مجلة الأبحاث في الحماية الاجتماعية
ISNN2716-8182/EISSN : 2772-3009
Vol.3-N°1/2022

الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة

La cybersécurité: Dangers, menaces et défis nécessitant des pratiques, des recommandations et des stratégies spécifiques

ساعــد بـوقـــرص

جامعة العلوم والتكنولوجيا هواري بومدين ، Saad.Boukers@Gmail.com

تاريخ الاستلام : 01 ماي 2022 **تاريخ القبول** : 23 ماي 2022 **تاريخ النشر**: 22 جوان 2022

الملخص

ان الفضاء السيبراني هو فضاء إفتراضي أو رقمي أُنشأَ عن طريق الترابط الموجود بين جميع أجهزة الميكروكمبيوتورات والهواتف الذكية والأجهزة اللوحية والأشياء المُتصِلة بالإنترنيت في العالم كله. يُعتبر الفضاء السيبراني سلاح ذو حدين لما يحتويه من فوائد من جهة ومن مخاطر وتهديدات من جهة أخرى خاصة وأن الجرائم السيبرانية أصبحت مُركبة ومُعقدة وخطيرة جدًا. بالإضافة لمخاطر الفضاء السيبراني المُتعددة، فللأمن السيبراني هو الآخر تحديات كثيرة ومُعقدة ويصعب على الكثير من المؤسسات التغلب عنها خاصة وأنها في تزايد مُستمر هذه السنوات الأخيرة. ان هذه الوضعية الجديدة للدول والمؤسسات والمنظمات والأفراد تتطلب تقنيات وتطبيقات وممارسات سليمة ضمن استراتيجية شاملة ودقيقة ومضبوطة تأخذ بعين الإعتبار كل الإحتمالات المُمكنة وبدون إستثناء للوقاية من مخاطر وتهديدات هذا الفضاء الجديد.

نقترح في هذه المقالة بعض المُمارسات السليمة أو الجيدة للوقاية من التهديدات السيبرانية وكذا بعض التوصيات لتقوية الأمن المعلوماتي لمؤسسة ما أو لبلد ما كالجزائر على سبيل المثال.

الكلمات المفتاحية

الفضاء السيبراني، التهديد السيبراني، الجريمة السيبرانية، الأمن السيبراني.

Résumé

Le cyberespace est un espace virtuel ou numérique créé par l'interconnexion mondiale de tous les micro-ordinateurs, smartphones, tablettes et objets connectés. Le cyberespace est une arme à double tranchant en raison de ses avantages d'une part et de ses dangers et menaces d'autre part, d'autant plus que la cybercriminalité est devenue évolutive, complexe et très dangereuse. En plus, des multiples dangers et cybermenaces du cyberespace, la cybersécurité a également de nombreux défis complexes que de nombreuses entreprises ne peuvent les surmonter, d'autant plus qu'ils sont en hausse ces dernières années. Cette nouvelle situation pour les États, les entreprises, les organisations et les individus exige des techniques, des processus et des bonnes pratiques via une stratégie globale prudente et bien pensée en prenant en compte toutes les possibilités - sans exception- pour prévenir les dangers et les menaces de ce nouvel espace.
Dans cet article, nous proposons quelques recommandations et bonnes pratiques pour renforcer davantage la sécurité informatique d'une entreprise ou d'un pays comme l'Algérie.

Mots clés

Cyberespace, cybermenace, cybercriminalité, cybersécurité.

1. مقدمـــة

لقد أصبحت الجريمة السيبرانية الشُغل الشاغل للدول والمؤسسات والمنظمات والأفراد هذه السنوات الأخيرة خاصة مع بروز فضاء جديد للحروب يُعرف بالفضاء الخامس خاص بالحروب الإلكترونية والسيبرانية والنفسية أو المعلوماتية.

للوقاية من مخاطر هذا الفضاء والذي هو في توسع آني ودائم فعلى المُختصين في الأمن السيبراني أخد بعين الإعتبار كل التدابير اللّازمة للوقاية من مخاطر هذا الفضاء الرقمي خاصة وأن المُجرمون السيبرانيون أصبحوا يعتمدون بالدرجة الأولى على استغلال نقاط ضعف العنصر البشري ثم الابداع والإعتماد على الذكاء الاصطناعي لما له من مزايا.

