**الجمهورية الجزائرية الديمقراطية الشعبية**

**وزارة التعليم العالي والبحث العلمي**

**جامعة ابن خلدون- تيارت-**

**كلية** :العلوم الاقتصادية،التجارية وعلوم التسيير

**قسم:** علوم التسيير

**ميدان:** علوم اقتصادية، تجارية وعلوم التسيير

**شعبة:** علوم المالية و المحاسبة

**تخصص:** مالية و بنوك

# مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماستر

**من إعداد الطلبة:**

بوعكاز نصير

بوعكاز سعيد محسن

**تحت عنوان:**

# التأمين من المخاطر السيبرانية

## - تجارب دولية -

**نوقشت علنا أمام اللجنة المكونة من:**

| | | |
|---|---|---|
| **أ. بوجلة ايمان** | **(أستاذ محاضر-ب- -جامعة ابن خلدون تيارت)** | **رئيسا** |
| **أ. يحياوي فطيمة** | **(أستاذ محاضر-ب- -جامعة ابن خلدون تيارت)** | **مشرفا و مقررا** |
| **أ. جحا نبيل** | **(أستاذ مساعد -ب- -جامعة ابن خلدون تيارت)** | **مناقشا** |

**السنة الجامعية : 2023/2022**

# الاهداء

الى الوالد الكريم الذي أفنى عمره في سبيل أن نرقى..

إلى الوالدة الكريمة التي ربت و سهرت لنصل الى ما نحن عليه ..

إلى زوجتي التي تقاسمني  مر الدنيا قبل حلوها ..

الى اخوتي و سندي ..

الى ابنائي  : منار . سيرين . يونس . لؤي .

الى زميلي في العمل و أخي : بن عوالي خليفة

إلى كل من أحبنا و أحببناه أهدي هذا العمل المتواضع

**نصير**

# الاهداء

الى روح الوالدين الكريمين اللذين كانا يأملان ان يريا أولادهما دوما في الطليعة ..

الى زوجتي نصفي الثاني و من حملت معي مشاق الدنيا ..

الى اخوتي الذين تكاتفت معهم للوصول الى بر الأمان ..

الى أبنائي عائشة . عبد الحميد . تسنيم . امين .

الى كل أحبابي و أصحابي كل باسمه و كل من منصبه اهدي ثمرة هذا العمل .

**محسن**

# شكر وعرفان

أولا نشكر المولى عز و جل الذي أمدنا بالصحة و القوة و الصبر لإنجاز هذه المذكرة

ثم نتقدم بالشكر الجزيل للأستاذة المشرفة أولا على قبولها بالإشراف علينا و على تواضعها و صبرها معنا وعلى ارشادها لنا

و الشكر موصول كذلك الى أعضاء لجنة المناقشة لقبولهم مناقشة هذا العمل المتواضع

كل من ساهم في إعداد هذا العمل من قريب او بعيد و لو بكلم تحفيزية شكرا لكم جميعا ...

# فهرس المحتويات

**الاهداء**

**الشكر والعرفان**

## الفهرس :

## الفصل الثاني : التجـارب الدوليــة في مجال التأمين السيبراني

**الملخص**

# المقدمة

لقد أصبح الأمن السيبراني ضرورة حيوية لحماية الأنظمة والشبكات والبيانات من التهديدات الإلكترونية المتزايدة في عصر الرقمنة الذي نعيشه حاليا. خاصة مع تزايد الاعتماد على التكنولوجيا في جميع جوانب الحياة، والذي ترافق معه تزايد التهديدات السيبرانية من حيث العدد والتعقيد، وتشمل هذه التهديدات الفيروسات، والبرمجيات الخبيثة، وهجمات الفدية، والهندسة الاجتماعية، مما يتطلب من الشركات والأفراد تبني استراتيجيات متقدمة للحماية من هذه المخاطر.

وتعود جذور الأمن السيبراني إلى سنة 1971 التي تعتبر سنة فاصلة في مجال كل من الخطر والأمن السيبرانيين حيث ظهر فيها أول برنامج خبيث وأول مضاد للبرامج الخبيثة ، فرسالة " أنا المخادع أمسك بي ان استطعت " بواسطة برنامج " creeper أو "الزاحف" تعتبر أول برنامج ضار، والذي استفز Ray Tomlinsonالذي قام بتطوير برنامج مضاد له أطلق عليه اسمreaper أو " الحاصد" وبذلك بدأت بذلك الملامح الأولى للأمن السيبراني ، وتتوالى السنوات ليتم تطوير أول مكافح فيروسات تجاري سنة 1987 يهدف إلى حماية البيانات الحساسة من السرقة أو التدمير غير المصرح به، مما يعزز استمرارية الأعمال وبناء الثقة بين الشركات وعملائها.

غير أن الأمن السيبراني يبقى غير كاف لضمان الاستقرار والاستمرارية خاصة في مجال الأعمال، الأمر الذي استدعى ضرورة إيجاد حلول إضافية لمواجهة المخاطر السيبرانية والتي تمثلت بالدرجة الأولى في التأمين، حيث ظهر التأمين السيبراني كوسيلة مهمة لدعم الشركات في مواجهة التهديدات السيبرانية، وقد نشأ هذا الأخير سنة 1997، حيث تم تقديم أول وثيقة تأمين سيبراني من طرف شركة American International Group، ويقدم هذا النوع من التأمين تغطية مالية لمساعدة الشركات على التعافي من الهجمات السيبرانية، بما في ذلك تكاليف الاستجابة والتحقيق والتعويض عن الخسائر المالية. يساهم هذا النوع من التأمين في إدارة المخاطر بشكل أكثر فعالية وضمان استمرارية الأعمال حتى في حالة وقوع هجوم سيبراني ، مما يعزز سمعتها ويزيد من ثقة العملاء بها.

لكن، برغم الفوائد العديدة للأمن السيبراني والتأمين السيبراني، تظل هناك إشكالية رئيسية تتعلق بقدرة الشركات، خاصة الصغيرة والمتوسطة منها، على تحمل التكاليف المرتفعة لتطبيق تدابير الحماية وشراء بوالص التأمين. كما أن التحديات المتعلقة بنقص المهارات المتخصصة وتطور التهديدات بشكل مستمر تضيف مزيدًا من التعقيد لهذه المسألة.

**أولا : الاشكالية المحورية**

ضمن هذه الرؤية جاءت إشكالية بحثنا التي تتضمن السؤال الجوهري التالي:

هل يمكن التأمين على كل الأخطار السيبرانية وعلى الآثار المترتبة عنها؟.

**ثانيا: الاسئلة الفرعية :**

- ما المقصود بالأمن والتأمين السيبراني؟
- ماهي أهمية الأمن والتأمين السيبراني؟
- هل يمكن ان يوفر الأمن والتأمين السيبراني الحماية الكافية من المخاطر السيبرانية؟

**ثالثا: فرضيات الدراسة**

1) يمكن التأمين من مخاطر برامج الفدية بطرقة مشابهة للتأمين على الحياة من خلال تحديد مبلغ التعويض عند إبرام عقد التأمين.
2) يعتبر التأمين السيبراني منتج مبتكر لكنه يتم بنفس طرق التأمين الأخرى.

**رابعا : أهداف وأهمية الدراسة :**

تتمثل أهمية وأهداف دراسة الموضوع في مايلي:

1- تحديد مفهوم الأمن السيبراني والتأمين السيبراني.

2- دراسة التحديات التي تواجه الشركات والدول في مجال الأمن السيبراني والتأمين السيبراني.

**خامسا :أسباب اختيار الموضوع**

اخترنا هذا الموضوع لسببين رئيسيين وهما :

1. باعتبار الأمن السيبراني ضرورة حتمية في ظل الاستعمال المتزايد لوسائل الإعلام والاتصال وشبكة الانترنت، يفرض ضرورة حماية الأنظمة والبيانات من التهديدات السيبرانية المتزايدة.
2. أهمية الأخطار السيبرانية فرضت على الشركات النظر بجدية إلى ضرورة التأمين من المخاطر السيبرانية

**حدود الدراسة :**

**الحدود المكانية:**

شركة اكسا(axa) الفرنسية والمجموعة الدولية الامريكية (aig) وشركة صحارى للتأمين ليبيا وشركة (saico)المملكة العربية السعودية وشركة جزائرية للتأمين وإعادة التأمين (caar).

**الحدود الزمانية :**

2022-2023

**منهج الدراسة :**

1- **المنهج الوصفي التحليلي:** لأننا بصدد دراسة ظاهرة ألا وهي الخطر النامي الخطر السيبراني والتأمين على الخطر السيبراني.

2- **المنهج المقارن:** مقارنة بين إنتهاج سياسة إدارة الخطر السيبراني داخل المؤسسة، وسياسية نقل الخطر إلى شركة التأمين. تمت المقارنة بين العقود التقليدية والجديدة )العقد السيبراني للتأمين( مع عمل مقارنة بين مختلف الشروط العامة والضمانات التي تقترحها شركات التأمين) والمقارنة بين تجارب الدول المتقدمة وتجارب الدول العربية والتجربة الجزائرية.

**صعوبات الدراسة:**

- موضوع التأمين السيبراني هو موضوع جديد بالنسبة المتقدمة وقليل نسبيا في الدول العربية ومنعدم في الجزائر.
- نقص المصادر التي تعالج أو التي تتطرق إلى موضوع التأمين السيبراني .

**هيكل الدراسة :**

تناولت دراستنا جانبين: جانب نظري والذي هو الفصل الأول (**الإطار النظر للأمن السيبراني و التأمين من المخاطر السيبرانية)** .

أما الفصل الثاني: تطرقنا من خلاله إلى تحديات الأمن السيبراني في العصر الرقمي فتناولنا فيه التعريف وأشهر قضايا الإختراق السيبراني في العالم المتقدم وتحدثنا عن شركات عالمية التي تعرضت لهجمات الاختراق وأيضا تكلمنا على بعض النماذج ملهمة للتأمين السيبراني من دول متقدمة و كذا تجارب الدول المتقدمة والدول العربية والتجربة الجزائرية في مجال التأمين السيبراني.

# الفصل الأول

# الإطار النظري

# للتأمين السيبراني

**تمهيد :**

يعد الأمن والتأمين السيبرانيان مهمين بشكل بالغ في عصرنا الرقمي المتقدم. مع تزايد استخدام التكنولوجيا والانترنت في مختلف جوانب حياتنا، أصبحت البيانات والأنظمة الرقمية أكثر عرضة للتهديدات والهجمات السيبرانية. يهدف الأمن السيبراني إلى حماية هذه الأنظمة والبيانات من الاختراقات والاختراقات الضارة، بينما يوفر التأمين السيبراني حماية مالية ضد الخسائر الناجمة عن الحوادث السيبرانية مثل الاختراقات والانتهاكات الأمنية وفقدان البيانات.

واجه الأمن السيبراني والتأمين السيبراني تحديات مستمرة نتيجة لتطور التهديدات السيبرانية والتكنولوجيا المتقدمة. هذه التحديات أوجبت على المؤسسات أن تكون مستعدة للتكيف مع هذه التحديات من خلال تبني استراتيجيات أمنية قوية واستثمارات في التدريب والتوعية للموظفين.

## المبحث الأول: ماهية الخطر السيبراني

سنتطرق في هذا المبحث إلى ماهية الأمن السيبراني و التامين السيبراني وذلك من خلال إعطاء تعريفات شاملة عن الأمن السيبراني و التأمين السيبراني .

### المطلب الأول : السيبرانية والخطر السيبراني

إن التطور التكنولوجي الحاصل في مجال الإعلام والاتصال حتم على الدول والهيئات التعامل بالأنترنت الأمر الذي ساهم في تسهيل كل المعاملات بين الدول والأفراد لكن هذا التطور وافقه زيادة في الأخطار المتعلقة بتكنولوجيات الاعلام والاتصال، فأصبحت السيبرانية ضرورية لحماية الأنظمة الإلكترونية من التهديدات السيبرانية المتزايدة. هذه التهديدات، التي تشمل اختراق البيانات وتعطيل البنية التحتية، تتطلب استراتيجيات فعالة لضمان الأمان الرقمي والخصوصية.

#### الفرع الأول : تعريف السيبرانية لغة و اصطلاحا :

لابد لنا أولا من تعريف السيبرانية لغة واصطلاحا حتى يتسنى للقارئ فهم هذا المصطلح الذي يبدو غريبا من أول وهلة وهذا الأمر طبيعي لأن الكلمة ليست عربية وسنوضح في هذا بتفصيل في هذا الفرع.

**أولا: لغة** : كلمة السيربانية جاءت من كلمة(**cyber**) باللغة الإنجليزية، وهي مشتقة من كلمة (**cybernetics**) وتعني (علم التحكم الآلي ) ، وأصل كلمة(**cyber**) من الفعل اليوناني القديم (**kybereo**)وتعني (التوجيه أو التحكم ). وذهب بعض الفقهاء إلى أن هذه التسمية جاءت من كلمة اللاتينية هي(**Cyber**) وتعني الفضاء المعلوماتي[1].

السيبرانية تعريب و ليس ترجمة للكلمة الحديثة .Cyber سيبراني تضاف إلى كلمة أخرى معروفة لتكوين(مصطلح مضاف ومضاف إليه) يتعلق بأجهزة و شبكات الحاسب تمت ترجمة هذا المصطلح (الخطر السيبراني )نسبة للمصطلح في المراجع الفرنسية المتداولة في مجال التأمينات .

[1]مقالة على موقع شركة التعاونية للتأمين ،17/5/2017.

**ثانيا: اصطلاحا:** تتعدد التعاريف المتعلقة بالخطر السيبراني، إلا أنها تتفق في تعريفها للأخطار السيبرانية بأنها:« **أولا** آثار انتهاك البيانات بدون الهجوم على نظام المعلومات، أو **ثانيا** آثار الهجوم على نظام المعلومات أي الدخول غير المشروع لنظام المعلومات[1]» .

**الفرع الثاني :تعريف الفضاء السيبراني:**

الفضاء السيبراني عبارة عن بيئة إلكترونية غير ملموسة معقدة التفاعل يتم فيها بناء نماذج لظواهر أو صور إلكترونية لظواهر شبه حقيقية في التفاعلات والتعاملات البعيدة، فالسيبرة عملية انعكاسية نشطة يعكس فيها مدخلات التفاعلات الإلكترونية في بيئة لا يستطيع الإنسان إدراكها، وبصورة أخرى هي عبارة عن شبكة إلكترونية لمجموعة من الخوادم الإلكترونية حيث تتفاعل هذه الشبكات التي تتوفر فيها قاعدة بيانات، فيما بينها باستخدام وسيلة تواصل افتراضية متجاوزة كل الحواجز الجغرافية والسياسية، سعيا وراء تحسين قدرة الاتصال والتعامل الإلكتروني، كما أنها محاكاة حاسوبية عادة ما تكون في صورة بيئة افتراضية لمستخدمي العالم الافتراضي[2] .

وهناك من عرف الفضاء السيبراني أيضا بأنه عالم افتراضي يتشابك مع عالمنا المادي، يتأثر به ويؤثر فيه بشكل معقد، حيث تقوم العلاقة بين العالمين على نظرة تكاملية تحمل بين طياتها مزايا ومخاطر لا تتوقف، وهناك من وصفه بالذراع الرابعة للجيوش الحديثة إلى جوار القوات البرية والبحرية والجوية، خاصة وأن الأنترنت تشهد معارك حقيقية تدور في هذا العالم الافتراضي، وهناك من يرى أنه يمثل البعد الخامس للحرب، كما يعرف على أنه المجال المادي وغير المادي الذي يتكون من عناصر تتمثل في أجهزة الكمبيوتر والشبكات والبرمجيات وحوسبة المعلومات والمحتوى ومعطيات النقل والتحكم ومستخدمو كل هذه العناصر، حيث تعد هذه العناصر العامل المشترك في جميع محاور استخدام الفضاء السيبراني، سواء أكانت الجهات المستخدمة قادرة على تعظيم قيمها وقدراتها بما في ذلك رفع كفاءة العنصر البشري أم كانت في مرحلة متأخرة[3] .

---

[1]Samia Tibah, Présentation Cyber risques, 2018, https://www.ccr.dz/images/pdf/cyber-risks-ccr.pdf. Accessed 15 Dec 2022.

[2]علي زياد علي: الصراع والأمن الجيوسيبراني في الساحة الدولية، دراسة في استراتيجيات الاشتباك الرقمي، عمان: دار أمجد للنشر والتوزيع، 2020، ص 53 – 54.

[3]نورة شلوش: "القرصنة الإلكترونية في الفضاء السيبراني، التهديد المتصاعد لأمن الدول"، مجلة مركز بابل للدراسات الإنسانية، م،8 ع،(2018) ، ص190.

وتعرف وزارة الدفاع الأمريكية الفضاء السيبراني بأنه: "مجال يتسم باستخدام الإلكترونيات (أي تكنولوجيا المعلومات) والطيف الكهرومغناطيسي في تخزين البيانات وتعديلها وتبادلها عن طريق أنظمة شبكات الاتصال والبنية التحتية المادية المرتبطة بها"، وعلى هذا التعريف تعمل الكيانات المدنية والعسكرية والإرهابية في الفضاء السيبراني لتنفيذ أنشطتها وعملياتها [1]، وبالتالي فالفضاء السيبراني هو استخدام تقنيات التكنولوجيا وكل ما يتعقبها من ذكاء صناعي من طرف الدول أو الوكلاء لتحقيق السيطرة على فضاء القوة السيبرانية، فيه يتم التحكم في كل ما يتعلق بالحياة المدنية والعسكرية، وبذلك يعتبر المجال الخامس لفضاء القوة الاستراتيجية.

تتفق جميع الدراسات أن هذا الفضاء [2]هو بيئة افتراضية تعتمد في بنيتها على التكنولوجية الحديثة في التعامل والتواصل بين العديد من الفواعل سواء كانوا أشخاص أو هيئات حكومية وغير حكومية من خلال شبكة إلكترونية (الحاسوب) لها استقلاليتها عن وسائل الاتصال، بمعنى أخر أن كل المعلومات والمعاملات المتداولة بقدر ما تسهل عملية الاندماج بين كل أجهزة الاتصالات والأقمار الصناعية، والفضاء الإلكتروني، بقدر ما تفتح المجال لعمليات الاختراق[3] .

ومن بين العلماء الذي يعتبره الباحثون بمثابة الأب الروحي والمؤسس لهذا الفضاء، عالم الرياضيات

الأمريكي الأستاذ **نوربرتفينر( winnersNorbert)** سنة **1948** الذي استطاع وضع تعريف دقيق لهذا الفضاء " **علم التحكم والتواصل عند الحيوان والآلة، لنقل الرسائل بين الإنسان والآلة، أو بين الآلة والآلة كما يعتبره علم القيادة أو التحكم في كل منهما** "[4]

[1]هربرت لين: "النزاع السيبراني في القانون الدولي الإنساني"، المجلة الدولية للصليب الأحمر، م 94، ع 886 (صيف 2012)، ص516.

