماية حسابك من القرصنة باستعمال تقنية الهندسة الاجتماعية "Social Engineering" أو سرقة المعطيات من قواعد البيانات

حفظ كلمات المرور

الحرص على عدم كتابة كلمة المرور على أوراق وتركها على مرأى العموم.

تسجيل كلمات المرور بالمتصفح

عدم تسجيل معطيات النفاذ (Login, Mot de passe) بالمتصفح للولوج إلى المنصّات أو حساب البريد الإلكتروني.

قواعد السلامة المعلوماتية المتعلّقة بالبريد الإلكتروني

عدم حفظ كلمات المرور والمعرفات في متصفح الواب

إستخدام كلمات مرور قوية وتغييرها دوريا

تجنب الرد عن الرسائل التي تطلب معلومات شخصية أو فدية

التثبت من هوية المرسل قبل فتح البريد

ضرورة فحص المرفقات بإستخدام مضاد فيروسات قبل فتحها

تفعيل خدمة المصادقة الثنائية عند فتح الحساب

لعبة الكلمة المفقودة

KALI - CERT - IPS - VIRUS - WEB - MPLS - SERVEUR - DNS - ADSL - SWITCH

V	I	R	U	S	B	O
W	E	B	A	D	S	L
K	A	L	I	D	N	S
I	P	S	C	E	R	T
S	W	I	T	C	H	T
S	E	R	V	E	U	R
N	M	P	L	S	E	T

B O T N E T

ISSN: 2811-6437