تم تنظيم هذه المقالة على النحو التالي: يتناول القسم الثاني بعض المفاهيم الأساسية كما نعرض وبإختصار نواقل الهجمات السيبرانية مع إعطاء بعض الأمثلة لهجمات سيبرانية في القسم الثالث. القسم الرابع مُخصص لعرض التحديات التي يعاني منها الأمن السيبراني. نناقش في

القسم الخامس بعض الممارسات الجيدة أو السليمة للوقاية من التهديدات السيبرانية متبوع ببعض التوصيات في القسم السادس وخاتمة عامة في القسم السابع.

2. مفاهيم أساسية

نتطرق في هذا القسم الى بعض المفاهيم الأساسية كالفضاء السيبراني والجريمة السيبرانية والتهديد السيبراني والأمن السيبراني.

1.2. مفهوم الفضاء السيبراني

1.1.2. تعريف الفضاء السيبراني

الفضاء السيبراني هو فضاء إفتراضي، أُنشأَ عن طريق الترابط الموجود بين جميع أجهزة الميكروكمبيوتورات والهواتف الذكية والأجهزة اللوحية والأشياء المُتصِلة بالإنترنيت وكل ما بها من معلومات وبرمجيات في العالم كله. يعتبر هذا الفضاء بالفضاء الخامس للحروب بعد الفضاءات البري والبحري والجوي والفضائي (BOUKERS, Le DICDTIC3, 2021).

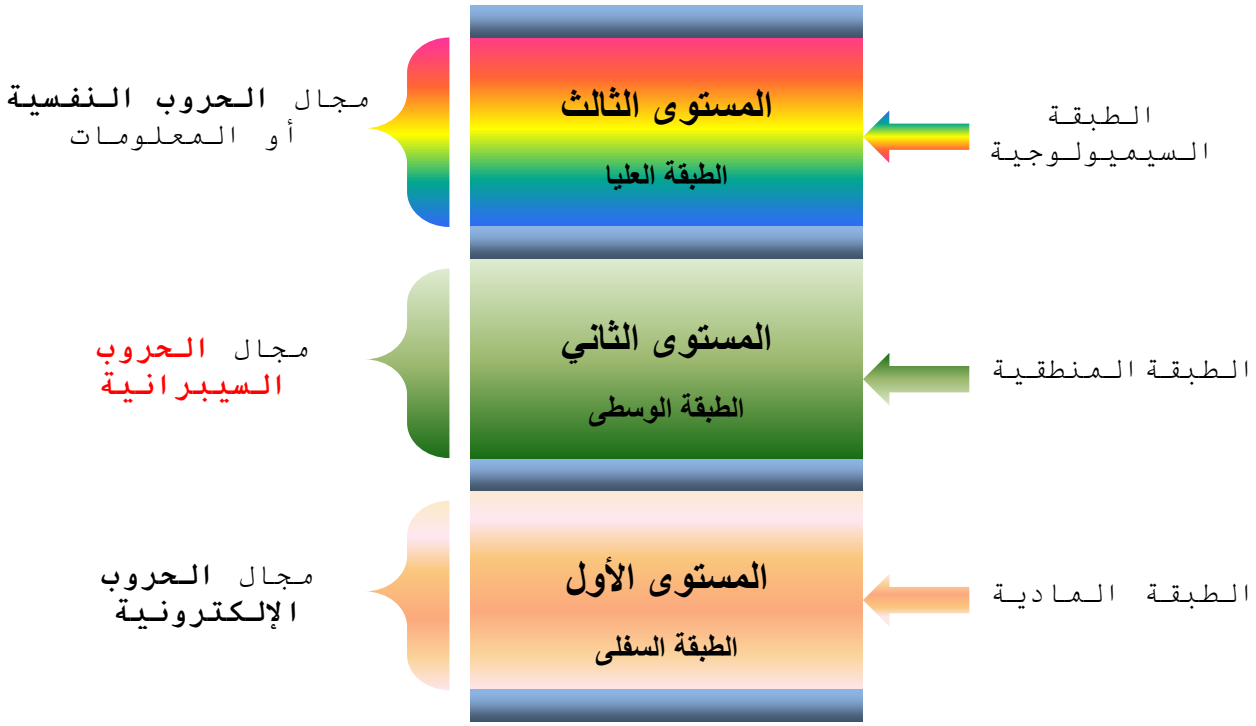
2.1.2. مكونات الفضاء السيبراني

يتكون هذا الفضاء الرقمي من ثلاثة طبقات كما هو موضح في الشكل (01) :

- **الطبقة المادية** وهي تُمثل كل ما هو مادي كالمنشآت والشبكات والميكروكمبيوتورات والخوادم والأشياء المُتصِلة بالإنترنيت...الخ. تُكوّن هذه الطبقة مجالاً للحروب الإلكترونية.