[2]أيريك ليوبولدسيرج لوست : ترجمة فتحي علي زمال، "أمن المعلومات"، المملكة العربية السعودية، مدينة الملك عبد العزيز للعلوم والتقنية، 2014 ، ص 10.

[3] عادل عبد الصادق: "الفضاء الالكتروني والرأي العام ، تغير المجتمع والأدوات والتأثير"، المركز العربي لأبحاث الفضاء الالكتروني: قضاياستراتيجية العدد 2459، 2013 .

[4]Dans son livre "Cybernetics or Control and Communication in the Animal and the Machine", publié en 1947, 2016 -20121 UK, page 16

**الفرع الثالث : أقسام الأخطار و التهديد في الفضاء السيبراني**

بقدر ما تتيح تكنولوجيا المعلومات و الاتصالات ، إمكانات هائلة، وغير مسبوقة، لإنتاجية أفضل فيأقسام الأخطار والتهديد في الفضاء السيبراني جميع القطاعات، للتواصل عبر القارات بالاعتماد على البنية التحتية لهذه التقنيات التي تمثل ارتباطا بين مصالح متعددة، وخدمات مختلفة، وبلدان عديدة، بقدر ما تفتح المجال لتكون عرضة للتهديد ( تهديد مقصود: كالاختراقات والاعتداءات، أو غير مقصود: كالإهمال، وقلة الوعي والإدراك )، قد يعرض أنظمتها المعلوماتية إلى خطر دائم، خاصة وأن التعقيدات الناشئة عما يرتبه العمل الإجرامي لا يفسح الفرصة لتحديد الهوية، ومعرفة مصدر الهجوم أو الاختراق وإمكانية الإثبات رغم القدرات والخبرات المتوفرة في مجال تقنيات المعلومات والاتصالات، لأن إحدى خاصيات الفضاء السيبراني " تبقى مجهولة الهوية "

**1 – الفئة الأولى:** تخص الإطار العام (الدول) : وهي مجموعة الأخطار التي يتعرض لها الأمن القومي[1] في المجالات السياسية، العسكرية، الاقتصادية، والاجتماعية، ويهدد البيئة التحتية والحرجة للدول، وأسواق المال والقطاعات المصرفية، والسلم الدولي، والمنشآت النووية، والمؤسسات الصحية، وقطاعات النقل بكل انواعه: البري والبحري والجوي .

**2 – الفئة الثانية:** وتخص الجوانب الشخصية للأفراد: سرقة البيانات الشخصية، وتسريبها، واستخدامها دون إذن، ودون وجه حق، وسرقة الأموال، واختراق انظمة المعلومات، والاعتداء على الملكية الفكرية، والصناعية، والعلامات التجارية، الاحتيال، والبريد غير المرغوب فيه، والجرائم ضد الأطفال، والمحتوى غير المشروع، وغيرها من المخاطر التي تعتبر جرائم سيبرانية لها علاقة مباشرة بالأشخاص وممتلكاتهم.

## المطلب الثاني :ماهية الأمن السيبراني

ويعني مجموع الإجراءات الواجب اتخاذها من قبل الأجهزة الأمنية أو الأخرى غيرها ذات العلاقة، للمحافظة على سرية المعلومات الإلكترونية، ومنع الاختراقات الفيروسية من أجل ضمان وصول المعلومات

[1] الأمن القومي: هو جميع الإجراءات القانونية، والإدارية، والعسكرية والأمنية، التي تهدف الى حماية بلد معين، ضد اي نوع من التهديدات والأخطار.

الحاسوبية إلى الجهات المختصة في الوقت المناسب، وضمان عدم وقوعها في أيدي الأعداء أو الأصدقاء على حد سواء خصوصا بعد الثورة الهائلة في عالم الاتصالات والتداولات الإلكترونية، حيث شكل هذا النوع من الأمن هاجسا استراتيجيا للقوى العالمية والمتمثلة في الولايات المتحدة الأمريكية والصين وروسيا، إذ تدور في وقتنا الحالي حرب إلكترونية بين هذه القوى من أجل اختراق المعلومات والتأثير على أسعار البورصة والعملات وغيرها من المنشآت[1] .

وتعتمد المجتمعات الحديثة بشكل متنامي على تكنولوجيا الاتصالات والمعلومات المتصلة بالشبكة العالمية، غير أن هذا الاعتماد المطرد ترافقه مجموعة من المخاطر الناشئة والمحتملة التي تهدد وبشكل أساسي الشبكات وأمن المعلومات والمجتمع المعلوماتي وأعضاءه، حيث أن سوء الاستغلال اليومي للشبكات الإلكترونية لأهداف إجرامية يؤثر سلبا على سلامة البنى التحتية للمعلومات الوطنية الحساسة لا سيما على المـــعلومات الشخصية، وهو ما جعل الأمن السيبراني يشكل جزء أساسيا من سياسة أمنية وطنية، وأصبح من المعلوم أن صناع القرار في الولايات المتحدة الأمريكية، دول الاتحاد الأوروبي، روسيا، الصين والهند وغيرها من الدول؛ يصنفون مسائل الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية، إضافة إلى إعلان أكثر من 130 دولة حول العالم عن تخصيص أقسام وسياسات خاصة بالحرب السيبرانية ضمن فرق الأمن الوطني، إذ تضاف جميع هذه الجهود إلى الجهود الأمنية التقليدية لمحاربة الجرائم الإلكترونية والاحتيال الإلكتروني والأوجه الأخرى للمخاطر السيبرانية[2] .

وعليه فإن **الأمن السيبراني** هو مزيج من العمليات والتقنيات الممارسة، والهدف منه حماية البرامج والتطبيقات والشبكات وأجهزة الكمبيوتر والبيانات من الهجوم، ويشمل الأمن السيبراني الأمن المادي للبرامج والتطبيقات والشبكات وأجهزة الكمبيوتر، وأمن غير مادي أو معنوي يتعلق بالبيانات والمعلومات من أي هجوم وأضرار متعمدة وسرقة المعلومات والتحكم في الوصول الصحيح للأجهزة والتطبيقات

[1] مصطفى إبراهيم سلمان الشمري: الأمن السيبراني وأثره في الأمن الوطني العراقي"، مجلة العلوم القانونية والسياسية، م 10، ع. 01، (جوان 2021) ص 164.

[2] علي زياد علي: الصراع والأمن الجيوسيبراني في الساحة الدولية: دراسة في استراتيجيات الاشتباك الرقمي، (عمان: دار أمجد للنشر والتوزيع، 2020) ص56.

والشبكات لحمايتها من الضرر الذي قد يحدث عبر الشبكات[1] في الفضاء السيبراني سواء من طرف الدول أو الفاعلين السيبرانيون الآخرين.

ومن ثم يحظى الأمن السيبراني بأهمية بالغة ذلك أن الحكومات والمؤسسات العسكرية والشركات والمؤسسات المالية والطبية وغيرها تقوم بجمع ومعالجة وتخزين كميات كبيرة جدا من البيانات على أجهزة الكمبيوتر والأجهزة الأخرى، وإن كثير من هذه البيانات معلومات حساسة كونها تتعلق بالملكية الفكرية أو معلومات أمنية أو شخصية أو بيانات مالية، إذ أن الدخول غير المصرح به إلى هذه المعلومات والبيانات له عواقب وخيمة، ولاسيما وأن هذه المعلومات تنتقل بين المؤسسات والشركات عبر الشبكات إلى أجهزة أخرى، ونظرا لارتفاع الهجمات الإلكترونية فإن الدول والمؤسسات والشركات تجد نفسها مضطرة لحماية بياناتها ومعلوماتها، بل أصبحت الهجمات والاختراقات الإلكترونية والتجسس الرقمي يمثلان أكبر تهديد للأمن الوطني لأي دولة في النظام الدولي[2] .

ويقصد بالأمن السيبراني مجموع الأطر القانونية و التنظيمية والهياكل التنظيمية والوسائل التكنولوجية الوطنية والدولية التي تهدف إلى حماية الحقوق والحريات الفضاء السيبراني الوطني كما تركز على حماية بيانات الأفراد ومؤسسات الدولة من الاستخدام غير المصرح به أو أي أذى يلحق بشبكة البيانات[3]

إذن فالأمن السيبراني له 3 جوانب:

- حماية بيانات الأشخاص الإلكترونية
- ومن خلالها حماية الشركات ومؤسسات الدولة وبياناتها وعملائها
- ثم حماية الأمن القومي وسلامة المواطنين ورفاهيتهم وخصوصيتهم لألا تستخدم هذه البيانات بطرق غير شرعية أو ضد أصحابها .

[1] مصطفى إبراهيم سلمان الشمري: الأمن السيبراني وأثره في الأمن الوطني العراقي"، مجلة العلوم القانونية والسياسية، م. 10، ع. 01، (جوان 2021) ص157.

[2] مصطفى إبراهيم سلمان الشمري: مرجع سابق، ص158 – 159.

[3] أكرم القصاص : من هم هاكرز الأنونيموسولماذا تردد إسمهم في الإحتجاجات الأمريكية ،مجلة اليوم السابع، تاريخ النشر 08/06/2020 تاريخ الإطلاع 25/12/2022 .

و يعتبر وجها لإحدى وجوه واقع العلاقات الدولية المعاصرة والتي وضعت مفهوم الأمن الوطني أو القومي كمحرك لهذه العلاقات ومعيارا للسيادة الوطنية كما أصبح هاجسا لكافة الدول اعتبارا بهدفها الأسمى في حماية سلمها وأمنها و التزاما باحترامها للأمن والسلم الدوليين بالموازاة مع محاربة الجريمة الإلكترونية والاحتيال الالكتروني وغيرها من المخاطر التي يأتي الأمن السيبراني على رأسها .

## المطلب الثالث : تعريف الأمن السيبراني

ما تضمنه الفضاء السيبراني من عمليات الدخول والخروج لمختلف مواقع تداول وتخزين المعلومات والبيانات يستوجب بالضرورة خلق قواعد وآليات تثبيت أصول الأمن لحماية هذه المواقع وأنظمتها المعلوماتية لذا يتبادر لأذهان كل ممتهن أو مستخدم لهذا الفضاء طرح السؤال التالي :ما هو الأمن السيبراني؟ .

التعاريف التي سنذكرها ستوضح أن هناك اختلاف في الطرح بين من يعتمد على الخبرة التقنية والميدانية لتفسير الظاهرة (الباحثون ) وبين من يركز على الجوانب التنظيمية والقانونية (الدوائر الحكومية)

**أولا :-بالنسبة للأكاديميين:** يعرف كل من(NeittaanmäkiPekka,LehtoMartti)الأمن السيبراني" على أنه مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها ويتضمن تنفيذ التدابير المضادة المطلوبة أما أستاذ الإتصالات في جامعة كاليفورنيا ريتشارد كمرر Kemmerer Richard ،" يعتبر الأمن السيبراني "مجموعة وسائل دفاعية التي من شأنها كشف واحباط المحاولات التي يقوم بها القراصنة"، وقد أيده في الطرح أحد أهم المختصين في الميدان، الأستاذ "إدوارد أموروزو" Edward Amoroso ،الذي عرفه" بأنه تلك الوسائل التي من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الإتصالات المشفرة .. إلخ ".

**ثانيا :-بالنسبة للدوائر الحكومية:** ركزنا على أهم الفواعل (الدولة والهيئات المختصة) فالولايات المتحدة الأمريكية المستهدف رقم واحد من طرف المجرمين، تعرف وزارة الدفاع الأمريكية الأمن السيبراني

على "أنه مجموعة الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها (الإلكترونية والمادية) من مختلف الجرائم، الهجمات، التخريب، التجسس والحوادث."

وكالة الأمن الرقمي الأوروبية (أول من أصدرت تشريع في هذا المجال[1] ) فعرفته بأنه" قدرة النظام المعلوماتي على مقاومة محاولات الاختراق أو الحوادث غير المتوقعة، التي تستهدف البيانات المتداولة أو المخزنة وفق إطار توافقي .

**ثالثا :- بالنسبة للمشرع الجزائري:** الأمن السيبراني يمثل مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به و سوء الإستغلال واستعادة المعلومات الإلكترونية ونظم الإتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية لحماية المواطنين والمستهلكين من المخاطر في وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة في الفضاء السيبراني[2].

**رابعا : - بالنسبة للاتحاد الدولي للإتصالات :**

"The term "cyber security" refers to various activities such as the collection of tools, policies, security safeguards, guidelines, risk management approaches, training, best practices, and technologies that can be [2]used to protect the cyber environment and the assets of organizations and Users".

العناصر المذكورة في التعريف حصرت الأمن السيبراني بين زاويتين: من حيث الأهداف يعتبر الأمن ذلك النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الإتصالات والمعلومات ويضمن إمكانات الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر و التهديدات كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج ولا تتحول الأضرار إلى خسائر دائمة، من حيث المهمة يعتبر الأمن مجموعة النشاطات ( تجميع وسائل، وسياسات، وإجراءات أمنية، ومبادئ توجيهية،

[1] أول إتفاقية تناولت هذا الموضوع : هي الاتفاقية التي صدرت في بودابست 2001.

[2] المادة الثانية(2)من القانون رقم 09-04 المؤرخ في 09.05.2009 : المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

ومقاربات الدارة المخاطر، وتدريبات، وممارسات فضيلة، وتقنيات) يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين[1] .

الكثير من المختصين يعتبرون هذا التعريف (النص الأصلي باللغة الإنجليزية) بمثابة أرضية إجماع لمختلف التوجهات الفكرية والمهنية، ومن خلالها يمكن إعطاء التعريف التالي: " أن الأمن السيبراني أو الإلكتروني هو مجمل القوانين، الأدوات، النصوص، المفاهيم والميكانيزمات الأمنية وطرق تسيير الأخطار والممارسات التقنية المتعلقة بتكنولوجيات المعلومات والاتصالات المستخدمة لحماية مصالح الدول والأشخاص، ليبقى الهدف في الأخير هي قدرة هذه الأدوات على مقاومة التهديدات المتعمدة من طرف قراصنة المعلومات أو غير المعتمدة من طرف المستخدمين ( الخطأ البشري) وبالتالي التحرر من الأضرار الناجمة عن تعطيل أو سوء استخدام تكنولوجيا المعلومات والاتصالات .

**ويعرف الأمن السيبراني بأنه** "مجموعة من الوسائل التقنية والتكنولوجية والعمليات التي يتم استخدامها لحماية الشبكات و الأجهزة والبرامج والبيانات ومن الهجمات أو التسلل الغير مسموح به "

**ويعرف أيضا بأنه** " أمن تكنولوجيا المعلومات أو حماية المعلومات "

**كما يعرف بأنه** "النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصال كما يحد من الأضرار في حال حصول هجمات أو تهديدات سيبرانية ويعيد الوضع إلى ما كان عليه بأسرع وقت "

## المطلب الرابع:أبعاد الأمن السيبراني

بغية تحقيق أمن قومي متكامل للدول ضد الهجمات السيبرانية يحمل مفهوم الأمن السيبراني أبعادا كثيرة نذكر منها ما يلي :

**أولا –البعد العسكري:**أين يوفر الأمن السيبراني للقوات العسكرية التواصل وتبادل المعلومات و الأوامر عن بعد بشكل آمن مع وجوب أن يكون قادرا على صد أي محاولة إختراق تؤدي إلى تدمير البيانات العسكرية لدولة العدو، بحيث يمس الأمن القومي مثلما حدث في إيران عند إختراق منشآتها النووية[1].

[1] التقرير :الصادر عن الإتحاد الدولي للإتصالات، حول "اتجاهات الإصلاح في الإتصالات للعام 2010–2011 "

**ثانيا-البعد الاقتصادي:** تظهر أهمية الأمن السيبراني بشكل أوسع وأكبر في المجال الاقتصادي لأن الفضاء الالكتروني أصبح أساسا للتعاملات التجارية والمالية والاقتصادية و أصبح الحاسوب أداة لتسيير الصناعة و الاقتصاد وهذا يستدعي الحرص على تحقيقه .

**ثالثا-البعد الإجتماعي** :يأخذ الأمن السيبراني شكلا مهما ومختلفا تماما في المجال الإجتماعي،فقد أصبحت مواقع التواصل الإجتماعي أداة إتصال عالمية بين البشر تمد بالمعلومات و الأفكار ولكن من ناحية أخرى قد عرضت أخلاق المجتمع للخطر من ناحية أنه يمس هوية الأشخاص ويهدد الحقوق والحريات و السلم الإجتماعي وعليه لابد من العمل أولا على تكريس مفهوم الأمن السيبراني ثم توعية الأفراد بمخاطر الإختراق .

**رابعا-البعد السياسي:** قد يشكل الأمن السيبراني وسيلة حماية للمعلومات و الوثائق الأساسية الحساسة لعمل قطاعات الدولة ،وعليه لابد من تحقيقه حتى لا تخلق خلافات دبلوماسية بين الدول،وفي حالات أخطر شهدت العلاقات الدولية حروب فعلية شرسة جراء إختراق الأمن السياسي وأبرز مثال الحرب الروسية الأوكرانية 2022 التي بدأت بحرب سيبرانية إنتهت بحرب فعلية مدمرة .

**خامسا-البعد القانوني** : يمثل القانون أداة ضبط المجتمعات وهو يحمل نفس الوظيفة بالنسبة للفضاء الإلكتروني إذ لابد أن تكرس الدول تشريعات خاصة و أطر قانونية تحدد الأعمال القانونية وغير القانونية في الفضاء الإلكتروني لأن الشيء الملاحظ أن الجريمة الإلكترونية تفتقر للصرامة في التعامل معها سيما بالنسبة للتشريعات الجنائية ،كما أصبح الأمن الإلكتروني حقا جماعيا من الحقوق الحديثة وتفرعت منه عدة حقوق كحق النفاذ إلى الشبكة العالمية للمعلومات وحق إنشاء المدونات الإلكترونية والحق في حماية البرامج المعلوماتية ويقابلها مجموع الالتزامات مثل التزام الإبلاغ عن المخالفات والجرائم خاصة ،كل هذا يتطلب وجود قوانين تواكب هذا التطور .

## المبحث الثاني : أنواع المخاطر السيبرانية القابلة للتأمين.

لمعرفة المخاطر القابلة السيبرانية القابلة للتأمين لا بد من التطرق أولا إلى الخصائص التي يتميز بها الخطر السيبراني .

[1] محمود علي عبد الرحمن إسامة، فاروق مخيمر: الفضاء الإلكتروني وأثره على مفاهيم القوة والأمن والصراع في العلاقات الدولية،مجلة كلية السياسة و الإقتصاد، جامعة محمد البشير الإبراهيمي ،برج بوعريريج، المجلد السادس عشر، العدد الخامس عشر، الجزائر ،2022،ص438.

