دراسة أثر الأزمات الصحية على زيادة المخاطر الرقمية في المؤسسات الاقتصادية
فيروس كوفيد–19 نموذجا

Study of the impact of healthdisasters on increasing digital risks ineconomic institutions - Covid-19 virus model

محمد قارة برنو *[1]، حكيم شبوطي [2]

[1]جامعة المدية، karabernou.mohamed@univ-medea.dz

[2]جامعة المدية، chabouti.hakim@univ-medea.dz

تاريخ الاستلام: 2021/05/16 تاريخ القبول: 2021/06/05 تاريخ النشر: 2021/06/30

ملخص:

تهدف الدراسة إلى معرفة أثر الأزمات الصحية العالمية على زيادة تحقق التهديدات والمخاطر الرقمية في المؤسسات الاقتصادية، معتمدين في ذلك على المسح المكتبي، ثم على الإحصائيات المستمدة من مواقع الشركات العالمية التي تقدم حلول الأمن الإلكتروني وكذا منظمة الصحة العالمية.

وقد خلصت الدراسة إلى أن الأزمات الصحية تؤثر سلبا على إنتاجية العمال بما فيهم موظفي أمن المعلومات مما يؤدي إلى زيادة المخاطر الرقمية.واختتمت الدراسة ببعض التوصيات، من أهمها استدعاء الموظفين الأكثر كفاءة خلال فترات الحجر الصحي، والتركيز على تدريب الموظفين على تقنيات الأمن الإلكتروني، واستخدام برامج عمل عن بعد أكثر أمانا وموثوقية للحد من المخاطر الرقمية ومجابهتها قبل حدوثها.

الكلمات المفتاحية: إدارة المخاطر؛مخاطر رقمية؛ هجمات إلكترونية؛أزمات صحية؛ كوفيد–19.

Abstract:

This study aims to know the impact of health crises on the realization of digital threats and risks in economic institutions, relying on the desk survey,then on the statistics of international companies that provide security solutions and the World Health Organization.

The study concluded that health crises negatively affect the productivity of workers, including information security personnel, which leads to an increase in digital risks, and its concluded with some recommendations like calling the most efficient employees during quarantine periods, focusing on training employees in electronic security techniques, and using secure programs to reduce digital risks and confront them.

Keywords:risks management; digital risks; electronic attacks; health disasters; covid-19.

* **محمد قارة برنو**

I. مقدمة:

تنشط المؤسسات الاقتصادية في محيط مفتوح، ما يجعلها عرضة للعديد من المخاطر، ومع توجه هذه المؤسسات إلى الاقتصاد المعرفي، والاعتماد على رقمنة نشاطاتها، أصبحت تتعرض لأنواع أخرى من المخاطر متمثلة في المخاطر الرقمية، التي من شأنها التأثير على نشاطات المؤسسة وأهدافها، لذلك تقوم هذه الأخيرة بانتهاج طرق واستراتيجيات لإدارة المخاطر الرقمية قصد التخفيف من حدتها أو القضاء عليها.

ورغم قيام هذه المؤسسات بإدارة مخاطرها الرقمية، إلا أنها قد تصبح غير مجدية بشكل كبير إذا تزامنت مع تفشي أزمات صحية عالمية غير متوقعة، حيث يصبح التحكم فيها أكثر صعوبة من ذي قبل، ولا تستطيع أغلب المؤسسات مجابهتها، بسبب ما تخلفه الأزمات الصحية من أضرار على الموظفين، وعلى البنية التحتية، وعلى الاقتصاد ككل.

وحتى تتمكن هذه المؤسسات من التصدي لهذه الأزمات الصحية، أصبح لزاما عليها التفكير بجدية والتخطيط المسقبلي للحيلولة دون تفاقم المخاطر الرقمية في حال حدوثها.

بناء على ما سبق، يمكننا طرح الإشكالية التالية:

كيف تؤثر الأزمات الصحية العالمية على المخاطر الرقمية في المؤسسات الاقتصادية؟

فرضيات الدراسة:

للإجابة على إشكالية البحث، تم الاعتماد على الفرضيات التالية:

الفرضية الأولى: تؤدي الأزمات الصحية إلى ارتفاع ميزانية الأمن المعلوماتي.