- **الطبقة المنطقية** وهي تشمل أنظمة الإستغلال والتطبيقات والبروتوكولات...الخ. تُمثل هذه الطبقة مجالًا للحروب السيبرانية.

- **الطبقة السيميولوجية** وهي تتكون من كل المحتويات (بيانات ومعلومات ورسائل...الخ) التي يطلع عليها مُستعملي الفضاء السيبراني أو يتبادلونها. تُعتبر هذه الطبقة مجالًا للحروب النفسية أو المعلوماتية.



الشكل 1 : طبقات الفضاء السيبراني

3.1.2. خصائص الفضاء السيبراني

للفضاء السيبراني خصائص كثيرة ومُتعددة وكل منها يمكن أن تُعتبر من مزاياه أو من مساوئه أو الإثنين معاً في بعض الحالات. نذكر على سبيل المثال ما يلي:

- فضاء مُعقد وواسع الإنتشار وسهل الولوج إليه ومُتغير وقابل للتوسيع آنياً.
- فضاء للتبادلات والمواجهات بين الفاعلين.
- فضاء إدارته لامركزية للغاية.
- فضاء تكون فيه التبادلات والتطورات سريعة.
- فضاء به خصوم متعددين ومنقلبين للغاية.

- فضاء يمكن أن يحتوي على هجمات سيبرانية معقدة والكشف عنها وعن مرتكبيها صعب.
- فضاء مُترابط كلياً وجميع حلقات سلسلته يمكن أن تُصاب بهجمة سيبرانية.

2.2. مفهوم "الجريمة السيبرانية"

الجريمة السيبرانية هي كل عمل ضار يحدث في الفضاء السيبراني كالإحتيال ونشر محتويات غير قانونية والهجمات التي تستهدف منظومات الإعلام للمؤسسات أو للأفراد بغرض التجسس أو التخريب أو الإبتزاز أو التأثير السلبي على الرأي العام.

وفقًا لـلباحث الفرنسي الأستاذ Colin ROSE ، فإن الجريمة الإلكترونية هي التهديد الأكبر الثالث للقوى العظمى وذلك بعد الأسلحة الكيميائية والبكتريولوجية والنووية.

3.2. مفهوم " التهديد السيبراني"

1.3.2. تعريف التهديد السيبراني

التهديد السيبراني هو برنامج ضار آت من الفضاء السيبراني يهدف إلى المساس بأمن الميكروكمبيوتورات والهواتف الذكية والأجهزة اللوحية والشبكات وغيرها من الأشياء المُتصلة بالأنترنت. يمكن أن يكون مرتكب التهديد السيبراني شخصًا أو دولة أو مجموعة قراصنة أو منظمة ذات أهداف جيوسياسية (BOUKERS, Introduction à la micro-informatique, 2021).

2.3.2. دوافع التهديدات السيبرانية

للتهديدات السيبرانية دوافع كثيرة ومتعددة نذكر منها على سبيل المثال ما يلي:

1 – التجسس في الميدان العسكري والصناعي؛

2 – الإبتزاز من أجل الحصول على فدية أو شيء آخر مادي أو معنوي؛

3 – التخريب؛

4 – تسجيل وجهة نظر؛

5 – الشهرة أو إظهار بعض الحقائق؛

6 – الإنتقام وتلطيخ السمعة أو المصداقية؛

7 – التحدي.

3.3.2. مخاطر التهديدات السيبرانية

للتهديدات السيبرانية هي الأخرى مخاطر كثيرة ومتعددة نذكر منها على سبيل المثال ما يلي:

1 – إعتراض البيانات؛

2 – إتلاف وتخريب البيانات؛

3 – سرقة الهويات الرقمية؛

4 – تعطيل المصالح والخدمات؛

5 – التجسس؛

6 – الإبتزاز؛

7 – التحايل والتصيُّد؛

8 – التأثير السلبي على الرأي العام.

4.2. مفهوم "الأمن السيبراني"

الأمن السيبراني هو مجموعة من التقنيات والممارسات الجيدة تهدف إلى حماية الأجهزة والبيانات والبرامج من الهجمات السيبرانية (BOUKERS, Introduction To Micro-informatics, 2021).

بصفة عامة فالأمن السيبراني يهتم بتأمين منظومات الاعلام الحساسة ومكافحة الجريمة السيبرانية وكذا الدفاع السيبراني.