## المطلب الأول : الخصائص التي يتميز بها الخطر السيبراني

إذا نظرنا الى الخصائص التي يتميز بها الخطر السيبراني يمكننا القول أنه لا يقبل التأمين في الأصل[1] مقارنة بالأخطار الأخرى التي يمكن التأمين عليها. حيث ان هذا النوع من الأخطار لا يمكن التحكم فيه 100% كباقي الأخطار، لأنه يتميز بخصائص أو أسس فنية تختلف عن باقي الأخطار الأخرى .

ومن بين الخصائص التي تتميز بها الكوارث السيبرانية نذكر ما يلي :

**01 –قابلة للتزايد بشكل ملحوظ في المستقبل[2]:** يمكن أن تصل خسائر الهجمات السيبرانية الى خسائر بملايير الدولارات كمتوسط خسارة بمعنى مبلغ مساوي لمبلغ خسائر الكوارث الطبيعية التي لا يؤمنها المؤمنون إلا بعمليات إعادة التأمين عادة. في الوقت الحاضر يمكن التأمين على الأخطار السيبرانية لأن تكلفتها لم تصل للأخطار الكبرى كالكوارث الطبيعية، لكن في المستقبل هناك تخوف على أن تفوق هذه الأخطار قدرة السوق ومن ثم عدم التأمين عليها، فكل شيء مرتبط بعامل الوقت والتطور التكنولوجي والإحصائيات

**02 – أخطار جد مترابطة[3]:** ترابط الأجهزة وأنظمة الإعلام الآلي مع ترابط المستخدمين، يستطيع أن يكون مصدر غموض للمؤمن (ترابط الأنظمة يزيد من ترابط الأخطار السيبرانية نسبيا). ولا يستطيع ضمان الخطر السيبراني عندما تكون الكارثة تفوق قدرته وتهدد شركة التأمين، إلا إن وجدت إعادة تأمين.

**03– عدم وجود قاعدة بيانات إحصائية موثوقة بخصوص التصريح بالكوارث السيبرانية [4]:** غياب قاعدة بيانات إحصائية دقيقة تحرم المؤمنين من أداة عمل أساسية لنمذجة المخاطر السيبرانية ومنها تحديد قسط التأمين المتناسب مع الخطر السيبراني، و تحرم جميع الجهات الفاعلة الاقتصادية في مصدر المعلومات التي من شأنها أن تساهم في زيادة الوعي بالخطر السيبراني

---

[1]Comission Cyber Risk : Rapport : Assurer le risque Cyber, Tome 1, Club des Juristes, 2018, Page 21

[2]Comission Cyber Risk : Rapport : Assurer le risque Cyber, Op Cit, p 22.

[3]Comission Cyber Risk:,Ibid, p 25.

[4]ComissionCyberRisk : Ibid, p 28.

**04 – خسائر كبيرة غير ملموسة، يصعب تقييمها**[1]:الكوارث السيبرانية تحقق ضرر فعال و خسارة مالية كبيرة، لكن الأهم لنا هو خاصية الخطر غير الملموس، فالأخطار الأخرى القابلة للتأمين جلها ملموسة ويمكن رؤيتها بسرعة أو اكتشافها، (كالحريق، أضرار المياه، الصواعق..). لكن الكارثة السيبرانية تكتشف إلا بعد مدة من حدوثها، وبعض الأحيان لا تكتشف أصلا. و المؤمن له يستطيع أن يكتشف الكارثة بعد مدة من حدوثها وهنا تدخل مسألة هل يعتد المؤمن بتاريخ اكتشاف الخطر أو حدوثه في مدة سريان العقد.

**05 – خطر جد صعب التأمين عند تحليله، بسبب تقنية وحساسية المعلومات المتبادلة** [2]:عدم تقييم الخطر جيدا بسبب عدم شفافية المعلومات المتبادلة بين المؤمن والمؤمن له.الكثير من المؤمن لهم لا يصرحون للمؤمن بالمعلومات (الأشياء المعنوية غير الملموسة ذات القيمة الاقتصادية). هذه البيانات، التي تهم جوهر نشاطها وقيمتها (المشاريع الحالية، براءات الاختراع... إلخ)، هي استراتيجية وسرية. فهذا إشكال، فلا يمكن تقييم المعلومات بهذه الطريقة، و لا يتمكن المؤمن معرفة القيمة الحقيقية للشيء المؤمن عليه، عكس التأمينات الأخرى أين يتم التعرف على قيمة الشيء المؤمن عند اكتتاب العقد.

## المطلب الثاني: أنواع المخاطر السيبرانية

### الفرع الأول :المخاطر الداخلية

تتمثل المخاطر السيبرانية الداخلية في التهديدات التي تأتي من داخل المنظمة نفسها، سواء من قبل الموظفين الحاليين أو المتعاقدين أو أي فرد آخر لديه وصول مشروع إلى أنظمة الشركة. هذه المخاطر قد تكون متعمدة أو غير متعمدة، وتشمل عدة أنواع رئيسية:

**1 الأعمال الخبيثة المتعمدة:** يشمل هذا النوع من المخاطر الأعمال التي يقوم بها موظف أو متعاقد عن عمد بقصد إلحاق الضرر بالمنظمة. يمكن أن تتضمن هذه الأعمال سرقة البيانات الحساسة، أو تخريب الأنظمة، أو بيع معلومات الشركة لمنافسين أو جهات خارجية. قد يستخدم المهاجمون الداخليون وصولهم المصرح به لتنفيذ هجمات مثل تحميل البرمجيات الضارة أو تسريب البيانات[3] .

[1]Comission Cyber Risk : Ibid, p 30.

[2]Comission Cyber Risk : Rapport : Assurer le risque Cyber, Op Cit, p 32.

.

[3]إبراهيم صفا : مقال عن التأمين السيبراني ، موقع تك عربي، 19 مارس 2024.

**2 الإهمال وعدم الوعي:** يشكل الموظفون الذين لا يدركون السياسات الأمنية أو لا يتبعونها بشكل صحيح مصدرًا كبيرًا للمخاطر. قد يتضمن ذلك ترك الأجهزة غير مقفلة، أو مشاركة كلمات المرور، أو الفشل في تحديث البرمجيات[1].

**3 سوء الاستخدام المتعمد للموارد:** يحدث هذا النوع من المخاطر عندما يستخدم الموظفون موارد الشركة لأغراض شخصية أو غير مشروعة. قد يشمل ذلك استخدام الشبكة لتنزيل محتوى غير قانوني، أو استغلال البنية التحتية ، مما يمكن أن يؤدي إلى إبطاء الأنظمة وتجاوز القدرات الشبكية .

**4 تهديدات الموردين والشركاء:** قد ينطوي الخطر الداخلي أيضًا على جهات خارجية مثل الموردين أو الشركاء الذين لديهم وصول إلى أنظمة الشركة. إذا لم تكن هذه الجهات ملتزمة بسياسات الأمان بنفس القدر، فإنها قد تشكل تهديدًا داخليًا عن طريق نقل البرمجيات الضارة أو تسريب البيانات دون قصد .

**5 الخروقات العارضة:** تشمل هذه المخاطر الأخطاء البشرية مثل إرسال معلومات حساسة إلى المستلم الخطأ عبر البريد الإلكتروني، أو تحميل ملفات تحتوي على بيانات حساسة من مواقع غير آمنة. هذه الأخطاء يمكن أن تؤدي إلى تسرب البيانات بدون نية ضارة، لكنها تظل تشكل خطرًا كبيرًا على أمن المعلومات[2] .

**الفرع الثاني: المخاطر الخارجية**

أهم الأخطار الخارجية للتأمين السيبراني تكمن في الهجمات على أنظمة الإعلام الآلي بكل أنواعها :

**1-هجمات حجب الخدمة(DDoS)**[3]:يرمز الاختصار DDoSلهجوم حجب الخدمة أو الحرمان من الخدمة وهو أسلوب منتشر وشائع يستخدمه القراصنة عن طريق إغراق المواقع بسيل من البيانات غير اللازمة يتم إرسالها عن بعد[1] .

[1]إبراهيم صفا : مرجع نفسه.

[2] https://wiselyinsure.com/ar/

[3]Distributeddenial-of-service

**2- البرمجياتالخبيثة:** هي برمجية يتم تضمينها أو إدراجها عمدا، في نظام الحاسوب لأغراض ضارة، بدون رضا المالك. فقد تستخدم لعرقلة تشغيل الحاسوب، جمع معلومات حساسة، أو الوصول إلى أنظمة الكمبيوتر الخاصة[2] من الأمثلة عن البرمجيات الخبيثة مايلي : .الفيروساتViruses، أحصنة طروادةTrojans، القنابل الموقوتةLogicBomb، باب المصيدةBackdoor، الديدان worms Computerإلخ...

**3- حصان طروادة(Trojan)** :بكل بساطة حصان طروادة عبارة عن برنامج خبيث، يقوم بالتحكم عن بعد بجهاز أو كمبيوتر شخص قام بفتح هذا البرنامج في حاسوبه.

**4- برامج التجسس(keylogger)**:تسجل برامج التجسس جميع المعلومات، مثال كل ما تقوم الضحية بكتابته، يسجله هذا الفيروس .فإن كتبت على الساعة 12:30 كلمة: السلام عليكم، يسجلها البرنامج ويرسلها إلى المخترق .

**5- برامج نزع الفدية(RANSOMEWARE)**:نوع من البرمجيات الخبيثة، يقوم من خلالها الهاكر، بتشفير ملفات المؤسسة او الشخص الضحية الذي يقوم بفتح البرنامج في حاسوبه و من ثم يطلب منه مبلغ معتبر من المال لكي يقوم الهاكر بفك تشفير ملفاته.وفي هذا الصدد، الفدية كانت محل جدال في موضوع ضمانها من المؤمنين.

من أكبر المؤسسات التي كانت ضحية هذا الفيروسRenaultالفرنسية[3].تشير المعطيات أن 40 % من حواسيب المراقبة الصناعية المستعملة لكاسبارسكي ، اخترق في سنة2017 ناهيك عن الأخطار الأخرى التي تصيب أنظمة المعلومات .

**6- فيروسات جديدة الجيل الأخير:** بيغاسوس(Pegasus)من آخر الفيروسات أو برامج التجسس الذي أنشئه Group NSO هو برنامج سري[1] تم إنشائه لبيعه للحكومات ، لأغراض أمنية و هذا ما صرحت به

---

[1]https://arabic.cnn.com/scitech/2016/12/08/sc-081216-what-ddos-attack. Accessed 15 Dec 2022.

[2] https://ar.wikipedia.org/wiki/برمجياتخبيثة Accessed 15 Dec 2022.

[3] http://www.liberation.fr/planete/2017/05/12/renault-parmi-les-cibles-d-une-cyberattaque-mondiale_1569124 .Accessed 15 Dec 2022.

الشركة . لكن مؤخرا تم استعمالهلاختراق إطارات في دول مجاورة ، الشركة باعت البرنامج و لها لوحة تحكم لعمل تسجيل خروجDisconnectمن نظام حصان طروادة لأي مستعمل للبرنامج لأغراض غير تلك المحددة في البرنامج . و هل نفهم من هذا أن الشركة تتجسس أيضا على ماذا يفعل مستعمل البرنامج ؟ . هناك سؤال تم طرحه أيضا لو تتمكن عناصر إرهابية أو إجرامية من التحكم في البرنامج . اجاب صانعو البرنامج أن هذا غير ممكن لأن البرنامج يباع في شكل جهاز مادي »HARDWARE« و غير مادي .»SOFTWARE« ملايين الدولارات دفعتها الدول لإقتناء هذا النوع من البرامج التي تسمح لها بالتحكم في اجهزة الهاتف بمجرد ضغطة زر عبر ثغرات من نوع Remote code» RCE. execution»

7-**اختراق خطوط اتصال** :VOICE PHREAKINGقيام جماعة من المخترقين باختراق سيرفر يقدم خدمات اتصال، ومن بعد تملكه لرقم الهاتف (هاتف الخادم أو السيرفر)، يقوم بالاتصال بخطوط اتصالاته التي تأخذ أموال مقابل المكالمة (أرقام الهاكر التي تأخذ أرصدة عند الاتصال بها). ومن ثم يضخم فاتورة المؤسسة التي تمتلك سيرفر الإتصال الذي تم اختراقه .

**8- الصفحات المزورة للمواقع، لسرقة بيانات تسجيل الدخول للضحايا(Phishing)**بعد أن يستنسخ المخترق الموقع المراد استنساخه، يقوم بإرسال رابط مزور للضحايا، فتقوم بإدخال معلوماتها ومن تم يلتقطها المخترق.

## المطلب الثالث: الخطر السيبراني والتأمين

### الفرع الأول : المخاطر التي يغطيها التأمين السيبراني

يغطي التأمين السيبراني الخسارة المالية المباشرة للأشخاص أو للشركات بسبب أضرار ناجمة عن حدث سيبراني، والحدث السيبراني هو ببساطة أي وصول فعلي أو مشتبه به غير مصرح به إلى نظام تكنولوجيا المعلومات، أو هجوم إلكتروني، أو انتهاك للخصوصية، والغالبية العظمى من الخسائر المالية هي

[1]Ronen Bergman, "Weaving A Cyber Web Nov2019,https://www.ynetnews.com/articles/0,7340,L-5444998,00.html.Accessed 15 Dec 2022.

خسائر الطرف الأول وتشمل سرقة الأموال، وسرقة البيانات، أو الإضرار بالأصول الرقمية، يشمل التأمين أيضا بشكل عام مساعدة كبيرة في الحوادث السيبرانية وإدارتها قبل وقوع الحادث وبعده[1].

و من التغطيات التي يوفرها التأمين السيبراني نذكر مايلي :

**01 – دعم ما قبل الحادث :** يساعد التأمين السيبراني في إدارة المخاطر السيبرانية ويمنع وقوع الحوادث السيبرانية. يمكن لشركات التأمين توفير إمكانية الوصول إلى خبرات الأمن السيبراني وخدمات استخبارات التهديدات، وإجراء تقييمات لضعف تكنولوجيا المعلومات، وتقديم تدريب للموظفين على الأمن السيبراني، والمساعدة في إدارة كلمات المرور.

**02 – إشعارات العملاء** :عادة ما يطلب من الشركات إخطار عملائها بخرق البيانات، خاصة إذا كان الأمر ينطوي على فقدان أو سرقة معلومات التعريف الشخصية[2] .(PII) غالبا ما يساعد التأمين السيبراني الشركات على تغطية تكلفة هذه العملية.

**03 – استعادة الهويات الشخصية** :تساعد تغطية التأمين السيبراني المنشآت على استعادة الهويات الشخصية لعملائها المتضررين.

**04 – خروقات البيانات** :الحوادث التي يتم فيها سرقة البيانات والمعلومات الشخصية أو الوصول إليها دون الحصول على إذن مناسب.

**05 – استعادة البيانات :** يمكن عقد التأمين ضد المسؤولية السيبرانية الشركات من الدفع مقابل استرداد أي بيانات تم اختراقها بسبب الهجوم.

**06 – إصلاح أضرار النظام**:تغطية تكلفة إصلاح أنظمة الحاسوب المتضررة بسبب الهجوم السيبراني من خلال بوليصة التأمين السيبراني.

**07 – مطالب الفدية** :غالبا ما تشهد هجمات برامج الفدية أن المهاجمين يطلبون رسوما من ضحاياهم لفك تشفير البيانات المخترقة أو استردادها ولو أنه يجب أن يكون آخر الخيارات، بل ويجب التشديد في ذلك بعد

[1]موقع (ifegypt.org) ، نشرة الاتحاد المصري للتأمين ،2017–2021

[2]Personally Identifiable Information معلومات التعريف الشخصية

نفاذ كل السبل والطرق لأجل استرجاعها، حيث من أن بعض حكومات الدول تنصح بعدم دفع الفدية لأن ذلك يجعل هذه الهجمات مربحة للمجرمين.

**08 – معالجة الأضرار الناتجة عن الهجوم** :يساعد عقد التأمين السيبراني المنشأة على دفع ما يلي[1]:

- الرسوم القانونية المتكبدة من خلال انتهاك سياسات أو لوائح الخصوصية المختلفة.
- تكاليف توظيف خبراء في مجال الأمن أو التحليل الجنائي للحاسوب والذين سيمكنونهم من معالجة الهجوم، أو استعادة البيانات التي تم اختراقها، وهذه قد تدفع مرة واحدة، باعتبار أنهم موظفون رسميون في المنشأة.

**09 – تغطية تكاليف ما يلي:**

- استئجار نظام أو شركة معنية بالاتصالات التي تخدم العملاء Call Centre ، وذلك من أجل السرعة في استقبال الاتصالات الواردة عن سبب إنقطاع خدمة المنشأة ، وهذا يعمل على حماية سمعتها ، أو بحسب ما تراه المنشأة في طريقة تعاملها مع عملائها وزبائنها.
- تكاليف استشارات العلاقات العامة في كيفية التعامل مع العملاء حيث لكل عميل تعامل بحسب درجة أهميته، من أجل حماية سمعة المنشأة[2].
- تكاليف التحليل الجنائي.
- أي رسوم قانونية ناتجة عن الاستجابة للهيئات الرقابية والتشريعية للحدث الحاصل، ويعد هذا النوع من التغطية مناسبا بشكل خاص للشركات التي تتعامل أو تخزن أي معلومات شخصية خاصة بعملائها.
- المسؤولية عن الخسائر التي يتكبدها شركاء الأعمال الذين لديهم إمكانية الوصول إلى بيانات المنشأة، أو الأضرار أو التسويات التي يجب عليها دفعها بسبب الدعاوى، أو بمعنى آخر المطالبات المتعلقة بالإصابات الناتجة عن تصرفاتها .
- يمكن أن يوفر التأمين السيبراني غطاء للأعمال التجارية إذا أدى التواجد على الوسائط الرقمية إلى قيام شخص ما برفع دعوى ضد المنشأة بداعي التشهير، أو القذف، أو انتهاك حقوق الملكية الفكرية، وفي حال أثبت القضاء ما قام به المأمن له ، فإن هذا الغطاء

[1] موقع (ifegypt.org) ، نشرة الاتحاد المصري للتأمين ،2017-2021.

[2] موقع (ifegypt.org) ، نشرة الاتحاد المصري للتأمين ،2017-2021.

مناسب بشكل خاص للشركات التي تعتمد على نقل البيانات الرقمية عبر البريد الإلكتروني، أو عبر أية قنوات أخرى .

**10 – تكاليف المسؤولية** :يوفر التأمين السيبراني غطاء للأعمال التجارية إذا أدى التواجد على الوسائط الرقمية إلى قيام شخص ما برفع دعوى ضد المنشأة بداعي التشهير، أو القذف، أو انتهاك حقوق الملكية الفكرية، في حال تم إثبات ذلك .