الفرضية الثانية: تؤثر الأزمات الصحية سلبا على إنتاجية موظفي أمن المعلومات.

الفرضية الثالثة: يؤدي الحجر الصحي الناجم عن الأزمات الصحية إلى زيادة القابلية للاختراق والهجمات الإلكترونية.

أهداف الدراسة:

تهدف هذه الدراسة إلى ما يلي:

- التعرف على مدىتأثير الأزمات الصحية على المخاطر الرقمية.
- طرق التقليل من أثر المخاطر الرقمية في حال حدوث أزمات صحية غير متوقعة.
- زيادة الوعي لدى المؤسسات العامة والخاصة بضرورة التخطيط للحد من تأثير الأزمات الصحية على المخاطر الرقمية.

منهج الدراسة:

تم استخدام المنهج الوصفي التحليلي الذي يعبر عن الظاهرة المراد دراستها تعبيرا كميا وكيفيا، والذي لا يتوقف عند حد جمع البيانات اللازمة لوصف الظاهرة، وإنما يصل إلى تحليلها وتفسيرها بغية الوصول إلى الاستنتاجات التي من شأنها أن تساهم في معرفة أثر الأزمات الصحية والأوبئة على المخاطر الرقمية التي تتعرض لها المؤسسة.

II. الإطار النظري لإدارة المخاطر الرقمية.

II-1 مفهومالمخاطر (Risks): سنتطرق فيما يلي إلى مجموعة من التعاريف والتصنيفات قصد التعرف على مفهوم المخاطر في المؤسسات الاقتصادية.

II-1- 1 تعريف المخاطر:توجد عدة تعريفات تناولت مفهوم المخاطر، نذكر منها الآتي:

– تعرف المخاطر على أنها مجموعة أحداث متزامنة أو متتابعة إمكانية حدوثها غير مؤكدة، وحدوثها يصيب أهداف المؤسسة التي تخضع لهذه الوضعية(Barthélémy، 2000، صفحة 13).

– كما تعرف على أنها الحالة التي يكون فيها إمكانية أن يحدث انحراف معاكس عن النتيجة المرغوبة أو المتوقعة أو المأمولة(حماد، 2003، صفحة 16).

– كما يمكن تعريفها على أنها الأضرار المحتملة من بعض العمليات الجارية في المؤسسة، والتي قد تحدث نتيجة تمكن مصادر التهديدات من استغلال إحدى نقاط الضعف الموجودة(العريشي و الشلهوب، 2016، صفحة 52).

من خلال استعراض جملة من التعاريف، نستطيع تعريف المخاطر على أنها " مجموعة من الأحداث المحتملة والتي تؤدي في حال وقوعها إلى حدوث نتائج غير مرغوبة على أداء المؤسسة وأهدافها".

II–1– 2 تصنيفالمخاطر:يمكن تصنيف المخاطر حسب عدة معايير، نذكر بعضا منها فيما يلي(طاهري، 2014، الصفحات 21-26):

– حسب إمكانية تحقيق الربح: وتنقسم إلى مخاطر مضاربية، وهي التي تتحملها المؤسسة بإرادتها على أمل تحقيق ربح مثل التقلبات النقدية وإفلاس الموردين؛ ومخاطر بحتة، وهي التي تكون نتيجة حادث طارئ خارج عن إرادة المؤسسة، مثل الأزمات الطبيعية أو التقنية أو البشرية.

– حسب مصدرها: وتنقسم إلى مخاطر داخلية، وهي تلك الناجمة عن المؤسسة نفسها، مثل حوادث العمل أو الأخطار المعلوماتية؛ ومخاطر خارجية، وهي تلك الناجمة عن محيط المؤسسة، مثل الأزمات الطبيعية، المنافسة أو تقليد المنتجات.

– حسب نتائجها: وتنقسم إلى مخاطر توثر على الأفراد، مثل حوادث العمل؛ مخاطر تصيب أصول المؤسسة، مثل الحرائق والانفجارات؛ ومخاطر تخص الأمن المالي للمؤسسة، مثل الإفلاس.

– حسب طبيعتها: وتنقسم إلى مخاطر اقتصادية، وهي التغيرات الفجائية التي قد تحدث في أي مؤشر اقتصادي يمس محيط المؤسسة بحيث تؤثر على نشاطها؛ مخاطر بشرية، وهي التي يتسبب فيها فعل بشري متعمد أو غير متعمد؛ ومخاطر طبيعية، وهي الناتجة عن قوى طبيعية.