5.2. مفهوم "الأمن المعلوماتي"

ان الأمن المعلوماتي هو أشمل من الأمن السيبراني لأنه يهتم بالأمن السيبراني بالإضافة الى تأمين كل ما هو مادي من منشآت وأجهزة من السرقة والتخريب والولوج الغير مرخص له والكوارث الطبيعية والغبار والرطوبة وما الى ذلك.

♦ الأهداف الرئيسية للأمن المعلوماتي

الأهداف الرئيسية الأربعة للأمن المعلوماتي هي السلامة والسرية والتوافر وعدم النكران أو التنصُّل.

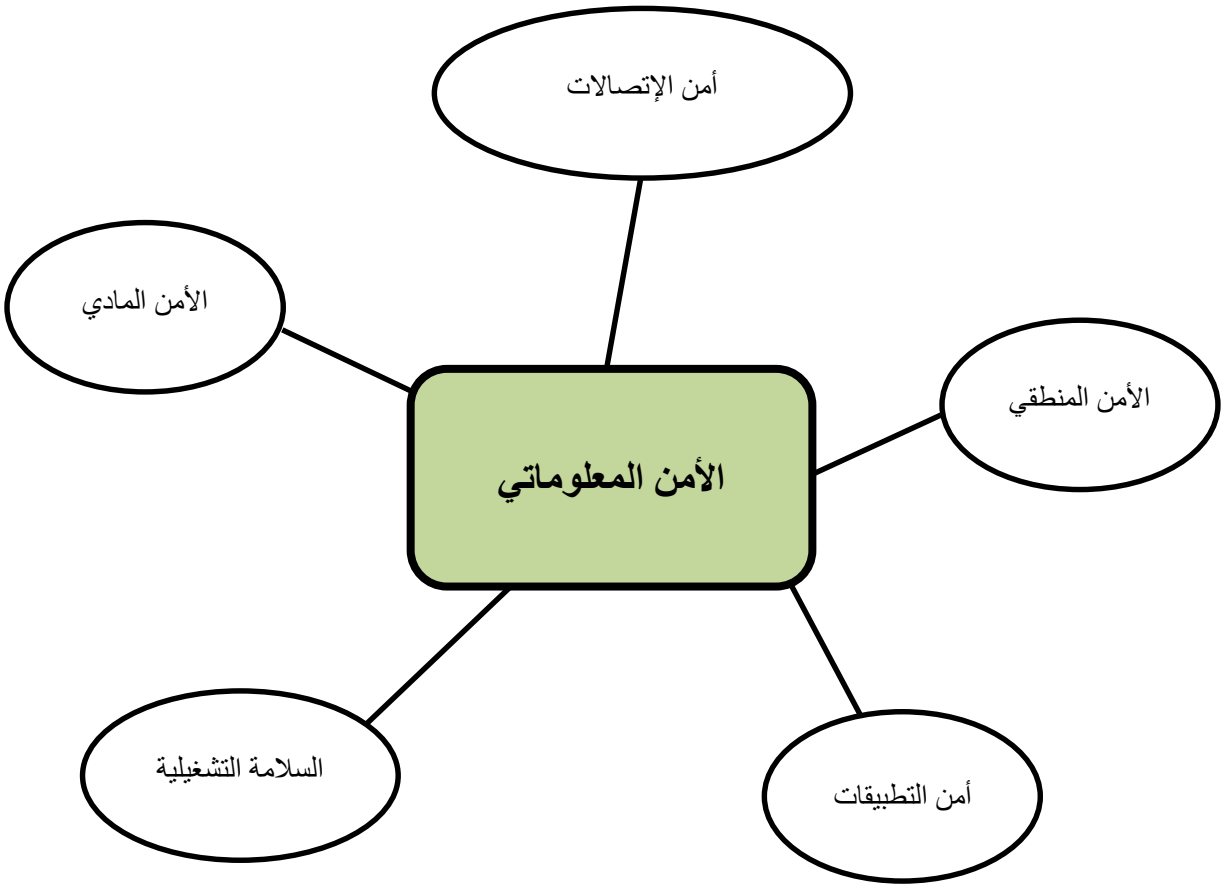
• **السلامة** وهي عملية تضمن التمثيل الدقيق والغير مُتغير لمعلومة أو لنظام معلوماتي ما بحيث أنها تضمن بأن أية معلومة أو أي نظام معلوماتي لا يمكن تعديلهما إلا من طرف المُستخدمين المُرخص لهم وكذا العمليات المُرخص لها أيضاً.

• **السرية** وهي عملية تهدف الى جعل المعلومات المُتبادَلَة خلال عملية تبادل معلومات غير مفهومة لأي شخص غير معني بهذه العملية. يتم ضمان سرية المعلومات المُرسلة أو المُخزنة بإستخدام تقنيات التشفير.