**11 – الأضرار التي لحقت بالأصول الرقمية** :تحمي هذه التغطية أعمالك من الأضرار التي قد تلحق بالأصول الرقمية، مثل موقع الويب الخاص بك أو صورك. فهو يحمي من فقدان البيانات أو تلفها أو تغييرها وكذلك سوء استخدام برامج وأنظمة الحاسوب .

**12 – انقطاع الأعمال** :هذا جانب مهم في معظم سياسات التأمين السيبراني، حيث إذا أدى فشل تكنولوجيا المعلومات أو الهجوم السيبراني إلى مقاطعة عمليات العمل الشركة ، فستقوم شركات التأمين بتغطية خسارة دخل الشركة خلال فترة الانقطاع، بما في ذلك إذا كان ذلك بسبب زيادة تكاليف ممارسة الأعمال في أعقاب الحادث، ويمكن أن يكون هذا بمثابة شبكة أمان مهمة عندما تتطلع إلى استعادة نمط عملها الطبيعي.

**الفرع الثاني :المخاطر السيبرانية المستثناة من تغطية التأمين السيبراني :**

كما هو الحال مع أي عقد تأمين، من المهم على أي منشأة مراجعة ليس فقط ما تغطيه شركة التأمين الخاصة بها، بل أيضا ما يتم استبعاده، فيجب العمل على النظر في الاستثناءات وكذلك التعريفات والشروط عند فحص العقود، حيث هناك العديد من الاستثناءات التي تعتمد في العقد الخاص بالتأمين السيبراني، والتي هي نفسها موجودة في وثائق التأمين الأخرى مثل الحرب والإرهاب، وهناك أيضا غيرها من الاستثناءات، و التي نذكر منها ما يلي[1]:

**01 – عمليات أمنية سيئة** :إذا حدث الهجوم بسبب سوء إدارة التكوين لدى المنشأة أو وجود عمليات أمنية غير فعالة.

[1]إبراهيم صفا :(المخاطر السيبرانية المستثناة من تغطية التأمين السيبراني) ، موقع تك عربي ،27 مارس 2024.

**02 – الانتهاكات السابقة** :الانتهاكات أو الأحداث التي حدثت قبل قيام المنظمة بشراء عقد التأمين.

**03 – الخطأ البشري** :أي هجوم إلكتروني ناتج عن خطأ بشري من قبل موظفي المنشأة.

**04 – الهجمات الداخلية** :فقدان أو سرقة البيانات بسبب هجوم داخلي، مما يعني أن الموظف كان مسؤولا عن الحادث[1].

**05 – نقاط الضعف الموجودة مسبقا** :إذا تعرضت إحدى المؤسسات لاختراق بيانات نتيجة الفشل في معالجة أو تصحيح ثغرة أمنية معروفة مسبقا.

**06 – تحسينات الأنظمة التقنية** :أي تكاليف تتعلق بتحسين أنظمة التكنولوجيا، مثل تقوية الأنظمة والتطبيقات، والشبكات.

**07 – اختصاص المحكمة** :من المفيد دائما التحقق من المناطق التي ينطبق عليها عقد التأمين، ففي حين أن عقود التأمين التي يتمشراؤها في دولة معينة، قد تشمل مناطق معينة أخرى تم إدراجها في العقد المبرم، وبالتالي أي دولة أو منطقة خارج عقد التأمين كانت سببا فيما حدث فلن تغطى إذا ثبت ذلك من خلال التحليل الجنائي للحدث السيبراني، وبالتالي يتم استبعادها.

**08 – المطالبات المقدمة من الكيانات ذات الصلة** :في حين أن التأمين الإلكتروني سيحمي عملك من فقدان بيانات العملاء وأي مطالبات تنشأ نتيجة لهذه الخسارة، إلا أن عقود التأمين لا تتضمن عادة مطالبات المسؤولية المقدمة من الكيانات ذات الصلة بعملك مثل الموظفين والمقاولين والشركات التابعة المملوكة جزئيا لشركتك، أو أي جهة تم ربطها معك، فعلى سبيل المثال، إذا طلب الموظفون التعويض عن فقدان معلوماتهم الشخصية بعد اختراق البيانات، فلن تتم تغطية ذلك.

**09 – الإصابات الجسدية والأضرار في الممتلكات** :ستحل وثائق التأمين السيبراني محل الخسائر في المجال الرقمي، ولكنها لن تغطي عادة الأضرار التي تلحق بالممتلكات المادية أو الإصابات الجسدية

[1]إبراهيم صفا :مرجع سبق ذكره.

(الوفاة أو المرض أو الإصابة الجسدية) الناتجة عن حادث سيبراني، حيث غالبا ما يتم تغطيتها بواسطة وثائق تأمين أخرى مثل عقد او وثيقة التأمين على الممتلكات أو وثيقة تأمين المسؤولية.

**10 – البنية التحتية الوطنية الحيوية** :يتم استبعاد الخسائر الناجمة عن فشل أو انقطاع البنية التحتية الوطنية الحيوية مثل : الكهرباء والغاز، والمياه، والأقمار الصناعية، والاتصالات، وكما هو الحال مع الحرب والإرهاب، فإن المخاطر كبيرة للغاية وتتجاوز قدرة شركات التأمين على التغطية، فتقوم باستثناء ذلك.

**11 – الحرب السيبرانية** :تعد الخسائر التي تتكبدها الشركات نتيجة للحرب السيبرانية والهجمات السيبرانية التي قد تكون مرتبطة بتصرفات دولة أو حكومة معينة من الاستثناءات الشائعة نظرا لكون المخاطر كبيرة جدًا وتتجاوز قدرة شركات التأمين الفردية.

**12 – الغرامات والعقوبات** :لن يغطي التأمين الإلكتروني الغرامات، أو العقوبات، أو العقوبات الجنائية، أو المدنية، أو التشريعية التي تلتزم شركتك بدفعها قانونا.

من المؤكد أنه ستكون هناك اختلافات في الاستثناءات بين شركات التأمين، لذا من المهم فهم الشروط والأحكام، وبالتالي يجب التحدث إلى وسيط تأمين، أو وكيل تأمين، أو شركة التأمين التي تتعامل معها مباشرة إذا لم تكن متأكدا من الشروط التي تم وضعها في عقد التأمين[1].

## المطلب الرابع :أهم شركات الأمن السيبراني في العالم :

لأجل حماية فعالة و ناجعة لابد للمؤسسات و الشركات و حتى الأشخاص اختيار الشركة المختصة في الأمن السيبراني التي تقدم أفضل الخدمات للتأكد من أنها في حماية من أي هجمات الكترونية .

هناك عدة شركات مختصة في مجال الامن السيبراني في العالم تقدم خدماتها للمؤسسات والشركات والأفراد منخلال حمايتهم من مختلف الأخطار السيبرانية.

[1]إبراهيم صفا : مرجع سبق ذكره.

يوضح الجدول التالي أهم أشهر 10 شركات متخصصة في مجال الأمن السيبرانيوتصدرت "سافير" قائمة أفضل شركات الأمن السيبراني في العالم، وفقًا لتقرير نشره موقع الشركة المتخصصة في التسويق الرقمي "إيندكسي" Indexsy.[1] :

| | | | |
|---|---|---|---|
| | سافير Sapphire | إنجلترا | • تعتبر الشركة التي تأسست عام 1996 واحدة من أقدم مزودي خدمات الأمن وأكثرهم ثقة في السوق.<br>• تقدم "سافير" مجموعة كاملة من خدمات اختبار الاختراق لعملاء كل من القطاعين العام والخاص، والاستفادة من الخبرة المكتسبة على مدار سنوات في هذا المجال لصالح الجميع. |
| **2** | آي بي إم سكيورتي IBM Security | الولايات المتحدة | تركز الشركة التي تأسست عام 1994 على حلول أمن المؤسسات. |
| **3** | مكافي McAfee | الولايات المتحدة | تضم الشركة التي تأسست عام 1987، حلول أمان تتمثل في الحماية السحابية وحماية الأجهزة والشبكات من البرامج الضارة والفيروسات والتهديدات المحتملة الأخرى. |
| **4** | سايبر آرك CyberArk | الولايات المتحدة | تأسست شركة الأمان السحابية عام 1999، وتقدم منتجات حماية للمؤسسات، وحلولاً صناعية. |
| **5** | سيسكو Cisco | الولايات المتحدة | تأسست عام 1984، ونمت لتصبح واحدة من أفضل شركات الأمن السيبراني في العالم، وتوفر أمن الشبكات والحماية من التهديدات. |

[1] https://www.argaam.com/ar/article/articledetail/id/1500023

| | | | |
|---|---|---|---|
| 6 | سي إيه تكنولوجيز CA Technologies | الولايات المتحدة | تأسست عام 1976، وأصبحت شركة الاستشارات الأمنية تابعة لشركة "برودكوم"Broadcom التي تهدف إلى توفير حلول برمجيات البنية التحتية وأشباه الموصلات – في نوفمبر 2018. |
| 7 | آب جارد APPGuard | الولايات المتحدة | تم تأسيسها عام 2011 وهي تعرف بواحدة من أكثر شركات الأمن السيبراني ثقة في العالم. |
| 8 | أفاست Avast | الجمهوريةا لتشيكية | تأسست في 1988، وهي مزود معروف لحلول الأمن السيبراني ولديها مجموعة براءات اختراع متزايدة لتقنيات تحديد المواقع، والتعلم الآلي والذكاء الاصطناعي، واكتشاف البرامج الضارة وحظرها. |
| 9 | سيمانتك Symantec | الولايات المتحدة | تأسست عام 1982، وتركز على الحماية من التهديدات على الجوالات والخدمات السحابية. |
| 0 | أفيرا Avira | ألمانيا | تأسست عام 1986، وتقدم مجموعة من منتجات الحماية من التهديدات تشمل برامج إدارة كلمات المرور، وبرامج مكافحة الفيروسات وغيرها. |

## المبحث الثالث: التأمين السيبراني

عرف بأنه عبارة عن إحدى المنتجات الجديدة في مجال أعمال التأمين يهدف إلى حماية الشركات من المخاطر القائمة الآتية عبر الإنترنت، وبشكل أعم من المخاطر المتعلقة بالبنية التحتية لتكنولوجيا المعلومات وأنشطتها، والتي غالبا لا تغطيها سياسات المسؤولية التجارية ومنتجات التأمين التقليدية.

تعمل تغطية التأمين السيبراني بنفس الطريقة التي تعمل بها الشركات التأمين ضد المخاطر المادية وأية كوارث تعمل على تغطيتها، وهو يغطي الخسائر التي قد تتكبدها المنشأة بسبب الهجوم السيبراني[1].

### المطلب الأول : الدوافع نحو التأمين السيبراني

[1]إبراهيم صفا : مقال عن التأمين السيبراني ، موقع تك عربي، 19 مارس 2024.

من القضايا الشهيرة التي أثارت الانتباه، هجومWannaCryالذي أصاب نظام الصحة في المملكة المتحدة وأوروبا، واختراق شركةEquifaxالأمريكية الضخم الذي تسبب في تسريب معلومات مالية لملايين الأفراد. كما تعرضت شركات التكنولوجيا الكبرى مثل Google و Facebookلهجمات سيبرانية تهددت البيانات الشخصية لملايين المستخدمين.

تتطلب هذه القضايا التحليل الدقيق والاستجابة الفورية، حيث يجب فهم أساليب الهجمات والثغرات المستغلة، واتخاذ إجراءات وقائية ودفاعية فعالة للحفاظ على أمان البيانات والمعلومات الحساسة. إن توسيع فهمنا لهذه القضايا يساعد في بناء استراتيجيات أمنية قوية وتعزيز الحماية ضد التهديدات السيبرانية المتزايدة.

من خلال تحليل القضايا الشهيرة في مجال الاختراق السيبراني، يمكن فهم الأساليب المستخدمة من قبل المهاجمين وتقييم الأضرار التي يمكن أن تحدثها هذه الهجمات. هذه القضايا تلقي الضوء على الضرورة الملحة لتعزيز التأمين السيبراني وتبني استراتيجيات دفاعية فعّالة لمواجهة هذه التهديدات المتطورة.

يوضح في المثالين التاليين وهما لمنشأتين في بريطانيا، الدور الإستباقي الذي يمكن أن يلعبه هذا النوع من التأمين في المساعدة على التعامل مع الحوادث السيبرانية:

**01 – عملية احتيال التصيد:**

لاحظت إحدى شركات العلاقات العامة وجود مشكلة في رسائل البريد الإلكتروني الخاصة بها، وقد قامفريق تقنية المعلومات الخاص بالشركة بتحقيق مبدئي وخلصت إلى أن السبب الأكثر ترجيحا هو أنهناك نشاط ضار، وقد اتصلت الشركة بشركة التأمين الخاصة بها، والتي قامت بدورها بنشر فريق التحليل الجنائي الرقمي الخاص بها في موقع الشركة للتحقيق بالأمر، وأكدت أن الشركة كانت بالفعل ضحية لهجوم البرامج الضارة، وأكدت أيضا أن المتسللين الذين نشروا البرامج الضارة قد تمكنوا من الوصول إلى أنظمة المؤمن عليه، وأن البيانات الشخصية من المحتمل أن تكون معرضة للخطر[1].

وبعد التحقيق في مدى الاختراق، قام فريق تقنية المعلومات في الشركة بإزالة البرامج الضارة وسد الثغرة الأمنية في شبكة الشركة التي سمحت بالاختراق. بعد ذلك قامت شركة التأمين بتعيين مستشار قانوني لتقديم

[1]إبراهيم صفا : مقال عن التأمين السيبراني ، موقع تك عربي، 19 مارس 2024

المشورة للمؤمن له بشأن التزامات الإخطار، ثم قامت بترتيب إخطار الجهة التنظيمية والتشريعية وأصحاب البيانات ذوي الصلة.

**02 – هجوم الفدية:**

أدى هجوم برنامج الفدية إلى تشفير خادم لمطعم بالكامل، مما أثر على سجلات نقاط البيع الخاصة به، بمعنى آخر أنه أصبح غير قادر فعليا على ممارسة مهامه التجارية، وقد ساعدت شركة التأمين المطعم على العودة إلى العمل، وتغطية تكاليف تقنية المعلومات المرتبطة بالترميم وانقطاع الأعمال الذي عانى منه المطعم نتيجة لعدم قدرته على التجارة[1].

من خلال المثالين السابقين يمكننا ان نستخلص الدور الفعال لشركات التأمين بعد التعرض للهجمات السيبرانية . و بعد معرفة العالم بجدية الأمر اصبح الطلب على التأمين يتزايد عاما بعد عام ففي النصف الثاني من عام 2022، ارتفعت شدة المطالبات بالتأمين بنسبة كبيرة بالنسبة للمنشآت الصغيرة، مما يدل على أن ضحايا لهذه الفئة من المنشآت غالبا ما يكونون أهدافا لفرص إيجاد الثغرات و في كل مرة من الممكن اختراقهم وقد تكون تلك الثغرات لم تعالج وبالتالي تصبح طامة على الذين لا يكترثون لهذه المشاكل الرقمية .

أما الشركات الكبيرة فبالتأكيد وضعها يصبح معقد أكثر بحكم معاملاتها و سمعتها إذا لم تقم بما يلزم لتأمين شبكتها .

فكل المنشآت طالما أنها تحمل بيانات عملاء ومنتجات يجب أن تحمي نفسها من أي هجمة سيبرانية متوقعة أو غير متوقعة. [2]

## المطلب الثاني : أهمية التأمين السيبراني

من خلال المثالين السابقين، يتبين لنا كيف أصبح التأمين السيبراني ضروريا وبشكل متزايد لجميع المنشآت، وذلك مع تزايد مخاطر الهجمات السيبرانية ضد البرامج والتطبيقات والأجهزة والشبكات والمستخدمين، وذلك لأن اختراق البيانات أو فقدانها أو سرقتها يمكن أن يؤثر بشكل كبير على الأعمال التجارية، بدءا من فقدان العملاء إلى فقدان السمعة والإيرادات.

[1] إبراهيم صفا :مرجع سبق ذكره .

[2] الجزء الأول :التأمين ضد حوادث الأمن السيبراني (التأمين السيبراني) ، موقع:(tech3arabi.com)

قد تكون المنشآت أيضا مسؤولة عن الأضرار الناجمة عن فقدان أو سرقة بيانات الطرف الثالث، ويمكن لعقد التأمين السيبراني أن يحمي المنشأة من الأحداث السيبرانية، بما في ذلك أعمال الإرهاب السيبراني، وتساعد في معالجة الحوادث الأمنية.

على سبيل المثال نذكر هنا مثالا مهما لاختراق متسللين لشبكة بلاي ستيشن التابعة لشركة سوني في عام 2011، حيث قاموا بسرقة بيانات 77 مليون مستخدم. كما منع الهجوم مستخدمي شبكة الألعاب الإلكترونية من الوصول إلى الخدمة لمدة 23 يوما، وقد تكبدت المنشأة المعروفة عالميا تكاليف تزيد عن 171 مليون دولار كان من الممكن تغطيتها بالتأمين السيبراني، ومع ذلك، لم يكن لديها سياسة من أجل ذلك، مما جعلها أن تقوم بتحمل التكاليف الإجمالية للأضرار السيبرانية[1].

**الفرع الأول : التغطية السيبرانية للشركات**

تعد التغطية السيبرانية ضرورية للشركات بجميع أحجامها وعبر مختلف الصناعات، وفيما يلي بعض الأمثلة على المنشآت التي قد تستفيد من التأمين السيبراني، بما في ذلك الناشئة والصغيرة أيضا[2]:

**01 – المنشآت الناشئة وشركات التكنولوجيا** :غالبا ما تتعامل الشركات الناشئة وشركات التكنولوجيا مع بيانات العملاء الحساسة، وتطور تقنيات مبتكرة، وتعتمد بشكل كبير على الأنظمة الرقمية، وهي معرضة بشكل خاص للتهديدات السيبرانية بسبب بنيتها التحتية الرقمية وقد تواجه مخاطر مالية ومخاطر تتعلق بالسمعة في حالة وقوع حادث سيبراني. ويمكن أن تساعد التغطية السيبرانية في التخفيف من هذه المخاطر.

**02 – المنشآت المالية** :تتعامل البنوك والاتحادات الائتمانية وشركات التأمين والمنشآت الأخرى مع كميات كبيرة من بيانات العملاء الحساسة والمعاملات المالية، وهم يواجهون مخاطر مثل تحويلات الأموال غير المصرح بها، وسرقة الهوية، وهجمات برامج الفدية، يمكن أن يساعد التأمين السيبراني في تخفيف الخسائر المالية والمساعدة في الامتثال للتشريعات والأنظمة النافذة الرسمية.