II–2 مفهوم إدارة المخاطر:

يقصد بإدارة المخاطر "التحكم بوقوع الخطر عن طريق تحديد أسباب حدوثه، وحساب احتمال تحققه، وحجم الخسارة المتوقعة وقياسها كميا حال حدوثه، ثم اختيار وتطبيق أفضل الوسائل لمواجهة تلك الأخطار والحد من آثارها، ومن ثم مراقبة فعالية وملائمة هذه الوسائل"(عكور، 2010، صفحة 25).

كما يمكن تعريفها على أنها "عملية قياس وتقييم للمخاطر، وتطوير استراتيجيات لإدارتها، كنقلها إلى جهة أخرى، أو تجنبها، أو تقليل آثارها السلبية، أو قبول بعض أو كل تبعاتها"(العريشي و الشلهوب، 2016، صفحة 55).

وهنا نجد أن عملية إدارة المخاطر تتبع الخطوات التالية:

– تحديد أسباب جميع أنواع المخاطر التي تخفض قيمة المؤسسة في حال حدوثها.

– حساب احتمال وقوع هذه المخاطر والخسائر المتوقعة عند حدوثها كميا.

– تطوير واختيار الوسائل الفعالة والملائمة لمواجهة هذه المخاطر.

– تطبيق الطرق التي تم اختيارها لإدارة المخاطر.

– تقييم ومراجعة فاعلية وملائمة هذه الوسائل كأسلوب لإدارة المخاطر.

II-3 مفهوم المخاطر الرقمية وأنواعها:

مع توجه العديد من الدول في العالم نحو تطبيقات الحكومة الإلكترونية والمدن الذكية، وكذا انتقال المؤسسات الاقتصادية إلى الاقتصاد الرقمي، الذي أنتج لنا بدوره تطبيقات وتكنولوجيات جديدة مثل التجارة الإلكترونية، الحوسبة السحابية، البيانات الضخمة، العملات الرقمية، إنترنت الأشياء والتوائم الرقمية وغيرها من التقنيات الحديثة، ظهرت نتيجة لذلك عدة مخاطر مرتبطة بهذه التطبيقات والنشاطات صارت تهدد بقاء المؤسسات وقدرتها على نموها وتحقيق أهدافها، اصطلح عليها باسم "المخاطر الرقمية".

فقد عرفت المخاطر الرقمية بأنها " عواقب اعتماد تقنيات جديدة، هذه العواقب جديدة وغير متوقعة"(Oliveira، 2021).

يمكننا تصنيف المخاطر الرقمية على أنها(Oliveira، 2021):

– مخاطر الأمن السيبراني:هنا نشير إلى مخاطر الهجمات الإلكترونية، غالبًا ما يكون هدف هذه الأنواع من الهجمات هو الوصول إلى معلومات حساسة ثم استخدام تلك المعلومات لأعمال ضارة. على سبيل المثال، الابتزاز ومنع تدفق العمليات التجارية العادية.

– مخاطر القوى العاملة: مخاطر القوى العاملة هي أي مشكلة تتعلق بالقوى العاملة يمكن أن تشكل خطرًا على أهداف المؤسسة. بمعنى آخر، مخاطر القوى العاملة هي أشياء مثل نقص المهارات وارتفاع معدل دوران الموظفين.

–مخاطر الامتثال: يشير هذا الخطر إلى أي متطلبات أو قواعد جديدة مطلوبة لتقنية جديدة. عندما تتبنى تقنية جديدة، تكون مؤسستك معرضة لخطر عدم الامتثال للمتطلبات التنظيمية للعمليات التجارية والاحتفاظ بالبيانات وممارسات الأعمال الأخرى.

– مخاطر الطرف الثالث:هذه هي المخاطر المرتبطة بالاستعانة بمصادر خارجية لبائعي الطرف الثالث أو موفري الخدمات. على سبيل المثال، تعتبر نقاط الضعف المتعلقة بالملكية الفكرية أو البيانات أو العمليات أو الشؤون المالية أو معلومات العملاء أو غيرها من المعلومات الحساسة من مخاطر الجهات الخارجية.