• **الوفرة** هو صفة نظام معلوماتي قادر دائما على الحفاظ على خدمته أي دون إنقطاع.

• **عدم التنصُّل** (أو عدم النكران) هو خاصية نظام معلوماتي قادر على ضمان عدم إنكار مُعاملة مُنفذة من قبل أحد المشاركين فيها أي ضمان توفير الدليل عند الحاجة.

بشكل عام، يتم قياس أمن نظام معلوماتي من خلال أمن أضعف عناصره أو حلقاته ولهذا فالسياسة الأمنية الفعّالة يجب أن تأخذ بعين الاعتبار وبشكل أساسي كل عناصر المجالات الخمسة للأمن المعلوماتي المذكورة في الشكل التالي:



الشكل 2 : المجالات الرئيسية للأمن المعلوماتي

بالإضافة إلى هذا فالأمن المعلوماتي الشامل يجب أن يكون مصحوبا بقانون متطور ومرن لمُكافحة الجريمة السيبرانية بفعالية. كما يجب أن يكون مصحوب أيضا بتسيير جيد للمعلومة جوهره إدارة المخاطر المتعلقة بالميكرومعلومة وما إلى ذلك.

للتذكير فان نظام تسيير أمن المعلومة هو الهدف الرئيسي للمعيار الدولي ISO 27001 ، الذي يحدد خصائصه (feelagile, s.d.g).

3. نواقل الهجمات السيبرانية

يستغل المجرمون السيبرانيون وسائل وقنوات مختلفة للوصول الى أهدافهم الضارة بالضحايا. بصفة عامة، يمكننا تجميع نواقل الهجمات السيبرانية في الثمانية أنواع التالية:

1.3. الثغرات أو نقاط الضعف في الأنظمة والتطبيقات والشبكات والويب

على سبيل المثال، بالنسبة للبرمجيات أو التطبيقات فالثغرة الأمنية هي عيب أو نقطة ضعف في برنامج أو في تكوينه أوفي تثبيته تَسمح لمُجرم سيبراني بتقويض أحد الأهداف الرئيسية للأمن السيبراني المذكورة أعلاه.

2.3. الثغرات الخاصة بالعنصر البشري (Vulnérabilités humaines)

ان نقاط الضعف الخاصة بالعُنصر البشري وعاداته الرقمية السيئة كثيرة جدا بحيث أنه يُمثل أكبر نقطة ضعف للأمن المعلوماتي وكذا الأمن السيبراني.

3.3. التحايل الاجتماعي (Ingénierie sociale)

التحايل الإجتماعي أو ما يُعرف بفن الإقناع هو ممارسة التحايل للحصول على معلومات أو أموال من شخص طبيعي أو معنوي عن طريق عمليات الإحتيال النيجرية أو الرئيس المدير العام (Arnaques nigériennes ou au président).

4.3. التصيُّد الإحتيالي (Phishing ou hameçonnage)

التصيُّد الإحتيالي هو نوع من عمليات الإحتيال عبر الفضاء السيبراني تهدف إلى الحصول على معلومات شخصية تحت ستار شركة أو منظمة ذات مصداقية ومعروفة لمستخدمي الفضاء السيبراني. المثالان الآتيان يوضحان بأن خيال المحتالين لا حدود له.