[1] إبراهيم صفا : مقال عن التأمين السيبراني ، موقع تك عربي، 19 مارس 2024.

[2] موقع (ifegypt.org) ، نشرة الاتحاد المصري للتأمين ،2017-2021.

**03 – المنشآت المعنية بالخدمات المهنية** :غالبا ما تتعامل شركات المحاماة وشركات المحاسبة والشركات الاستشارية وشركات الخدمات المهنية الأخرى مع معلومات العميل السرية. وقد تكون أهدافًا للهجمات الإلكترونية التي تهدف إلى سرقة بيانات العميل أو الملكية الفكرية. يمكن أن يوفر التأمين السيبراني تغطية للنفقات القانونية الناتجة عن انتهاكات البيانات أو انتهاكات الخصوصية أو مطالبات العميل.

**04 – المنشآت الصغيرة والمتوسطة** :قد تعتقد الشركات الصغيرة خطأً أنها أقل عرضة للاستهداف بالهجمات السيبرانية، ومع ذلك، أصبحت الشركات الصغيرة والمتوسطة مستهدفة بشكل متزايد لأنها غالبًا ما تكون لديها موارد أقل للأمن السيبراني ويُنظر إليها على أنها نقاط دخول إلى شبكات أكبر. يمكن أن تساعد التغطية السيبرانية الشركات الصغيرة على التعافي من التأثير المالي للحوادث السيبرانية.

**05 – مقدموا الرعاية الصحية** :يعد قطاع الرعاية الصحية هدفًا رئيسيا للهجمات السيبرانية نظرًا لوفرة السجلات الصحية القيمة للمرضى والمعلومات الشخصية الحساسة. يجب على مقدمي الرعاية الصحية، بما في ذلك المستشفيات والعيادات والممارسات الخاصة، النظر في التأمين السيبراني للحماية من التكاليف المرتبطة بانتهاكات البيانات والعقوبات التنظيمية والدعاوى القضائية المحتملة.

**06 – المنشآت القانونية** :يمكن التأمين السيبراني المنشآت القانونية من التفاوض بنجاح على العواقب المعقدة للهجوم السيبراني وتقليل الأضرار التي تلحق بعملياتها وسمعتها من خلال تقليل المخاطر المالية وتقديم التوجيه المهني. ويمكنه دفع تكاليف الدعاوى القضائية المحتملة، وخدمات مراقبة الائتمان، والرسوم القانونية والاستجابة لخرق البيانات، وتحقيقات التحليل الجنائي الرقمي، وإخطار الأطراف المتضررة، والتكاليف القانونية. بالإضافة إلى ذلك، قد يتم تغطية مدفوعات برامج الفدية والغرامات التنظيمية وخسائر انقطاع الأعمال عن طريق التأمين السيبراني[1].

تحتاج المنشآت إلى تقييم مخاطرها المحددة والتشاور مع أخصائي التأمين لتحديد المستوى المناسب من التغطية السيبرانية المطلوبة، وينبغي أخذ عوامل مثل : طبيعة العمل، وحجم البيانات الحساسة، والاعتماد على التكنولوجيا، ولوائح الصناعة في الاعتبار عند تقييم ضرورة ومدى التغطية التأمينية السيبرانية.

[1] موقع (ifegypt.org) ، نشرة الاتحاد المصري للتأمين ،2017-2021

**الفرع الثاني : كيفية عمل التأمين السيبراني:**

تتم عملية تأمين السيبراني بشكل مشابه لأشكال التأمين الأخرى، حيث يتم بيع السياسات من قبل العديد من الموردين الذين يقدمون أشكالا أخرى من التأمين التجاري، مثل التأمين ضد الأخطاء والسهو، والتأمين ضد المسؤولية، والتأمين على الممتلكات. غالبا ما تتضمن وثائق التأمين السيبراني تغطية الطرف الأول، أي الخسائر التي تؤثر بشكل مباشر على المنشأة، وتغطية الطرف الثالث، أي الخسائر التي تتكبدها المنشآت الأخرى بسبب وجود علاقة عمل مع المنشأة المتضررة[1].

ويساعد عقد التأمين السيبراني المنشأة على دفع أي خسائر مالية قد تتكبدها في حالة وقوع هجوم إلكتروني أو خرق للبيانات. كما أنها تساعدهم على تغطية أية تكاليف تتعلق بعملية الإصلاح، مثل دفع تكاليف التحقيق، والتواصل في الأزمات، والخدمات القانونية، والمبالغ المستردة للعملاء .

**الفرع الثالث: الأمن السيبراني وعلاقته بالتأمين سيبيراني :**

يرتبط التامين السيبراني بالأمن السيبراني ارتباطا وثيقا لكن هذا الارتباط يحمل وجهين حدهما سلبي والآخر إيجابي[2].

**أولا : الايجابيات :**

- إن شركات التامين تطالب من يتقدم بالطلب على التأمين بتقديم مجموعة من الوثائق التي تثبت مستوى الأمن السيبراني لديها لذا فإن ضمان توافر الأمن السيبراني ضرورة حتمية للحصول على التأمين السيبراني متوفر ولابد من أن يكون مستوى هذا الأمن مرتفع ،كما أنه بالنظر إلى مفهوم العوامل المساعدة على تحقق الخطر ومدى تأثيرها على قرار شركات التأمين بقبولها للتأمين على الخطر من عدمه فإننا نجد الأمن السيبراني كأحد العوامل المساعدة التي تركز عليها شركة التأمين ومن هنا نجد أن التأمين السيبراني يساهم في زيادة الأمن السيبراني.

[1] موقع (ifegypt.org) ، المرجع نفسه.

[2] نتيجة قراءات وحصيلة علمية.

- يساهم الأمن السيبراني في تحسين فعالية التأمين السيبراني من خلال تعزيز التشخيص المبكر للتهديدات، وتطوير استراتيجيات الحماية الفعالة، وتنفيذ تدابير الوقاية والاستجابة المناسبة. وبالتالي تعزيز القدرة على التحمل والاستجابة للتهديدات السيبرانية بشكل أفضل وفعال

**ثانيا: السلبيات:**

- **ارتفاع التكاليف** :قد يكون التأمين السيبراني مكلفًا بالنسبة للشركات والمؤسسات، خاصة إذا كانت تعتمد على سياسات شاملة تشمل تغطية واسعة النطاق. هذا يمكن أن يؤدي إلى زيادة التكاليف العامة والتأثير على الأرباح.
- **مخاطر التحريض** :قد يؤدي وجود تأمين سيبراني شامل إلى زيادة المخاطر التحريضية، حيث يمكن للمؤسسات الشعور بالاطمئنان إلى أنها مغطاة تمامًا من خلال التأمين، مما قد يؤدي إلى انخفاض الحذر والاستعداد للتعامل مع التهديدات السيبرانية بشكل فعال.
- **تقليل الاستثمارات في الأمن السيبراني** :قد يؤدي الاعتماد على التأمين السيبراني إلى تقليل الاستثمارات في الأمن السيبراني بشكل عام، حيث يمكن للشركات أن تعتمد بشكل كبير على التأمين كحلاً للتعويض عن الخسائر بدلاً من تكثيف جهود الوقاية والتدابير الأمنية.
- **الاعتماد الزائد على التأمين** :قد يؤدي الاعتماد الزائد على التأمين إلى إهمال الجوانب الأخرى من إدارة المخاطر السيبرانية، مثل التوعية الأمنية للموظفين وتطوير سياسات الأمان القوية، مما قد يجعل الشركة أكثر عرضة للهجمات السيبرانية.

من أجل تفادي هذه النقاط السلبية، يجب على الشركات والمؤسسات أن تتبنى نهجًا متوازنًا يجمع بين الاستثمار في التأمين السيبراني وتعزيز الأمان السيبراني من خلال تحسين الممارسات وتعزيز الوعي الأمني للموظفين[1].

## المطلب الثالث :عقد التأمين السيبراني:

من خلال هذا المطلب سنحاول فهم تطور عقود تأمين الإعلام الآلي إلى غاية العقد السيبراني للتأمين، وكذلك التعريف بهذا العقد وهذا ما تم تسمتيه بالإطار المفاهيمي للعقد السيبراني للتأمين.

[1] نتيجة قراءات وحصيلة علمية.

عقد تأمين أخطار الإعلام الآلي الكلاسيكي يختلف عن عقد تأمين الأخطار السيبرانية ، لكن عنده نقاط تشابه مع هذا الأخير و منها إختفاء أو فقد المعلومات و كذلك فقد الإستغلال.

**تطور التأمين :** التأمين بدأ بضمان الأجهزة بوثائق تأمين من نوع كسر الماكينات، وهذا الجانب المادي من الإعلام الآلي (ضمان الأجهزة الوظيفية للإعلام الآلي من الأخطار)[1] .

مع مرور الزمن تعقدت المسألة لينتقل إلى ضمان المعلومات نفسها(من المجال المادي الملموس انتقلنا إلى المجال غير المادي، غير الملموس ) وهو الجانب الثاني في تعريف (الإعلام الآلي ).

**الفرع الأول : تعريف العقد السيبراني للتأمين:**

هو عقد تأمين أضرار يكتتب بين المؤمن له و المؤمن ، يدفع الأول قسط تأمين (مبلغ من المال) ، و يدفع الثاني (شركة التأمين) في حال تحقق الخطر المبين في وثيقة التأمين مبلغ تأمين للمؤمن له (مكتتب العقد) أو المستفيد المبين في العقد و ذلك في ضمان الأضرار و المسؤولية المدنية عند رجوع الغير على المؤسسة أو (الشخص الطبيعي ) المؤمن له (تعويض مالي) ، و مساعدة عينية لحل الأزمة السيبرانية (تعويض عيني) و ذلك بإرسال فريق خبراء في الإعلام الآلي عند حدوث الكارثة السيبرانية".

**الفرع الثاني : أركان العقد السيبراني للتأمين:**

1-**إنعقاد العقد السيبراني للتأمين :** (التراضي) ينعقد العقد السيبراني للتأمين ككل عقد تأمين الأشياء، من تلاقي الإيجاب والقبول، أهلية التعاقد، عدم وجود عيوب،الرضا، الشكلية للإثبات فقط وليست شرطا للانعقاد[2].

2-**محل عقد التأمين السيبراني :** عقد التأمين السيبراني ، ككل عقد أشياء محله هو الخطر. الخطر هو القصد الجنائي أو الخطأ الواقع على المعلومات ومنه تسبيب أضرار عدة للمؤمن له، فهذا هو محل عقد التأمين السيبراني. أما محل الشيء المأمن هو المعلومات .ويجب شرح هذا الشيء المأمن المميز عن باقي الأشياء المؤمنة.

3- **معلومات الشيء محل التأمين:**تنقسم إلى أربعة أقسام هي :[1]

[1] Jean Bigot, Traité de droit des Assurances, Assurance Dommages, Chapitre 3 L'Assurance des risques informatiques, Op cit, p 390.

[2] عبد الرزاق بن خروف: التأمينات الخاصة في التشريع الجزائري، دار الخلدونية، القبة القديمة، الجزائر، التأمينات البرية الجزء الأول، 2017 ص 109.

3-1المعلومات ذات الطابع الشخصي:المعلومات ذات الطابع الشخصي هي كل معلومة تتعلق بشخص محدد، سواء كانت معروفة بالفعل أو يمكن تحديدها مباشرة أو غير مباشرة عبر رقم أو عناصر متعددة. تشمل هذه المعلومات الاسم، اللقب، عنوان المنزل، عنوان البريد الإلكتروني، رقم الهاتف، الصور، الفيديوهات، البصمات الرقمية، بطاقات الهوية، وعناوينIP2 ، وغيرها. هذا التعريف واسع ويشمل مجموعة كبيرة من البيانات الشخصية.

**3-2نوع المعلومات الثانية في المؤسسة** : البيانات الاستراتيجية للمؤسسة [3] .

**3-3 المعلومات المرتبطة بالمؤسسة:** معلومات عن صناديق الإستثمار هي محل استهداف من طرف القراصنة أيضا. بمناسبة العناية الواجبة أو التدقيق الإلزامي في المعطيات Due Diligence ، المؤسسات المستهدفة، لها معطيات عن الشركات التي تريد شراءها أو بيعها.

**4-نوع آخر من البيانات الاستراتيجية التي تكون محل استهداف:** بيانات البحث و التطوير...الخ ، بيانات أخرى هي استراتيجية للمؤسسة ومنها:

**4-1** العقود المكتتبة مع الشركاء**Partenaires**لإطلاق خدمة جديدة أو عرض جديد.

**4-2** العقود المكتتبة مع مزودي الخدمة**Prestataire**.

**4-3** الخطة الاستراتيجية أو خطة العمل**PlanBusiness**لتطوير المؤسسة .

**4-4** الإستجابة لنداءات المناقصة **Réponse aux appels d'offres** .

**الفرع الثالث : التزامات المؤمن (شركة التأمين في العقد السيبراني للتأمين):**

هناك ثلاث أنواع كبرى من التغطيات وهي :[4]

**1- ضمانات المساعدة وتسيير الكارثة (تعويض عيني) :**

---

[1] Laure Zicry, Cyber-Risques Le nouvel enjeu du secteur bancaire et financier, Op Cit, P23.

[2]Internet Protocol رقم التعريف الخاص بالجهاز على الشبكة

[3]Laure Zicry, ibid,p26.

[4] Laure Zicry, op cit, p 109.

تكاليف المساعد والمستشار في تسيير الكارثة[1] :

عندما يكتشف المؤمن له (المؤسسة) الكارثة السيبرانية التي حلت به، في غالب الأحوال يقع في حالة هيستيريا لا يستطيع التحكم في الكارثة، فلن يجد سريعا الأشخاص ذات الكفاءة التي تستطيع التحكم في الكارثة. ولن يعرف الالتزامات التي تقع على عاتقه عند حدوث كارثة سيبرانية.

لهذا يجب اكتتاب عقد تأمين سيبراني، لأن من بين الضمانات التي يقترحها هي ضمانات المساعدة، حيث لشركة التأمين خبراء و مختصين في تسيير الكارثة معترف بهم .فتغطي له شركة التأمين مختلف تكاليف هذه الخبرة . و أول شيء تقوم به شركة التأمين هو ارسال الخبراء للتحكم في الأزمة السيبرانية .

**2-ضمانات المسؤولية المدنية:**

انتهاك سرية معلومات زبائن وعمال المؤسسة من طرف الهاكر يبرز أهمية حماية النظام المعلوماتي للمؤسسة. عدم احترام التزامات السرية من طرف المؤسسة يعرّضها للمسؤولية القانونية. تأمين المسؤولية السيبرانية يغطي تكاليف المحاماة ويعوض الضحايا عن الأضرار المالية والمعنوية التي تعرّضوا لها جرّاء الهجمات السيبرانية[2].

**3- تأمين الأضرار :**

المؤسسة التي حلت بها الكارثة، يجب عليها ليس فقط التحكم في الهجمة بل حتى تبرير مسؤوليتها عند رجوع الزبائن التي سرقت معلوماتهم ، ويجب عليها تغطية الأضرار التي أصابتها، لأنها مسؤولة وضحية في نفس الوقت .

تستطيع فقد الإستغلال أي نشاطها يتأثر و تخسر أموال كبيرة في فترة الكارثة السيبرانية لأن نشاطها توقف، و تستطيع أن تخسر أموال أيضا عندما تكون ضحية ابتزاز سيبراني بهجمة لحجب خدمتها أو فيروس نز ع الفدية Extorsion Cyber(DDOS Attack , Ransomeware)

شركة التأمين تغطي كل الخسائر المالية التي تتكبدها المؤسسة المؤمنة لها في فترة الكارثة السيبرانية وتساعدها على إعادة إقلاع نشاطها في أسرع وقت ممكن فتغطي التكاليف الإضافية للإستغلال، وتتحمل أيضا فقد الإستغلال (خسارة هامش الربح).

[1] Laure Zicry, ibid, p 110.

[2]Laure Zicry, Op Cit,p116.

## الخلاصة الفصل:

يعمل الأمن السيبراني والتأمين السيبراني معًا لتوفير حماية شاملة للشركات والأفراد ضد التهديدات السيبرانية، حيث يعمل الأمن السيبراني على منع وتقليل المخاطر، في حين يوفر التأمين السيبراني الحماية المالية في حالة وقوع حادث .

يجب التفكير الفعلي في أمر وثيقة التأمين السيبراني، والحصول على عرض أسعار لذلك، مع العلم أنه لا يزال عالميا سوق التأمين السيبراني حديث العهد، بالنسبة لعالمنا العربي فهو منتشر في بعض دول الخليج كالسعودية والإمارات، وفي ليبيا حديثا، وهذه إشارة مهمة للاهتمام العربي في هذا النوع من أنواع التأمين أما في الجزائر فهو منعدم لذا يجب التفكير بجدية و التعامل بصرامة من أجل اللحاق بركب الأمم في مجال المعلوماتية .

ليس كل شركة تأمين تستطيع تقديم تغطيات تأمينية لهذه الوثيقة المهمة، إلا إذا كانت ملمة بمهام تقنية المعلومات ومخاطرها، وتستطيع القيام بالتغطيات المالية اللازمة، سواء بدفع المطالبات للأطراف المتضررة، أو في عمليات الإعادة لدى شركات إعادة التأمين. وما يجب التوصية به للمنشآت سواء أكانت حكومية أم خاصة، أن هذه الوثيقة من الممكن اعتبارها وثيقة رسمية مهمة للجهات الرقابية والتشريعية .

# الفصـــل الثـــاني

# التجارب الدولية في مجال التأمين السيبراني

**تمهيد:**

تتنوع التجارب الدولية في مجال التأمين السيبراني حسب السياسات والتشريعات المحلية، واحتياجات السوق، ومستوى الوعي بمخاطر الأمن السيبراني.

في العالم المتقدم، تصطدم المنظومات الرقمية المتطورة بتحديات أمنية متنوعة، ومن أبرزها تهديدات الاختراق السيبراني. تتنوع هذه القضايا من تسريبات البيانات الحساسة والمعلومات الشخصية، إلى الهجمات الضارة على البنية التحتية الرقمية، وتعرض الشركات والحكومات لخسائر مالية و خسارة في السمعة.

هذه التهديدات و مع تزايد حدتها حتمت على هاته الدول النظر بعين الاعتباراالى هذا الخطر فيما يلي تحديات الأمان في العصر الرقمي أي تجارب الدول في مجال التأمين السيبراني بدءا بالدول المتقدمة و التي ظهر عندها هذا النوع من الخطر و هذا النوع من التأمين ثم الدول العربية التي بدأت تتعرف تدريجيا على هذا النوع من التأمين أما الجزائر فهي لم تعرف بعد هذا النوع من التأمين فهي متأخرة نوعاما عن الدول العربية و بعيدة عن الدول المتقدمة .