– مخاطر الأتمتة: إلى جانب الأتمتة، سيكون هناك خطر حدوث مشكلات مثل مشكلات التوافق مع التقنيات الأخرى، ونقص الموارد، وقضايا الحوكمة، من بين أمور أخرى.

– مخاطر المرونة: يشير هذا النوع من المخاطر إلى مخاطر الأحداث السلبية التي تحدث عند تبني تقنية جديدة وصعوبة تقليل الضرر الناجم.

-مخاطر خصوصية البيانات: يشير هذا إلى مخاطر القدرة على حماية البيانات الحساسة. تتضمن هذه البيانات عادةً الأسماء الكاملة وعناوين البريد الإلكتروني وكلمات المرور والعناوين الفعلية وحتى تواريخ الميلاد، يمكن للمخترقين إساءة استخدام هذه البيانات بسهولة كطريقة لإيذاء هويتك أو إساءة استخدامها.

II-4 الأمن المعلوماتي:

إدارة المخاطر والأمن المعلوماتي وجهان لعملة واحدة، فوظيفة الأمن المعلوماتي في الأخير ما هي إلا محاولة لتفادي حدوث التهديدات التي بدورها تتحول إلى مخاطر في حال حدوثها.

II-4- 1 مفهوم الأمن المعلوماتي وعناصره:

يقصد بأمن المعلومات (ويطلق عليه أيضا الأمن السيبراني) من زاوية أكاديمية، "العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها، ومن أنشطة الاعتداء عليها"(ليتيم، 2015، صفحة 239).

كما يمكن تعريفه انطلاقا من أهدافه، بأنه "النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار التي تترتب في حال تحقق التهديدات والمخاطر، كما يتيح إعادة الوضع إلى ما كان عليه، بأسرع وقت ممكن بحيث لا تتوقف عجلة الإنتاج ولا تتحول الأضرار إلى خسائر دائمة"(سمير، 2017، صفحة 257).

تتلخص عناصر الأمن المعلوماتي في النقاط التالية(ليتيم، 2015، الصفحات 239-240):

- **السرية والموثوقية (Confidentiality)**: وتعنيالتأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.
- **التكاملية وسلامة المحتوى (Integrity)**: أي أنه لا بد من التأكد من أن المحتوى لم يتم العبث به، أي أنه لم يتم تدمير أي جزء من أجزاءه في أي مرحلة من مراحله، عن طريق القرصنة أو الدخول غير المشروع إليه، من أي من العابثين الذين يقومون بالدخول إلى محتوى المعلومات لتدميره سواء كان تدمير كلي أو جزئي.
- **استمرارية توفر المعلومات أو الخدمة (Availability)**: ويقصد بها عملية التأكد من استمرار عمل النظام المعلوماتي، واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع معلوماتية، وأن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها.
- **عدم إنكار التصرف المرتبط بالمعلومات (Non-denial of information relatedbehavior)**: أي ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها أنه هو الذي قام بهذا التصرف، بحيث تتوفر قدرة إثبات أن تصرفا ما قد تم من طرف شخص ما في وقت معين (خطر انتحال الشخصية).

II–4– 2 وسائل المحافظة على أمن المعلومات:هي مجموعة من الآليات والإجراءات والأدوات والمنتجات التي تستخدم بواسطة المؤسسات للوقاية من المخاطر والتهديدات التي تتعرض لها الأجهزة الحاسوبية والشبكات ونظم المعلومات وقواعدها، أو التقليل منها، ويمكن تلخيصها فيما يلي(العريشي و الشلهوب، 2016، الصفحات 111-121):

– الجدران النارية (Firewalls): الجدار الناري هو جهاز أو برنامج يقوم بمراقبة العمليات التي تمر عبر شبكة المعلومات، بحيث يرفض أو يقرر أحقية المرور طبقا لقواعد معينة، وبذلك يكون هو المسؤول عن حجب محاولات الاختراق التي من الممكن أن تتعرض لها الأجهزة الحاسوبية للمؤسسة عند الاتصال بشبكة الإنترنت.