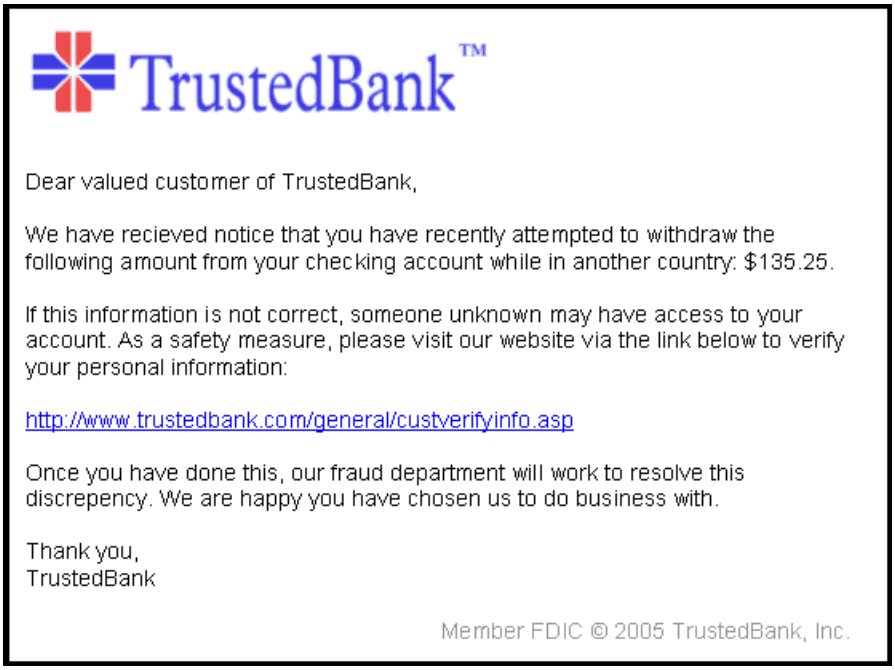
المثال الأول : شهدت سنة 2018 حملة تصيد إحتيالي متطورة باستخدام إسم النطاق حيث أُرسلت فيها آلاف الرسائل النصية القصيرة تَعِدُ مُتلقيها بتذكرتان للسفر مجانيتان على خطوط شركة الطيران الجوية الفرنسية بمناسبة احتفالها بالذكرى السنوية الـ 85 كما هو موضح في النص التصيُّدي الآتي :

الشكل 3 : نص تصيُّدي استهدف زبائن شركة الخطوط الجوية الفرنسية (Filiponne, 2018)

فكما نلاحظ فموقع الهاكر يختلف عن موقع الخطوط الجوية الفرنسية في حرف واحد فقط حيث أنه استعمل حرف من الحروف الأبجدية الصوتية وهو حرف a تحته نقطة كما هو مُشار اليه في الرابط التصيُّدي مما يجعل عملية كشف الإحتيال صعبة جدا.

عند الضغط على الرابط يطلب الهاكر من الضحايا إدخال معلومات شخصية لقرصنتها.

المثال لثاني وهو خاص أيضا بحملة تصيد إحتيالي أخرى استهدفت زبائن بنك " Trust Bank" والحيلة المذهلة التي استخدمها الهاكر هي إضافة حرفان"ed" لإسم البنك "Trust**ed** Bank" كما هو موضح في النص التصَّيدي الآتي :


TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

الشكل 04 : نص تصيُّدي ثاني استهدف زبائن بنك Trust Bank

نستخلص من خلال هذين المثالين بأن نكون جد منتبهين ومركزين بشكل خاص للطبيعة الجذابة أو الغير عادية لنص بريد إلكتروني. وبالتالي يجب عدم الثقة في أي عملية تتطلب إدخال معلومات شخصية ومصرفية. في حالة الشك يوصى بعدم الرد على مثل هذه الرسائل ولا يُنقر على الروابط ولا تفتح المرفقات.

وحتى نضع القارئ العزيز في الصورة فحسب دراسة قام بها نادي خبراء المعلومات والأمن الرقمي الفرنسي CESIN

(Club des Experts de la Sécurité de l'Information et du Numérique) فإن 80% من الشركات الفرنسية قد أُستهدفت بعمليات التحايل التصيُّدي كما هو موضح في الشكل الإحصائي التالي :

الشكل 5 : الهجمات الإلكترونية الأكثر شيوعا ضد الشركات (Gaudiaut, 2021)

5.3. وسائط التخزين المحمولة.

6.3. رسائل البريد الإلكتروني التي تحتوي على مرفقات مُصابة أو روابط ضارة.

7.3. الملفات الموزعة.

8.3. تحميل التطبيقات والملفات المُصابة.

4. تحديات الأمن السيبراني

بالإضافة الى مخاطر الفضاء السيبراني الكثيرة والمتعددة فللأمن السيبراني هو الآخر تحديات كثيرة ومتنوعة وهذا ما يُؤكد بأن **الخطر صفر** أو **الأمن 100%** في ميدان الأمن السيبراني

غير موجودان وذلك مهما أُتخدت من احترازات وتقنيات. في هذه الفقرة نحاول ذكر وبإختصار أهم تحديات الأمن السيبراني.

♦ الإنسان : ان أكبر وأخطر تحديات الأمن السيبراني هو العُنصر البشري والمُتمثل فيما يلي :

- التمكن من التحكُّم في ردود الفعل العاطفية؛
- السياسة الأمنية معقدة وتستند إلى أحكام بشرية؛
- أنظمة الأمن هي من تصميم الإنسان والإنسان هو الذي يُسيرها ويُثبت معايرها ويستعملها؛
- إساءة استخدام الحقوق : حتى نظام أو تطبيق جيد وموثوق به يمكن أن يتعرض للهجوم من قبل الأشخاص الذين ينتهكون حقوقهم؛
- الموارد البشرية : يُعد نقص المتخصصين في مجال أمن منظومات الأمن تحديًا حقيقيًا للشركات.