## المبحث الأول : واقع الأمن والتأمين السيبراني على الصعيد العالمي

من خلال هذا المبحث سوف نرى أهمية موضوع التأمين السيبراني من خلال اطلاعنا على أشهر قضايا الإختراق في العالم حيث أن أكبر الشركات العالمية كانت عرضة لهجمات سيبرانية تكبدت من خلالها خسائر ضخمة ثم تطرقنا الى التجارب الدولية في مجال التأمين السيبراني .

### المطلب الأول: أشهر قضايا الاختراق السيبراني في العالم المتقدم :

تحدثنا فيما يلي عن أشهر قضايا الإختراق في العالم لمعرفة مدي جدية الموضوع ثم تناولنا تجارب بعض الدول المتقدمة و تجارب الدول العربية و التجربة الجزائرية في مجال التأمين السيبراني حيث أصبح هذا النوع من التأمينات ضرورة حتمية .

من أشهر الاختراقات الإلكترونية "السيبرانية" القضية التي حازت على أوساط شبكات التواصل الاجتماعي والشوارع الأمريكية وهي قضية التأثير على الانتخابات الأمريكية عام 2016 .

وقد رصد الباحثون في معهد IBM ، أن الخسائر التي تكبدتها الولايات المتحدة بسبب هذه القضية وصلت الي ما يزيد عن 35 مليون دولار أمريكي، وعلى الرغم من توجيه البعض أصابع الاتهام إلى روسيا بتنفيذ تلك الاختراقات إلا أن مهندسي تقنية المعلومات يدركون جيدا أن هذا الاتهام هو (هراء تقني) لا يمكن أن يستند على أي دليل تقني يؤكد لهم صحته أو إثباته وخاصة أن الشخص المخترق مهما كان بسيطاً إلا أنه لا يمكن أن يكون غبياً إلى درجة أن يترك الأثر الرقمي IP واضحاً للعيان، كما أنه يمكنه الاختفاء الكترونياً تحت نطاق أي دولة يختارها سواء عبر مناطق روسيا أو كوريا الجنوبية بينما هو قابع في أحد شقق ميامي أو لوس أنجلس.

أما القضية الأخرى الأكثر شهرة في مجال الجرائم الإلكترونية على مستوى العالم فقد كانت قضايا طلب دفع الفدية PayRansom والابتزاز الإلكتروني Cyber Extortion ،حيث قام كثير من المجرمين الإلكترونيين" الهاكرز Hackers " باختراق أجهزة أشخاص و منظمات وحصلوا من خلال تلك الأجهزة على معلومات حساسة أو وثائق سرية أو وسائط متعددة ثم قاموا بنسخ تلك البيانات إلى أجهزتهم وابتزاز أصحابها بمبالغ مادية حتى يقوموا بإعادة تلك المعلومات لهم، أو حتى يقوموا بعدم نشرها على الانترنت.

## شركات عالمية تحت هجمات الاختراق

هناك العديد من الشركات العالمية التي تواجه هجمات الاختراق على نظمها الإلكترونية والشبكات المعلوماتية. تشمل هذه الشركات البنوك، والشركات التكنولوجية الكبيرة، والشركات الصناعية، والحكومات، وغيرها

أهم الشركات العالمية التي تعرضت للاختراق : [1]

**شركة Target الامريكية :** في ديسمبر 2013 ، كانت شركة Target ، وهي ثالث أكبر سلسلة متاجر أمريكية للبيع بالتجزئة ضحية لهجوم حاد من قراصنة الانترنت ، حيث تعرض 70 مليون عميل إلى اختراق لمعلوماتهم الشخصية ، بما في ذلك تفاصيل حساباتهم المصرفية. ونتيجة لذلك، تعرضت سمعة الشركة لضربة خطيرة.

كلف هذا الهجوم الإلكتروني حوالي مليار دولار أمريكي (خاصة للبطاقات المصرفية التي أعيد إصدارها). وقد خفض هذا الحدث أرباح المجموعة في الربع الرابع من عام 2013 بمقدار 440 مليون دولار أمريكي. استقال الرئيس التنفيذي بعد بضعة أشهر على اثر هذه الحادثة .

في مارس 2015 ، أمر قاضي مينيسوتا شركة Target بدفع 10 مليون دولار أمريكي للعملاء الذين تعرضوا لأضرار بسبب هذا الهجوم.

**شركة eBay الأمريكية العملاقة :** في مايو 2014 ، تعرضت شركة eBay الأمريكية العملاقة لهجوم إلكتروني ادي الى سرقة بيانات 140 مليون حساب مصرفي لعملائها حيث ضمت البيانات المسروقة أسماء وعناوين بريد الإلكتروني وعناوين بريدية وأرقام هواتف وتواريخ ميلاد وكلمات مرور هذا وقد سرقت كلمات مرور موظفين شركة eBay أيضا.

**شركة Sony Pictures :** في 24 نوفمبر 2014 ، اخترق المتسللون أنظمة الكمبيوتر في Sony Picturesفي مواقع مختلفة للشركة ، بما في ذلك مقرها في لوس أنجلوس وأصبحت البيانات المسروقة، بما في ذلك الأفلام الجديدة والمعلومات السرية متاحة للجمهور على شبكة الانترنت.

[1] الهجمات الإلكترونية (السيبرانية) والتأمين(ifegypt.org)

**شركة Orange** : تعرضت شركة المحمول الفرنسية Orange لهجومين عبر الإنترنت في غضون بضعة أشهر في يناير وأبريل 2014 ، حيث تمت سرقة ملايين البيانات الشخصية للعملاء وبلغت تكلفة هذه الحوادث التي تكبدتها شركة Orange أكثر من 24 مليون يورو (29 مليون دولار أمريكي)[1].

**إختراق إلكتروني للخطوط البريطانية للطيران عام 2018** : تقدم رئيس شركة الخطوط الجوية البريطانية للطيران باعتذار عن خرق حدث لنظام الشركة الأمني، ووعد بتقديم تعويضات للعملاء المتضررين ، وقال أن القراصنة شنوا "هجوما معقدا وإجراميا" على موقع الشركة.وقالت الشركة إن بيانات شخصية ومالية تخص عملاء الشركة تعرضت للاختراق ، ووصلت عملية الاختراق الإلكتروني الى نحو 380 ألف عملية شراء تذاكر، ولكن البيانات التي حصل عليها القراصنة لم تشمل تفاصيل الرحلات وجوازات السفر، كما أوضحت الشركة[2].

## المطلب الثاني: سوق التأمين السيبراني

للثقافة التأمينية، يتم التطرق إلى واقع سوق التأمين السيبراني في العالم الغربي والعربي و المحلي.

### الفرع الأول: السوق السيبراني للتأمين في الدول المتطورة

ظهر هذا المنتوج التأميني في الولايات المتحدة الأمريكية أول مرة. أين سوق المعلوماتية كان معروف منذ مدة .[3]

تمت إضافة الحماية على معلومات المستهلكين في أنظمة المعلومات بسرعة نظرًا للمخاطر المتزايدة لتسريب هذه المعلومات. فقد أقرت الولايات المتحدة قوانين لحماية المعلومات الشخصية، والتي تحدد الالتزامات والمسؤوليات على المؤسسات للحفاظ على سرية هذه المعلومات.

تعتبر المعلومات ذات الطابع الشخصي كل معلومة ترتبط بشخص محدد، سواء كانت معروفة بالفعل أو يمكن تحديدها مباشرة أو بطريقة غير مباشرة، فيشمل الاسم، العنوان، رقم الهاتف، والبيانات الأخرى التي يمكن استخدامها لتحديد هوية الشخص .

---

[1] أكبر 10اختراقات للبيانات تم الكشف عنها ، (https://aitnews.com/2018/12/13).

[2] موقع (aitnews.com) مرجع سبق ذكره.

[3] Laure Zicry, Cyber-Risques Le nouvel enjeu du secteur bancaire et financier, Op.cit., p 107.

بدأ عقد التأمين السيبراني في الولايات المتحدة وتم نقله لأوروبا، حيث بدأ السوق ينمو في إنجلترا وانتشر لاحقًا في فرنسا. وقد ازدادت شعبية هذه العقود بعد حدوث كوارث سيبرانية في أوروبا، مثل هجمات Ransomware التي أثرت على العديد من المؤسسات. تغطي عقود التأمين السيبراني الخسائر المالية الناجمة عن الهجمات السيبرانية وتوفر ضمانات متنوعة تتناسب مع آثار هذه الهجمات.

بالنسبة إلى الضمانات[1]. هناك من الزبائن (المؤسسات خاصة والقليل من الأشخاص الطبيعيين) من يشترون قيمة ضمانات ضعيفة بعض الشيء بالنسبة إلى البعض الآخر (2 مليون، 5 مليون يورو)، وهناك من يشتري حتى 100 مليون يورو (المؤسسات الكبرى) .

**الفرع الثاني: سوق التأمين السيبراني في دول العالم العربي**

هناك القليل جدا من الشركات التي تقوم بهذا النوع من التأمينات، بالخصوص في دول الخليج.[2]

**دور الاتحاد المصري للتأمين**[3]يقوم الاتحاد المصري للتأمين بدراسة هذا النوع من التأمين من خلال الحصول من الأسواق العالمية على العديد من وثائق تأمين الجرائم الالكترونية ودراستها باللجان المختصة بالاتحاد لإعداد منتج جديد يتناسب مع السوق المصري .

تعد أكبر مشكلة لترويج هذا النوع من التأمين هي إقناع العملاء بهذا النوع من التأمين وعلى الجانب الآخر تقع المسؤولية على أطراف العملية التأمينية (شركات التأمين والوسطاء والهيئات) كل في دوره لنشر الوعي بين الفئات المستهدفة للتعريف بهذا النوع من التأمين وأهميته في التخفيض من مواجهة هذه المخاطر .

1- **السوق السيبراني في الجزائر (مشروع قيد الإنجاز)** : سوق تأمين أخطار الإعلام الآلي التقليدية (الأجهزة واسترجاع المعلومات) في الجزائر موجود منذ مدة. ومع هذا كانت الشركة الوطنية للتأمين وإعادة التأمين[4]السباقة لإدخال هذا النوع من التأمينات في التسعينات[5] ويضمن حماية أجهزة المؤسسات وأجهزة الأشخاص الطبيعيين، وحتى استرجاع معلوماتهم ومفاتيح البرامج إلخ ...

---

[1]Laure Zicry, op cit, p 108.

[2] https://insurancemarket.ae/cyber-security-insurance,Accessed 15 Dec 2022.

[3] موقع الاتحاد المصري للتأمين,التأمين ضد الجرائم الإلكترونية Blom Alexander. Mr,

[4]Benmicia Youcef, Assurance des risques informatiques, Institution de parrainage : Compagnie Algérienne d'Assurance et de réaussurance (CAAR), Institut de financement du développement du Maghreb arabe, 1992.

[5] 2022, https://caar.dz/tous-risquesAccessed 15 Dec 2022.

هذا بخصوص الأخطار التقليدية التي تضر بالأجهزة (الحريق، السرقة، أضرار المياه، الصواعق ... إلخ)، كلها أخطار ملموسة ويمكن رؤيتها[1].

أما بخصوص موضوعنا، تأمين الخطر السيبراني هو قطاع مستقبلي في سوق التأمين الجزائري، يكون كحل وتهيئة لأرضية رقمنه القطاعات في الجزائر، فالرقمنة لا تخلو من الآثار السلبية.

ليس هناك في الجزائر شركة تؤمن ضد الخطر السيبراني لكن هو مشروع جديد لأن هناك فراغ كبير في هذا القطاع يجب سده، فهناك الكثير من العوائق التي تعيق هذا القطاع حتى في أوربا .

كما تم سن قوانين ومراسيم جديدة تكلمت عن حماية المعطيات ذات الطابع الشخصي، وحماية معلومات الركاب، والمعلومات الإدارية وأنشئت لجنة لحماية الأنظمة المعلوماتية في الجزائر و أنشئت لجنة لحماية الأنظمة المعلوماتية في الجزائر[2] وهناك الكثير من التطور الحاصل في الموضوع

نظمت الشركة المركزية لإعادة التأمين يوم دراسي أو أيام دراسية تتكلم فيها عن الأخطار النامية. والخطر السيبراني بالخصوص، قال رئيس مجلس إدارة الشركة إنه من المهم معرفة نتائج التجارب الأجنبية والسويسرية والفرنسية والألمانية في إدارة المخاطر الجديدة ( الأخطار النامية )[3].

## المبحث الثاني :نماذج عن تأمين الأخطار السيبرانية

نعرض فيما يلي تجربة كل من فرنسا و الولايات المتحدة الأمريكية في مواجهة و تأمين الأخطار السيبرانية من خلال شركتين رائدتين في مجال التأمين هما شركة اكسا الفرنسية و شركة ا اي جي الأمريكية :

### المطلب الأول: نماذج غربية عن التأمين السيبراني

#### الفرع الأول :تجربة فرنسا:

[1] نَبَاشْ مِلْخَيْر نُورْيَا، تأمين المخاطر المعلوماتية، انظر: قسم: تجربة CAAR في المجال، المؤسسة الراعية: الشركة الجزائرية للتأمين وإعادة التأمين(CAAR) ، معهد تمويل التنمية للمغرب العربي، 1992.

[2] مرسوم رئاسي رقم 05-20 ممضي في 20 جانفي 2020 وزارة الدفاع الوطني، يتعلق بوضع منظومة وطنية ألمن الأنظمة المعلوماتية، الجريدة الرسمية عدد4 مؤرخة في 26 جانفي 2020 ، ص 05.

[3] Hiscox, Novembre 2016 Séminaire de la CCR – Alger, https://www.ccr.dz/images/pdf/seminaire1.pdf. Accessed 15 Dec.

في فرنسا ، كانت واحدة من كل شركتين ضحيتين لهجوم من الشركات الصغيرة والمتوسطة في عام 2021. فرنسا هي أيضا أول دولة في الاتحاد الأوروبي تتأثر ببرامج الفدية ، وهي فيروسات تهدد بتدمير بياناتك للحصول على فدية .[1]

الفيروسات والقرصنة والأعمال الخبيثة ... لذلك أصبحت المخاطر السيبرانية حقيقة لا يمكن إنكارها ويمكن أن يكون لها تأثير خطير على عمل الأشخاص و المؤسسات ، لذلك تقدم شركة أكسا للتأمين تغطية شاملة من هاته التهديدات .

وقد أعطينا مثال على ذلك شركة (اكسا) للتأمين فقمنا بتعريف الشركة ثم تحدثنا عن خدمات التأمين السيبراني التي تقدمها هذه الشركة.

**شركة اكسا للتأمين AXA ASSURANCE :**

اكسا هي أكبر شركة تأمين فرنسية في العالم حيث يتجاوز دخلها السنوي 120 مليار دولار وتدير أصول بحوالي تريليون دولار.

بدأت كشركة تعاونية صغيرة قبل أن تنمو بعد قيامها بعدة اندماجات مع شركات تأمين أخرى. شكلت بشكلها الحالي بعد اندماجها سنة 1996 مع اتحاد تأمينات باريس. استحوذت الشركة سنة 2003 على مجموعة موني الأمريكية المتخصصة في مجال التأمين على الحياة في صفقة بلغت 1.5 مليار دولار. في يونيو 2006 اشترت من كراديت سويس شركة فينترفور في صفقة بلغت 10.6 مليار دولار. يدير فرع الشركة الاستثماري أكسا انفست ماناجرس أصولا تفوق 1000 مليار يورو [2].للشركة حضور في 60 دولة . تعد من مكونات مؤشر الكاك 40 الذي يعد من أهم مؤشرات البورصة في باريس لأكبر 40 شركة فرنسية .

**و من بين الخدمات التي تقدمها شركة اكسا للتأمين السيبراني ما يلي :**

- استجابة شاملة للتهديدات السيبرانية الجديدة: سرقة بيانات العملاء ، وانقطاع الأعمال ، والإضرار بسمعة المؤسسات الإلكترونية ... .

[1]RansomwareBarometerjanvier,2021.

[2] Asset Management – Investment Expertise – AXA Investment Managers – Business Highlights". 27-09-2007 /2023-02-12.

- الاستفادة من الدعم للحفاظ على العمل من خلال رقم مخصص يمكن الوصول إليه 7/24 للإبلاغ عن كل المتطلبات وتبادلها مع شبكة خبراء الشركة.
- الاستفادة من التغطية التي تتكيف مع حجم كل الشركات . تم تصميم عقد مخصص لكل من الموظفين والشركات الصغيرة والمتوسطة والشركات الكبيرة ، وكلها معنية بمخاطر تكنولوجيا المعلومات.
- تحديد أصل وآلية ومدى البرامج الضارة المزروعة في نظام الكمبيوتر .
- إزالة البرامج الضارة ومعالجة البيانات المصابة أو التالفة.
- صياغة توصيات لحماية وأمن نظام الكمبيوتر من أجل تجنب حدوث هجمات ضارة جديدة مع تغطية نفقات المؤسسة .
- منذ دخول اللائحة العامة لحماية البيانات حيز التنفيذ ، عندما تتعرض الشركة للهجوم ، يكون لديها التزام قانوني بإبلاغ عملائها لإجراء تكلفة له ، والتي يغطيها عقد هاته الشركة .
- تغطي شركة التأمين خسارة الهامش الإجمالي (وفقا لشروط وأحكام العقد) الناتجة عن انخفاض حجم الأعمال ، إذا كان نتيجة المباشرة في عمل من المعلومات الضارة (بما في ذلك الفيروسات وبرامج الفدية ورفض الخدمة) .

## الفرع الثاني: تجربة الولايات المتحدة الأمريكية

تعتبر الولايات المتحدة الأمريكية الدولة الأكثر عرضة للتهديدات و الهجمات السيبرانية و وعيا منها بذلك فإنها تسعى مثل غيرها من الدول المتقدمة الى ايجاد حلول للتصدي للهجمات السيبرانية بمختلف أنواعها ،كما تسعى كذلك الى تأمين شركاتها و مؤسستها و مواطنيها من مختلف الهجمات التي قد يتعرضون لها خاصة و أن الأنترنت اصبحت تدخل في كل معاملاتها التجارية و المالية و الاقتصادية.

ولتوضيح ذلك أكثر اعطينا مثال بشركة المجموعة الدولية الامريكية للتأمين حيث قمنا بتعريف بالشركة ثم تحدثنا عن بعض النماذج للخدمات و التغطيات السيبرانية التي تقدمها الشركة.

### المجموعة الدولية الأمريكية American International Group, Inc :

تُختصر إلى **AIG**هي شركة تأمين أمريكية متعددة الجنسيات مع أكثر من 88 مليون عميل في 130 بلدا. اعتبارا من عام 2015 توظف شركات AIG حوالي 65،000 شخص .