– مضادات الفيروسات (Antivirus): يقصد بها البرمجيات التي تستخدم لمنع واكتشاف وإزالة البرمجيات الخبيثة، بما فيها من فيروسات الحاسب، الديدان، أحصنة طراودة، برامج التجسس وغيرها من الأشكال والبرامج المصممة خصيصا للإضرار بالأجهزة الحاسوبية.

– التوقيع الإلكتروني (E-signatures): هو طريقة لتوقيع الوثائق الإلكترونية، ولمساعدة مستقبِل الرسالة من التحقق من مصدر الرسالة ومن هوية المرسل، بالإضافة إلى التحقق من أن محتوى الرسالة لم يجري عليه أي تغيير أثناء إرسالها بعد توقيع المرسِل عليها، حيث أنها تمنع المرسِل من إنكار توقيعه أو جحود إرسال الرسالة.

– **الشهادات الرقمية (Digital Certificates)**: تصدر الشهادات الرقمية عن جهة ثالثة ذات مصداقية معروفة للجميع، للتحقق من تطابق المفتاح العام مع هوية الشخص الذي صدرت لأجله الشهادة الرقمية، وهي تحتوي على معلومات على هوية الشخص حامل الشهادة مثل الاسم، هوية مصدر الشهادة، تاريخ إصدار وانتهاء صلاحية الشهادة، والمفتاح العام لحامل الشهادة، بحيث تقوم بربط المفتاح العام بهوية المرسِل.

– نطاق الاستخدام (scope of use): من خلال هذه الطريقة يتم تحديد مستخدمي النظام، والموارد المسموح لهم بها، ومنحهم صلاحيات الوصول إليها عن طريق نظام الترخيص، فهي وسيلة للمحافظة على أمن المعلومات بحيث يتم التحكم في الدخول أو التحكم في الوصول إلى المعلومات أو أجزاء النظام.

– سجلات الأداء (Log files): تحتوي كل الأجهزة الحاسوبية على سجلات تكشف استخدامات الجهاز وبرمجياته والنفاذ إليه، وهي ما يعرف بسجلات الأداء أو سجلات النفاذ إلى النظام، ولها أهمية كبيرة عند تعدد المستخدمين في الشبكات الحاسوبية، وهي تتباين من حيث نوعها وطبيعتها وغرضها، فهناك سجلات الأداء التاريخية والسجلات المؤقتة، وسجلات النظام، وسجلات الأمن، وسجلات قواعد البيانات والتطبيقات، وسجلات الصيانة والأمور التقنية، وغيرها.

– أنظمة التحقق من الهوية (Identityverification): هي من الوسائل المادية التي تختص بالحماية من الدخول غير المصرح به، أو من الاقتحام بغرض سرقة أجهزة حاسوبية أو ملفات أو وثائق أو سجلات ذات أهمية، أو التحايل على الموظفين بهدف الوصول إلى المعلومات.

– عمليات الحفظ (Back-up operations): تتعلق عمليات الحفظ بعمل نسخ احتياطية من المواد المخزنة على وسائط التخزين، ويكون الحفظ إما داخل النظام في ملفاته، أو خارجه على أقراص خارجية، وينبغي أن تخضع عمليات الحفظ لقواعد محددة سلفا وموثقة، وذلك لضمان توحيد معايير الحفظ وحماية النسخ الاحتياطية.

– أنظمة المراقبة المرئية (Visual surveillance systems): وهي تتمثل في كاميرات المراقبة وملحقاتها من أجهزة تسجيل وتحكم، بحيث توضع في مكان مناسب وكاشف للموقع المراد مراقبته، ويتم توصيلها بكابل مخصص لنقل الصورة إلى جهاز للتسجيل الرقمي يتصل بأحد الأجهزة الحاسوبية في مكان معين، ويقوم بمتابعته مجموعة محدودة من المراقبين.

II–4– 3 تأثير المخاطر الرقمية على أداء المؤسسات الاقتصادية :

لقد أصبح الفضاء الإلكتروني جاذبا لقطاعات المجتمع كافة، وباتت المعرفة محرك الإنتاج والنمو الاقتصادي، كما أيقن الجميع أن مبدأ التركيز على المعلومات والتكنولوجيا يعد عاملا من العوامل الأساسية للنهوض بالاقتصاد، كما أن استخدام أجهزة الحاسب وشبكات المعلومات والاتصالات في تطوير الصناعات وتحريك الاقتصاد ومعالجة كل المعاملات الاقتصادية والمالية، كل ذلك أدى إلى ضرورة توفير الأمن المعلوماتي لضمان حماية هذه المعلومات.