♦ المنظمات تُخاطر عند استعمالها للفضاء السيبراني.

♦ التشفير له نقاط ضعف وكلمات المرور يمكن كسرها.

♦ الإبتكار في خدمة الهجمات السيبرانية ولهذا فإن المراقبات التقليدية للمخاطر يجب أن تتكيّف مع التهديدات الحالية والمُستقبلية.

♦ ظهور تقنيات جديدة وبالتالي نقاط ضعف جديدة وباستمرار وحتى للشركات التي لديها موارد لابأس بها.

♦ توسُع وتطور رقعة الهجومات السيبرانية وذلك راجع الى الإرتفاع المذهل لعدد الأشياء المُتصلة بالإنترنيت (IoT) وكذا عدد مُستعملي الإنترنيت من جهة وتهديدات الدول فيما بينها والذي أدى الى تصاعد عدد الحروب السيبرانية والتجسس السيبراني من جهة أخرى.

♦ المرونة السيبرانية بإعتبارها ميزة الشركات التي تتمتع بالقدرة على الإستعداد والتكيُّف مع التهديدات المتطورة وكذلك إسترداد قدراتها بسرعة من الهجمات السيبرانية. في هذا الإطار يُلاحظ عدم إقامة تدريبات حل الأزمات لعدد كبير من الشركات.

♦ القوانين التشريعية في ميدان الأمن السيبراني والتي من المفروض أن تكون متطورة وسريعة تساير وتتكيّف مع تطور الجرائم السيبرانية من أجل مكافحتها في الوقت المناسب.

5. الممارسات الجيدة

بالإضافة إلى التكنولوجيا فالحس السليم والحذر الدائم يسمحا لنا في الكثير من الأحيان تجنب مخاطر الفضاء السيبراني. في هذا الإطار نعرض بعض الممارسات الجيدة التي يجب على مستعمل الفضاء السيبراني أخذها بعين الإعتبار.

♦ السيطرة على ردود أفعالنا العاطفية (الأمن السيبراني للعقل البشري)؛

- كن حذرًا على الإنترنت ؛
- كن حذرًا مع هاتفك الذكي أو جهازك اللوحي مثل الميكروكمبيوتر؛
- كن حذرًا عند استخدام نظام المراسلة الخاص بك؛

♦ كلمات المرور يجب أن تكون مُعقدة وقوية وأن تُغيَّر بانتظام ولكل تطبيق كلمة مرور خاصة به؛

♦ التحيين المُنتظم للبرامج عبر إجراء تسييري للتحيينات مُخطط ومعروف مُسبقاً؛

♦ أن تكون لديك إستراتيجية حفظ البيانات مُنتظمة ومُخطط لها بشكل صحيح ودقيق؛

♦ فصل الإستخدامات الشخصية عن الإستخدامات المهنية؛

♦ عدم تثبيت برامج أو تطبيقات من مواقع غير رسمية؛

♦ استخدام الحلول الأمنية المُثبتة (جدار الحماية والبرامج المُضادة للفيروسات)؛

♦ فحص وتحليل وسائط التخزين المحمولة كاليو اس بي مثلا قبل إستخدامها؛

♦ قم بتنظيف محفوظات التصفُّح بانتظام، سواء على الهاتف المحمول أو الجهاز اللوحي أو جهاز الميكروكمبيوتر الخاص بك بعد كل إستخدام للإنترنت؛

♦ في حالة عدم استعمال كاميرة الويب الخاصة بجهاز الكمبيوتر يستحسن إيقاف تشغيلها حتى لا يستطيع مُجرم سيبراني استغلالها عن بعد لأغراض دنيئة؛

♦ عند نهاية إستعمال البريد الإلكتروني أو تصفُّح الإنترنيت بإستعمال ميكروكمبيوتر مُشترك يجب قطع الإتصال بالموقع أو البريد الإلكتروني ومسح سجل التصفُّح ثم إغلاق البريد الإلكتروني أو موقع الويب.

♦ قبل الدخول في موقع ويب وأخذ معلومات منه يجب محاولة تقييم موثوقيته بالإجابة على الأسئلة: من؟ - ماذا؟ - أين؟ - متى؟ - لماذا؟ وكيف؟

♦ قم بإيقاف تشغيل الميكروكمبيوتر أو الهاتف المحمول أو الجهاز اللوحي أثناء فترات عدم النشاط.