تعمل الشركة من خلال ثلاث قطاعات AIG :لحوادث الملكيات، AIGالحياة والتقاعد، والشركة المتحدة للضمان .(UGC) تقدم AIG لحوادث الملكيات منتجات التأمين للعملاء الأفراد والتجارية والمؤسسية. توفر AIGالحياة والتقاعد التأمين على الحياة وخدمات التقاعد في الولايات المتحدة .تركز UGC على تأمين كفالة الرهن العقاري والتأمين على الرهن العقاري. كما تقدم المجموعة الخدمات المالية في عمليات أسواق رأس المال العالمية، بما في ذلك الاستثمار المباشر والمصالح المحتفظ بها.

يقع مقر الشركة الرئيسي في مدينة نيويورك، ويقع مقرها المسؤول عن أوروبا والشرق الأوسط وأفريقيا (EMEA) في لندن، ويقع مقرها الآسيوي في هونغ كونغ .وتخدم الشركة 98٪ من شركات قائمة فورتشن 500، و 96٪ من قائمة فورتشن 1000، و 90٪ من فورتشن غلوبال 500، وتقدم خدمات التأمين ل 40٪ من قائمة فوربس 400 لأغنى الأميركيين. وقد احتلت المجموعة المرتبة الأربعين في قائمة فورتشن 500 لعام 2014 .

وفقا لقائمة «فوربس غلوبال 2000» لعام 2014، فإن AIG هي رقم 42 في تصنيف أكبر الشركات العامة في العالم.في 31 مارس 2015، كانت القيمة السوقية لشركة AIG بقيمة 75.04 مليار دولار[1].

سيبرإيدج CyberEdge هي تغطيةالسيبرانية التي تقدمها AIG تتضمن العديد من الحلول المرنة التي تسمح للشركات بالحصول على التغطية السيبرانية التي تتطابق مع متطلباتهم.

فيما يلي بعض النماذج للخدمات و التغطيات السيبرانية التي تقدمها الشركة :[2]

**الاستجابة الأولى First Response**

عندما يشتبه في انتهاك الامن السيبراني ( الالكتروني) فإن معظم الاعمال ليس لديها القدرة على تشخيص المشكلة والاستجابة السريعة لها. تغطية سيبرإيدج للاستجابة الاولي تغطي الوصول في حالات الطوارئ الي مستشار قانوني ومتخصص في تكنولوجيا المعلومات من اللذين يمكنهم تقديم الدعم الحاسم والتنسيق المطلوب[3].

[1]المجموعة الدولية الأمريكية – ويكيبيديا(wikipedia.org) .

[2]الهجمات الإلكترونية (السيبرانية) والتأمين(ifegypt.org) .

[3]المجموعة الدولية الأمريكية ، المرجع سبق ذكره.

**ادارة الحدث Event Management**

بعد الهجوم السيبراني ( الالكتروني) تطلب المنظمات مجموعة من الخدمات لوضع أو الرجوع بأعمالهم مرة اخري للمسار الصحيح.

تدفع سيبرايدج الإدارة الحدث لكل من الخدمات القانونية وتكنولوجيا المعلومات والعلاقات العامة ، كذلك هو الحال لخدمات مراقبة الائتمان والهوية بالإضافة الي ذلك استعادة البيانات وتكاليف الاخطار بالخرق.

**المسئوليات وحماية البيانات Data Protection & Cyber Liability**

تقوم التغطية بالاستجابة لتعويضات ، مطالبات مسئولية الطرف الثالث الناشئة عن الفشل في امن الشبكات ويتضمن ذلك تغطية تكاليف الدفاع ومطالبات ، تعويضات المسئولية الناتجة عن خرق سرية البيانات الي جانب تكاليف الدفاع والغرامات القابلة للتأمين التي تتكبدها الشركة اثناء التحقيقات أو التي تطلب منها من قبل المنظم ، المراقب[1].

**انقطاع الشبكة Network Interruption**

غالبا جميع المستهلكين من الشركات تعتمد على البيع المباشر عبر المواقع الالكترونية وادارة علاقات العملاء Customers Relationship Management وحتي الصناعات التقليدية مثل التصنيع والنقل تتطلب الاتصال بالشبكة للعمل بكفاءة – لذلك فإن تغطية انقطاع الشبكة تغطي فقد خسارة الدخل ونفقات التخفيف عند توقف العمل أو تعليقه بسبب حادث أمن سيبراني، الكتروني.

**انقطاع الشبكة: الاستعانة بمصادر خارجية من مقدمي الخدمات :Network Interruption OSP**

الاستعانة بمصادر خارجية من مقدمي الخدمات Outsourced Service Providers (OSPs) للمؤسسات المتضررة للقيام بأعمال مثل استضافة المواقع – معالجة عمليات الدفع – جمع وتخزين البيانات.

[1] المجموعة الدولية الأمريكية – ويكيبيديا (wikipedia.org).

يمتد ذلك ليشمل تغطية انقطاع الشبكة ليشمل الخسائر وتكاليف التخفيف الناشئة عن استخدام خدمات ال OSP بسبب سقوط الشبكة ، النظام.

**انقطاع الشبكة : فشل النظام Network Interruption: System Failure**

ليس كل فشل أو سقوط بالنظام يكون بسبب خرق الأمن السيبراني، ولكن الانقطاع غير المقصود وغير المخطط بسبب اي عوامل اخري بخلاف الاختراق يمكن أن يؤدي أيضا إلى حدوث خسائر انقطاع الشبكة أو سقوط النظام[1] .

تقدم تغطية فشل النظام ، انقطاع الشبكة تغطية الخسائر وتكاليف التخفيف الناتجة عن فشل ، سقوط النظام الداخلي الذي لا ينشأ عن خرق الأمن السيبراني ولكن يمكن ان يكون بسبب خطأ بشري او مشكلة في البرامج.

**حادثة البيانات الإلكترونية Electronic Data Incident**

خرق الأمن السيبراني الالكتروني ليس هو السبب الوحيد الذي يمكن أن يتسبب في ضياع البيانات أو فسادها.الارتفاع في الطاقة، الكهرباء ، والكوارث الطبيعية، وارتفاع درجة الحرارة والتخريب المادي يمكن ايضا ان يؤدي إلى عدم إمكانية الوصول إلى البيانات .

نموذج تغطية حادثة البيانات الالكترونية يقوم ببساطة بإضافة حادث مؤمن منه الي قسم ادارة الحدث Event Management ويغطي هو الضرر العرضي أو خطر تدمير نظام الكمبيوتر للشركة.

**وسائل الاعلام الرقمية Digital Media**

[1] المجموعة الدولية الأمريكية ، المرجع نفسه .

في بيئة رقمية سريعة التحرك، أصبح من الأسهل الآن اكثر من أي وقت مضى على الشركات أن تنتهك تتعدي عن غير قصد على العلامات التجارية، inadvertentlyinfringe on trademarks، أو تختلس المواد الإبداعية misappropriatecreativematerial، أو تتفحص الحقائق بشكل غير كاف.

تغطي تغطية وسائل الإعلام الرقمية الأضرار والخسائر وتكاليف الدفاع فيما يتعلق بانتهاك حقوق الملكية الفكرية لطرف ثالث أو الإهمال فيما يتعلق بالمحتوى الإلكتروني.

**الابتزاز السيبراني الالكتروني Cyber Extortion**

قد تجد الشركات، الاعمال نفسها هدف لمجرمي الإنترنت الذين يقوموا بتشفير البيانات الخاصة بالشركات ليجبروهم على دفع فدية لشراء مفتاح لفتح هذه البيانات.

يغطي ال Cyber Extortion الخسائر الناجمة عن الابتزاز والتهديد.

وهذا يشمل الفدية لإنهاء الابتزاز فضلا عن الرسوم المتكبدة من المستشارين المتخصصين في الابتزاز السيبراني.

**قرصنة الهاتف Telephone Hacking**

بالإضافة الي القرصنة على الانترنت ، تواجه الشركات قرصنة الهواتف ويشار اليها باتصال الـ PBX من خلال الاحتيال.

هذا ويستهدف المحتالين أنظمة الهواتف لإجراء مكالمات من خلال مجموعة من الارقام المميزة .

وتقدم تغطية القرصنة للهواتف الرسوم المترتبة على الوصول غير المصرح به واستخدام انظمة هواتف الاعمال التجارية .

**جريمة الحاسوب Computer Crime :**

ويقصد هنا استخدام اجهزة الحاسوب في عمليات الغش لتحويل الأموال حيث يستخدم المجرمين التفاصيل التي تم الحصول عليها من خرق الأمن السيبراني لأجهزة الحاسوب لنقل الأموال بشكل احتيالي من حساب في مؤسسة مالية الي حساب اخر في جهة اخري .

يقدم هذا النوع تغطية الخسائر المالية المباشرة من تحويلات الأموال الإلكترونيةالاحتيالية الناشئة عن خرق الأمن السيبراني[1].

## المطلب الثاني : تجارب الدول العربية في مجال التأمين السيبراني

تُواجه الدول العربية، شأنها شأن الدول الأخرى حول العالم، تحديات متزايدة في مجال الأمن السيبراني، ممّا دفعها إلى اتخاذ خطوات لتعزيز قدراتها في هذا المجال، بما في ذلك تطوير برامج التأمين السيبراني.

وتتنوع تجارب الدول العربية في مجال التأمين السيبراني، ونذكر منها ما يلي:

### الفرع الأول :تجربة ليبيا :

للتحدث عن التجربة الليبية في مجال التأمين السيبراني استشهدنا بشركة الصحارى للتأمين كمثال عن شركة تأمين تقدم تأمين سيبراني للمغرب العربي أعطينا نبذة عن الشركة ثم تطرقنا الى التهديدات التي تغطيها هذه الشركة[2].

**شركة الصحارى للتأمين SAHARA INSURANCE COMPANY :**

هي شركة تأمين و إعادة تأمين ليبية تسعى إدارة شركة الصّحَارَى للتأمين إلى الارتقاء والتميز على جميع الأصعدة، ولذا ارتأت الإدارة إلى رفع رأسمالها إلى خمسة عشرة مليون دينار ليبي اعتباراً من عام 2007 علماً بأن الشركة خاضعة لقانون الإشراف والرقابة رقم 3 لسنة 2005 والقانون التجاري الليبي.استكملت الشركة منذ المراحل الأولى إجراءاتها القانونية وبناء جهازها الفني وفق أحدث المستجدات في صناعة التأمين.

[1] المجموعة الدولية الأمريكية – ويكيبيديا(wikipedia.org)

[2] التأمين السيبراني | شركة الصحارى للتأمين (sic.ly).

قامت شركة الصّحَارَى للتأمين بالتعاقد مع أكبر شركات إعادة التأمين العالمية لضمان الجودة والاستمرارية ورضا العملاء وتحقيق أعلى الإيرادات لمساهميها،ثم تعاقدت مع أكبر شركات إعادة التأمين العالمية لضمان الجودة والاستمرارية ورضا العملاء وتحقيق أعلى الإيرادات لمساهميها.

إن شركة الصحارى للتأمين لديها مقاربة خاصة لوثيقة التأمين السيبراني مناسبة للسوق الليبي يتم تصميمها بناء على احتياجات وظروف عمل كل زبون.

**التهديدات التي تغطيها شركة صحارى للتأمين :**

كما هو الحال مع أي وثيقة تأمين فإنه يوجد هناك أشكال مختلفة للتأمين السيبراني تغطي مختلف التهديدات السيبرانية و قد سعت هاته الشركة الى تغطية عدة تهديدات ومنها:

- تأمين ضد الاختراقات السيبرانية
- تأمين انقطاع الخدمة نتيجة الهجمات الالكترونية
- تأمين الفدية والابتزاز الإلكتروني
- تأمين خرق الخصوصية
- تأمين فساد أو تدمير الأصول الرقمية الناجمة عن المخاطر السيبرانية
- تأمين خسائر الإيرادات الناجمة عن المخاطر السيبرانية
- تأمين التبعيات القانونية الناجمة عن حوادث الأمن السيبراني.

**الفرع الثاني :تجربة المملكة العربية السعودية**

يعرف التأمين السيبراني انتعاشا كبيرا في دول الخليج مقارنة بدول المغرب العربي ، حيث تتجه هذه الدول الى مواكبة الدول المتقدمة من خلال اللحاق بالركب في مجال الاعلام والاتصال وبذلك بالاهتمام بمجال الأمن والتأمين السيبراني.

**شركة سايكو للتأمين SAICO :[1]**

بدأ نشاط الشركة منذ العام 1952 قبل صدور الأمر الملكي رقم32 بتاريخ2003/06/02. ولائحته التنفيذية والخاص بالرقابة على شركات التأمين التعاوني. كان للشركة نشاط بالتأمين التعاوني داخل المملكة من خلال مستثمرين سعوديين بالبحرين. وبعد صدور اللوائح الجديدة لسوق التأمين السعودي، تم إنشاء سايكو كشركة سعودية مساهمة بناءاً على قرار وزير التجارة والصناعة رقم 193

[1]SAICO Legacy – SAICO

بتاريخ2007/07/21 وتحت إشراف البنك المركزي السعودي. بلغ رأس مال شركة سايكو عند التأسيس 100 مليون ريال سعودي مقسمة إلى 10 ملايين سهم بقيمة اسمية قدرها 10 ريالات للسهم الواحد. وفي عام 2015 تمت زيادة رأس مال الشركة عن طريق طرح أسهم حقوق أولوية لمساهمي الشركة بمبلغ 150 مليون ريال ليصبح 250 مليون ريال مقسمة إلى 25 مليون سهم بقيمة اسمية قدرها 10 ريالات للسهم الواحد. وفي عام 2018 تمت زيادة رأس مال الشركة عن طريق منح أسهم مجانية لمساهمي الشركة بمبلغ 50 مليون ريال ليصبح 300 مليون ريال مقسمة إلى 30 مليون سهم بقيمة اسمية قدرها 10 ريالات للسهم الواحد.

صممت شركت سايكو للشركات والمؤسسات تغطية تأمينية ضد الأضرار التي قد تلحق بالأجهزة والخسائر المالية نتيجة الهجمات الإلكترونية، كما تسعى لتقييم التهديدات والأخطار السيبرانية والاستجابة لها والتعافي منها.

**المخاطر التي يتم تغطيتها هي الناتجة عن:**

- خرق الخصوصية.
- فساد أو تدمير الأصول الرقمية الناجمة عن المخاطر السيبرانية.
- مسؤولية الأمان والخصوصية.
- خسائر الإيرادات التجارية والإيرادات التجارية التابعة الناجمة عن المخاطر السيبرانية
- الابتزاز الإلكتروني.

**المنافع التي يتم تغطيتها هي:**

- تكاليف خرق الخصوصية.
- تكاليف استبدال الأصول الرقمية الناجمة عن المخاطر السيبرانية.
- تكاليف مسؤولية الأمان والخصوصية .
- مصاريف الدفاع.
- خسائر الإيرادات التجارية والإيرادات التجارية التابعة ومصاريفها الإضافية الناجمة عن المخاطر السيبرانية.
- مصاريف الابتزاز الإلكتروني أو دفعات ابتزاز إلكتروني تم دفعها .

## المطلب الثالث : تجربة الجزائر في مجال التأمين السيبراني

كشفت دراسة استطلاعية أجرتها "كاسبرسكى" حول "حالة الأمن الإلكترونى في القطاع الصناعي 2018" عن أبرز الدول العربية التي تعرضت لهجمات إلكترونية على شبكاتها وأنظمتها الصناعية، وهى كل من الجزائر بنسبة 66.2% والمغرب بنسبة 60.4% ومصر بنسبة 57.6% والمملكة العربية السعودية بنسبة 48.4% في طليعة البلدان التي تواجه مثل تلك الهجمات[1].

ورغم أن الجزائر تختل المرتبة الأولى من حيث التعرض للهجمات السيبرانية الا انه لايزال موضوع توفير تأمين للمنتجات المتصلة بالمخاطر الالكترونية "السيبرانية" أمر غير منتشر بسوق التأمين الجزائري بشكل كبير و يقتصر التأمين على الماديات و الأشياء الملموسة فقط .

**الشركة الجزائرية للتأمين و إعادة التأمين CAAR :**

CAAR هي أقدم شركة تأمين في الجزائر. في الواقع ، تم إنشاؤها في أعقاب الاستقلال في عام 1963.

بعدد قليل من الموظفين في أيامها الأولى ليصل عدد الموظفين اليوم إلى المئات ، سجلت CAAR العديد من النجاحات ، وأصبحت واحدة من الشركات الرائدة في مجال التأمين في البلاد[2].

**يغطي هذا التأمين:**

الوحدات المركزية، الذاكرات ، والبرامج والتعليمات والبيانات، الحواسيب، أجهزة الكمبيوتر المكتبية أو المحمولة.

كما يغطي : أضرار غير متوقعة في الممتلكات، نتيجة:

- التعامل غير السليم أو الإهمال أو الخبث من قبل موظف أو طرف ثالث خارج الشركة.
- من السرقة والهجوم وعواقبه. عيوب البناء وسوء التصنيع والعيوب المادية.
- الحرائق والصواعق والانفجارات من أي نوع (بما في ذلك أضرار الإطفاء والإنقاذ).
- عمل قوى الطبيعة مثل العواصف والفيضانات والبرد والانهيارات الأرضية (باستثناء الزلازل).
- عمل الماء والرطوبة
- التكاليف الإضافية الناتجة عن إنشاء معالجة البيانات عند توقف تشغيل النظام المؤمن عليه.

ينطبق هذا التأمين على المعدات المؤمن عليها أثناء تشغيلها أو أثناء الراحة ؛ أثناء عمليات التفكيك ، السفر إلى المباني المؤمن عليها ؛ أو إعادة التجميع أثناء عمليات الصيانة أو الإصلاح.[1]

[1] الهجمات الإلكترونية (السيبرانية) والتأمين(ifegypt.org)

[2] https://https//dz.linkedin.com/company/caarassurance.

ومما لا شك فيه انه يجب على كل المؤسسات والقطاعات تأمين تعاملاتها الإلكترونية فى المستقبل ضد الاختراقات، خصوصًا أن هناك توسعا واضحا فى الاعتماد على التكنولوجيا فى ظل الثورة الصناعية الرابعة.

**السوق السيبراني في الجزائر (مشروع قيد الإنجاز)** : سوق تأمين أخطار الإعلام الآلي التقليدية (الأجهزة واسترجاع المعلومات) في الجزائر موجود منذ مدة. ومع هذا كانت الشركة الوطنية للتأمين وإعادة التأمين السباقة لإدخال هذا النوع ويضمن حماية أجهزة المؤسسات وأجهزة الأشخاص الطبيعيين، وحتى استرجاع معلوماتهم ومفاتيح البرامج إلخ ... هذا بخصوص الأخطار التقليدية التي تضر بالأجهزة (الحريق، السرقة، أضرار المياه، الصواعق ... إلخ) كلها أخطار ملموسة ويمكن رؤيتها.