6. التوصيات

♦ إقامة تكوينات توعوية وتحسيسية للموظفين تجاه تهديدات ومخاطر الفضاء السيبراني.

♦ إقامة تكوينات تحسينية دورية ومتخصصة حسب المعايير الدولية للعاملين في مجال الأمن السيبراني.

♦ الشروع في توفير التكوينات المتخصصة في الدفاع السيبراني والأمن السيبراني على مستوى مؤسسات التعليم العالي.

♦ دمج موضوع "الأمن الرقمي" في المتوسطات والثانويات ومراكز التكوين المهني.

♦ دمج موضوع "الأمن السيبراني" في جميع مقررات التعليم العالي.

♦ يجب أن تتمتع كل الشركات بالمرونة السيبرانية من خلال استراتيجية استثمار مُستمر وطويل الأمد في ميدان مكافحة الجريمة السيبرانية. وهذا يعني أن يكون تكييف وسائل المكافحة دائم لمواكبة أو مسايرة تطور الهجمات السيبرانية.

- وضع ميثاق مُحكم وشامل لإستخدام موارد الميكرومعلوماتية على مستوى كل مؤسسة.
- التشريع: التشريع في ميدان الأمن السيبراني يجب أن يكون مرن ويساير التطورات السريعة لهذا الفضاء فمكافحة الجرائم السيبرانية تكون من خلال تشريع مُتطور وسريع يواكب تطورات الهجمات السيبرانية.
- إلزام الشركات والمنظمات والإدارات بأن تُؤمن الحد الأدنى من الحماية من التهديدات السيبرانية وكذا عمليات التعبئة والتحسيس المستمر للعمال.
- وضع **إستراتيجية وطنية شاملة** تلتزم بها كل الإدارات والمنظمات والشركات العمومية والخاصة لقمع الجريمة السيبرانية والوقاية منها.

7. الخاتمة

ان محتوى هذا المقال هو تحسيسي بالدرجة الأولى إتجاه مخاطر وتهديدات الفضاء السيبراني بإعتباره خامس فضاء للحروب بالنسبة للدول والشركات وبعض المُنظمات وحتى الأفراد. بالنسبة لي لن يكون هناك سلام في الفضاء السيبراني حتى نهاية العالم وذلك راجع الى كثرة تحدياته وخاصة التحديات الخاصة بالعُنصر البشري. ان كل ما أستطيع قوله أنه لا يوجد أمن سيبراني مُطلق، ولكن التركيز والتحكُّم في ردود أفعالنا العاطفية من جهة وتعدد الإجراءات المُضادة والمُتتابعة غالبًا ما يقود القراصنة للبحث في مكان آخر خاصة اذا أُمنت كل الحلقات المُكوّنة للأمن السيبراني، لأن الأمن السيبراني لأي منظومة معلوماتية يُقاس بالأمن المُخصص لأضعف حلقاته.

ان الأمن السيبراني لبلدنا العزيز الجزائر وكذا الشركات الوطنية والخاصة وحتى الأفراد يتطلب الإهتمام والتعبئة والتكيُّف مع التطور الآني والسريع للفضاء السيبراني من خلال إستراتيجية وطنية شاملة ومرنة للوقاية ومحاربة الجرائم السيبرانية.

المصادر

BOUKERS, S. (2021). *Introduction à la micro-informatique* (éd. 1ère édition). Baraki, Alger, Algérie: Mitidja Impression.

BOUKERS, S. (2021). *Introduction To Micro-informatics* (éd. 1st edition). Baraki, Algiers, Algeria: Mitidja Impression.

BOUKERS, S. (2021). *Le DICDTIC3* (éd. 1ère édition). Baraki, Alger, Algérie: Mitidja Impression.

Filiponne, D. (2018, 02 19). *Une vicieuse attaque de phishing usurpe Air France*. Consulté le 04 25, 2022, sur https://www.lemondeinformatique.fr/: https://www.lemondeinformatique.fr/actualites/lire-une-vicieuse-attaque-de-phishing-usurpe-air-france-70915.html

Gaudiaut, T. (2021, 07 06). *Les cyberattaques les plus courantes contre les entreprises françaises*. Consulté le 05 01, 2022, sur https://fr.statista.com/: https://fr.statista.com/infographie/15871/types-de-cyberattaques-les-plus-courantes-entreprises-francaises/

Qu'est-ce qu'un SMSI. (2022, 04 29). Récupéré sur https://feelagile.com: https://feelagile.com/quest-ce-quun-smsi/