أما بخصوص موضوعنا، التأمين من المخاطر السيبرانية هو قطاع مستقبلي في سوق التأمين الجزائري، يكون كحل وتهيئة للأرضية رقمنه القطاعات في الجزائر.

ليس هناك في الجزائر شركة تأمن ضد الخطر السيبراني لكن هو مشروع جديد لأن هناك فراغ كبير في هذا القطاع يجب سده، فهناك الكثير من العوائق التي تعيق هذا القطاع حتى في أوروبا والدول المتقدمة.

[1]Tous Risques Informatiques – CAAR

## خلاصة الفصل:

تجسد تجارب الدول المتقدمة في مجال التأمين السيبراني فهمها ومعالجتها للتحديات الرقمية من خلال استثمارات كبيرة في البنية التحتية السيبرانية والتقنيات الأمنية المتقدمة. هذه الدول قدمت منتجات تأمين سيبراني للشركات لحمايتها من خسائر البيانات والاختراقات. تتضمن هذه التجارب مزيجًا من القوانين الصارمة، الاستثمار في التكنولوجيا، التعاون بين القطاعين العام والخاص، وتعزيز الوعي والتدريب.

في المقابل، لا يزال التطور في مجال التأمين السيبراني في العالم العربي في مراحله البدائية. ومع ذلك، بدأت بعض الدول العربية بوضع تشريعات وتعزيز بنيتها التحتية التقنية وتبني تقنيات الأمن السيبراني. كما شهدت مبادرات للتعاون الدولي والإقليمي وتقديم منتجات تأمين سيبراني.

الجزائر اتخذت خطوات لتعزيز الأمن السيبراني من خلال تشريعات مثل قانون حماية البيانات الشخصية. لكنها تحتاج إلى استثمارات أكبر في بنيتها التحتية السيبرانية وتطوير منتجات التأمين السيبراني. التعاون مع القطاع الخاص والمنظمات الدولية يمكن أن يكون مفتاحًا لمواجهة التهديدات السيبرانية بفعالية وتعزيز الحماية الشاملة. على الرغم من التحديات، تسعى الجزائر لتعزيز جهودها في مجال التأمين السيبراني وتطوير استراتيجياتها بالتعاون مع الشركاء الدوليين.

# الخـــاتـمـة

من خلال ما تطرقنا اليه و من خلال دراستنا للموضوع سجلنا مايلي :

الخطر السيبراني خطر نامي يتمثل في الهجمات الإلكترونية التي تصيب المعلومات ويتميز على الأخطار الأخرى القابلة للتأمين بخصائص خاصة منها: أنه خطر غير مادي، غير ملموس، وغير مرئي ويتم اكتشافه بعد مدة من حدوثه هذا ما يبين صعوبة تأمين هذا الخطر وأن شركات التأمين قبلت بهذا الخطر تدريجيا ولم تقترب منه إلا بحذر. محل الأشياء المؤمنة التي تقع عليها هاته الأخطار هي المعلومات وتم تبيان تصنيفاتها وتقسيماتها وأنها ذات قيمة اقتصادية كما أنها تقيم بقيمة استرجاعها .

عقد التأمين السيبراني هو عقد تأمين أشياء تطبق عليه أحكام تأمينات الأضرار، فهو عقد تأمين أضرار (أشياء ومسؤولية)، وهو منتوج مستقبلي في الجزائر والوطن العربي كما أن من بين الضمانات التي يمنحها هذا العقد، أولا ضمانات عينية تتمثل في إرسال شركات التأمين لخبراء حماية الإعلام الآلي للمؤمن له المتضرر يوم وقوع الكارثة السيبرانية للتحكم فيها. وثانيا ضمانات نقدية يدفها المؤمن مثل مصاريف إعادة إقلاع النشاط، استرجاع المعلومات وإدارة الدعاوى الناشئة عن رجوع الغير بدعوى جماعية ضد المؤمن له لعدم حماية معلوماتهم.

**1 - نتائج الدراسة :**

تم التوصل في هذه الدراسة للنتائج التالية:

المعلومات أشياء معنوية ذات القيمة الاقتصادية صعبة التأمين عليها نظرا لخصائصها غير الملموسة، وصعبة التصريح بها نظرا لسريتها في الكثير من الأحيان واستثناءا يمكن وفقا لشروط التأمين عليها.

يقع الخلط في الكثير من الأحيان بين مختلف عقود التأمين السيبرانية بين أمرين اثنين، فهناك عقود كلاسيكية منها تأمين أخطار الإعلام الآلي المتعلق بالأخطار التي تصيب الأجهزة والمعلومات بطريقة غير مباشرة وهناك عقود جديدة منها عقد التأمين السيبراني التي تصيب مباشرة المعلومات، فيجب على الطرف الضعيف في التأمين فهم مضمون العقود جيدا قبل اكتتابها .

منتوج تأمين الخطر السيبراني لا يزال منتوج جديد في الدول الغربية، أما في الدول العربية فهو قليل جدا أما بالجزائر فهو منعدم و غير موجود تماما و ذلك راجع لعدة اسباب من أهمها ارتفاع تكلفة التأمين و غياب الثقافة التأمينية على هذا المنتج .

**2 – اختبار الفرضيات :**

بعد دراستنا للموضوع يمكننا اختبار الفرضيات فيما يأتي :

**الفرضية الأولى:** و التي نصت على : " يمكن التأمين من مخاطر برامج الفدية بطرقة مشابهة للتأمين على الحياة من خلال تحديد مبلغ التعويض عند إبرام عقد التأمين "تعتبر هذه الفرضية خاطئة لأن عقد التأمين السيبراني المتعلق ببرامج الفدية ينص على أن التعويض الذي يأخذه المأمن له مساو لحجم الفدية المطلوبة .

**الفرضية الثانية:** و التي نصت على : " يعتبر التأمين السيبراني منتج مبتكر لكنه يتم بنفس طرق التأمين الأخرى " تعتبر هذه الفرضية أيضا خاطئة لأن المخاطر السيبرانية لها خصائص مختلفة عن الخطر التقليدي القابل للتأمين ولكن بسبب الخسائر المادية الكبيرة التي تنتج عنها تم تكييف عقد التأمين ليتلاءم معها وهذا ما يمكن ان نستدل عليه من خلال ما تطرقنا اليه في آخر مطلب في الفصل الأول.

**3– الاقتراحات :**

بعد دراسة موضوعنا أردنا أن نقدم بعض الاقتراحات:

- تسريع تطوير الثقافة المتعلقة بالخطر السيبراني .
- القراءة الجيدة لمحتوى عقود التأمين السيبراني قبل إبرامها (الضمانات والاستثناءات) .
- الحث على الأخذ بآليات جديدة تتواكب مع هذه الجرائم الحديثة وليس فقط سن قوانين وعدم تطبيقها.
- تجميع البيانات الناتجة عن الحوادث السيبرانية (جمع قاعدة بيانات إحصائية للكوارث السيبرانية) .

**4 – آفاق الدراسة :**

تناولنا في موضوع بحثنا : "التأمين من المخاطر السيبرانية – تجارب دولية – " و قد حاولنا من خلاله تبيان أهمية الأمن و التأمين السيبراني بالنسبة للمؤسسات و الشركات و حتى الأفراد فهو موضوع حساس و لا بد من النظر اليه بجدية و إعطاءه حجمه لأنه لابد على الدول مواكبة التطور الرقمي الحاصل في مجال الإعلام و الإتصال و عليه فإن هذا المجال لا يخلو من الأخطار بل هي في تزايد مستمر و في تطور مستمر فالمخترقون و المجرمون يبحثون دوما عن أساليب و طرق جديدة و مبتكرة للتسلل و مهاجمة الأنظمة المعلوماتية بغية تحقيق المال .

# قائمة المصادر والمراجع

## قائمة المصادر والمراجع

### كتب:

1) عبد الرزاق بن خروف، التأمينات الخاصة في التشريع الجزائري، دار الخلدونية، القبة القديمة، الجزائر، التأمينات البرية الجزء الأول، 2017.
2) محمود علي عبد الرحمن، أسامة فاروق مخيمر: الفضاء الإلكتروني وأثره على مفاهيم القوة والأمن والصراع في العلاقات الدولية،مجلة كلية السياسة و الإقتصاد، جامعة محمد البشير الإبراهيمي ،برج بوعريريج، المجلد السادس عشر، العدد الخامس عشر، الجزائر ،2022.
3) عادل عبد الصادق: "الفضاء الالكتروني والرأي العام ، تغير المجتمع والأدوات والتأثير"، المركز العربي لأبحاث الفضاء الالكتروني: قضايا إستراتيجية العدد ،2459 ، 2013 .
4) علي زياد علي، الصراع والأمن الجيوسيبراني في الساحة الدولية: دراسة في استراتيجيات الاشتباك الرقمي، (عمان: دار أمجد للنشر والتوزيع، 2020).

### مذكرات:

5) أيريك ليوبولد–سيرج لوست : ترجمة فتحي علي زمال، "أمن المعلومات"، المملكة العربية السعودية، مدينة الملك عبد العزيز للعلوم والتقنية، 2014.
6) المهندس محمد بن سعود الخطيب، إستشاري الانظمة، 10 محرم 1435 هجري.
7) التقرير الصادر عن الإتحاد الدولي للإتصالات، حول "اتجاهات الإصلاح في الإتصالات للعام 2010–2011.
8) نادي الحقوقيون في فرنسا أنشأ لجنة حقوقيين في 2018 مختصة في تأمين الخطر السيبراني وكل ما يحيطه به، دراسة عبارة عن كتاب ،تأمين الخطر السيبراني تقرير جانفي 2018 يحتوي على 100 صفحة .

**مواد وقوانين :**

9) المادة الثانية(2)من القانون رقم 09-04 المؤرخ في 09.05.2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها، عرفت هذه الجريمة، كما عددت المادة (87 ) من قانون العقوبات، الجزاء المنتظر لكل من ثبت في حقه الإختراق وبالتالي المساس بحقوق الدولة أو المواطن.

10) مرسوم رئاسي رقم 05-20 ممضي في 20 جانفي 2020 وزارة الدفاع الوطني، يتعلق بوضع منظومة وطنية ألمن الأنظمة المعلوماتية، الجريدة الرسمية عدد4 مؤرخة في 26 جانفي 2020.

**مجلات :**

11) هربرت لين، "النزاع السيبراني في القانون الدولي الإنساني"، المجلة الدولية للصليب الأحمر، م ،94 ع ،886 (صيف 2012.(

12)نورة شلوش، "القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول"، مجلة مركز بابل للدراسات الإنسانية، م،8 ع، (2018.(

13)مصطفى إبراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي"، مجلة العلوم القانونية والسياسية، م. ،10 ع. ،01 (جوان 2021).

14)أكرم القصاص : من هم هاكرز الأنونيموس ولماذا تردد إسمهم في الإحتجاجات الأمريكية ،مجلة اليوم السابع، تاريخ النشر 08/06/2020 تاريخ الإطلاع 25/12/2022 .

**مواقع الكترونية عربية:**

15)موقع تك عربي للتأمين السبراني.

16) موقع الاتحاد المصري للتأمين ضد الجرائم الإلكترونية Blom Alexander. Mr,

17)ويكيبيديا – برمجيات خبيثة ، 2022 .

18)أكبر 10اختراقات للبيانات تم الكشف عنها ، (https://aitnews.com/2018/12/13).

19)التأمين السيبراني | شركة الصحارى للتأمين(sic.ly)

20)الهجمات الإلكترونية (السيبرانية) والتأمين(ifegypt.org) .

21)إبراهيم صفا : مقال عن التأمين السيبراني ، موقع تك عربي، 19 مارس 2024.

22) المجموعة الدولية الأمريكية – ويكيبيديا (wikipedia.org).

23)موقع شركة التعاونية للتأمين ،17/5/2017.

**مراجع باللغة الأجنبية**

**كتب و مقالات:**

1) Samia Tibah, Présentation Cyber risques, 2018,

2) Laure Zicry, Cyber-Risques Le nouvel enjeu du secteur bancaire et financier, Ronen Bergman, "Weaving A Cyber WebNov2019.

3) CNN 18, DDOS Arabic.

4) Dans son livre « Cybernetics or control and communication in the Animal and the machine 2016 -20121 UK,

5) Hiscox, Novembre 2016 Séminaire de la CCR – Alger.

6) Imene.A , 2018,L'industrie énergétique en Algérie espionnée ,

7) Jean Bigot, Traité de droit des Assurances, Assurance Dommages, Chapitre 3 L'Assurance des risques informatiques, Op cit, p 390.

8) Laure Zicry, Cyber-Risques Le nouvel enjeu du secteur bancaire et financier, Les Essentiels de la banque et de la finance, RB Editions, 2017.

9) LIBERATION, avec AFP, Ransomware Renault parmi les cibles d'une cyberattaque mondiale , publié le 12 mai 2017 ,

10) Samia Tibah, Présentation Cyber risques, 2018,

11) VERSPIEREN, CONTRAT D'ASSURANCE COLLECTIVE CYBER RISQUES, Conditions générales, 2022,

12) Comission Cyber Risk : Rapport : Assurer le risque Cyber.

13) ÉRIC A. CAPRIOLI, Banque et Assurance Digitales, Droit et Pratiques, RB Éditions, 2017,

14) Insurancemarket.Ae, 2022, "Cyber Security Insurance",

15) [1]Jean Bigot, Traité de droit des assurances, Assurance Dommages, Chapitre 3

16) RansomwareBarometerjanvier2021 .

**مواقع الكترونية أجنبية :**

1) https://web.archive.org/web/20070927080536/http:/www.axa-im.com/index.cfm?pagepath=abooutaxaim%2Fwhoweare%2Fbusinesshighlights

2) https://www.algerie360.com/letude-de-kaspersky-revele662-ordinateurs-touches-cyberatta

3) https://insurancemarket.ae/cyber-security-insurance/. Accessed 15 Dec 2022.

4) https://saisco.com.sa

5) https://caar.dz Tous Risques Informatiques - CAAR

6) https://www.ccr.dz/images/pdf/seminaire1.pdf. Accessed 15 Dec 2022. Voir aussi : Ccr, "La Protection Des Entreprises Contre Les Risques Émergents - Compagnie Centrale De Réassurance (CCR)". Ccr.Dz, 13 Janvier 2018,

7) https://www.ynetnews.com/articles/0,7340,L-5444998,00.html. Accessed 15 Dec 2022.

8) https://www.ccr.dz/fr/component/k2/item/39-assurances-un-seminaire-fait-le-point-sur-la-protection-des-entreprises-contreles-risques-emergents. Accessed 15 Dec 2022.

9) https://www.argaam.com/ar/article/articledetail/id/1500023

10) http://www.liberation.fr/planete/2017/05/12/renault-parmi-les-cibles-d-une-cyberattaque-mondiale_1569124 . Accessed 15 Dec 2022.

11) https://www.ccr.dz/images/pdf/cyber-risks-ccr.pdf. Accessed 15 Dec 2022.

12) https://reassurezmoi.fr/guide/wp-content/uploads/2021/01/assurance cyber risckesmmacq .pdf .accessed 15 dec 2021.

13) https://arabic.cnn.com/scitech/2016/12/08/sc-081216-what-ddos-attack. Accessed 15 Dec 2022.

14) https://caar.dz/tous-risques

15) https://https//dz.linkedin.com/company/caarassurance.

16) https://wiselyinsure.com/ar/

17) https://www.ifegypt.org/

18) https://caar.dz/wpcontent/uploads/2017/03/petits_systemes_informatiques.pdf. Accessed 15 Dec 2022.

19) https://www.ccr.dz/images/pdf/cyber-risks-ccr.pdf. Accessed 15 Dec 2022.

**الملخص :**

الأمن السيبراني يعد أساسيا في عالم التكنولوجيا الحديثة، حيث يهدف إلى حماية الأنظمة والبيانات الرقمية من التهديدات الإلكترونية. يتكون الأمن السيبراني من مجموعة من الإجراءات والتقنيات التي تهدف للحفاظ على سلامة البيانات وخصوصيتها، مما يسهم في منع الوصول غير المصرح به والاختراقات السيبرانية. يشمل الأمن السيبراني استخدام التشفير لحماية البيانات، وتنفيذ سياسات الوصول وإدارة الصلاحيات للتحكم في الوصول إلى الأنظمة، بالإضافة إلى تطبيق أنظمة كشف التسلل والحماية من الفيروسات والبرمجيات الضارة.

أما التأمين السيبراني فيعمل على توفير حماية مالية ضد الخسائر الناجمة عن الهجمات السيبرانية، مثل فقدان البيانات، أو انتهاك البيانات الشخصية، أو تعطل الخدمات الرقمية. يقدم التأمين السيبراني سبل للمؤسسات لتعويض الخسائر المالية واستعادة البيانات بسرعة بعد وقوع الحادث.

يواجه الأمن والتأمين السيبراني تحديات مستمرة نتيجة لتطور التهديدات والهجمات السيبرانية المتطورة باستمرار. يتطلب ذلك استمرارية التحديث والتطوير في استراتيجيات الأمن واستثمارات مستمرة في تحسين البنية التحتية السيبرانية وتعزيز الوعي السيبراني لدى الموظفين. بالرغم من هذه التحديات، يظل الأمن والتأمين السيبراني أموراً حيوية لضمان استمرارية عمل الشركات وحماية بياناتها في عصر الرقمنة المتقدمة.

"Cybersecurity" refers to the practice of protecting digital systems, networks, and data fromcyberattacks and unauthorizedaccess. It is crucial in today's digital age to ensure the confidentiality, integrity, and availability of information. Cybersecurityencompasses a range of measures, includingencryption, access control, intrusion detectionsystems, and antivirus software, aimed at safeguardingagainstvariousthreatssuch as malware, phishing, and ransomwareattacks.

"Cyber Insurance" providesfinancial protection againstlossesresultingfromcyberattacks and data breaches. It coversexpensesrelated to data recovery, legalfees, notification costs, and potentialliability claims. Cyber insurancepolicies are tailored to the specificneeds of organizations, offeringcoverage for various aspects of cybersecurity incidents.

Bothcybersecurity and cyber insurance face ongoing challenges due to the evolving nature of cyber threats and attacks. Continuous efforts are required to keep pace withemergingthreats and vulnerabilities, enhancesecuritymeasures, and raiseawarenessamongemployees. Despitethese challenges, investing in cybersecurity and cyber insuranceremainscritical for businesses to mitigaterisks and protecttheir digital assets in an increasinglyinterconnected world.

**الكلمات المفتاحية** : الأمن السيبراني ، التأمين السيبراني ، الجرائم الإلكترونية ،البرمجيات الضارة ، الفضاء السيبراني .