فعلى سبيل المثال، يشير تقرير صادر عن مجلس التجارة والتنمية التابع للأمم المتحدة ''اونكتاد'' إن حجم التجارة الإلكترونية حول العالم بلغ في عام 2018 ما يصل إلى 25.6 تريليون دولار، وذلك بزيادة نسبتها 8% عن عام 2017 وأشار نفس التقرير إلى أن أزمة فيروس كورونا ساهمت في تسريع انطلاق الحلول الرقمية، والأدوات والخدمات، لكن التأثير العام على حجم التجارة الإلكترونية في 2020 مازال من الصعب تحديده، وفقا لما قاله شاميكاسيريماني، المدير المختص بالتكنولوجيا واللوجستيات في أونكتاد(البورصة نيوز، 2020).

ونظرا لارتفاع معدل الجرائم الإلكترونية المنظمة والخطيرة، فإن ذلك يمثل تهديدا صريحا لنمو الاقتصاد الرقمي، ما لم تقم الدول باعتماد معايير الأمن الإلكتروني (مثل ISO 27001)بما يضمن الحد من هذه الجرائم.(سمير، 2017)

III. أثر الأزمات الصحية في زيادة المخاطر الرقمية:

نقصد بالأزمة الصحية حالة صعبة أو نظام صحيمعقد يؤثر على البشر في منطقة أو عدة مناطق جغرافية وقعت أساسا في الأخطار الطبيعية، من مكان معين لتشمل الكوكب بأسره. للأزمات الصحية عموما آثار كبيرة على صحة المجتمع، والخسائر في الأرواح والاقتصاد. قد تنجم عن الأمراض أو العمليات الصناعية أو سوء السياسات(ويكيبيديا، 2021).

III–1 نظرة تاريخية:

لقد مر العالم الحديث بعدة أزمات صحية، ذهب ضحيتها الملايين من البشر وفيما يلي أبرزها(BBC، 2021):

– **الطاعون الأسود**:شهدت أوروبا عامي 1348 و 1349 ما عرف باسم الطاعون الأسود الذي أسفر عن مقتل نحو 20 مليون شخص. وذكرت دراسة صدرت عام 2018 أن البشر كانوا المسؤولين عن العدوى في ذلك الوقت وليس الفئران.

– **الكوليرا**:في عام 1820 فتكت الكوليرا بالكثيرين في جنوب شرق آسيا وبلغ عدد الضحايا أكثر من 100 ألف شخص. وقد ظهرت في مدينة كالكوتا في الهند ومنها انتشرت في جنوب آسيا والشرق الأوسط وساحل البحر الأبيض المتوسط وقد وصل هذا الوباء إلى الصين.

– **الأنفلونزا الإسبانية**:في عام 1918اجتاح وباء الإنفلونزا الإسبانية العالم، وقد أودى بحياة ما يتراوح بين 40 و 50 مليون شخص، ووفقا لدراسة نشرتها بي بي سي عام 2018 كان عدد الضحايا كبيرا لأنه في عام 1918، كانت الفيروسات لا تزال حديثة الاكتشاف. وتقول ويندي باركلاي من جامعة إمبريال كوليدج بلندن: "لم يدرك الأطباء حينها بالطبع أن الفيروسات هي التي تسبب هذه الأمراض". وكان الطريق أمامهم لا يزال طويلا لاكتشاف الأدوية المضادة للفيروسات واللقاحات التي تساعد الآن في كبح تفشي المرض وتسريع التعافي منه.

– **الإيدز**:في عام 1976 ظهر في الكونغو وانتشر في مختلف أنحاء العالم، وقد بلغ عدد المصابين حوالي 36 مليونا. وفي عام 2014 توصل علماء إلى أن منشأ وباء الإيدز يعود إلى العشرينيات من القرن الماضي في مدينة كينشاسا الموجودة حاليا في جمهورية الكونغو الديمقراطية. وقالوا إن "مزيجا من الأحداث" شمل النمو السكاني وتجارة الجنس وحركة السكك الحديدية سمح بانتشار الفيروس المسبب للإيدز.

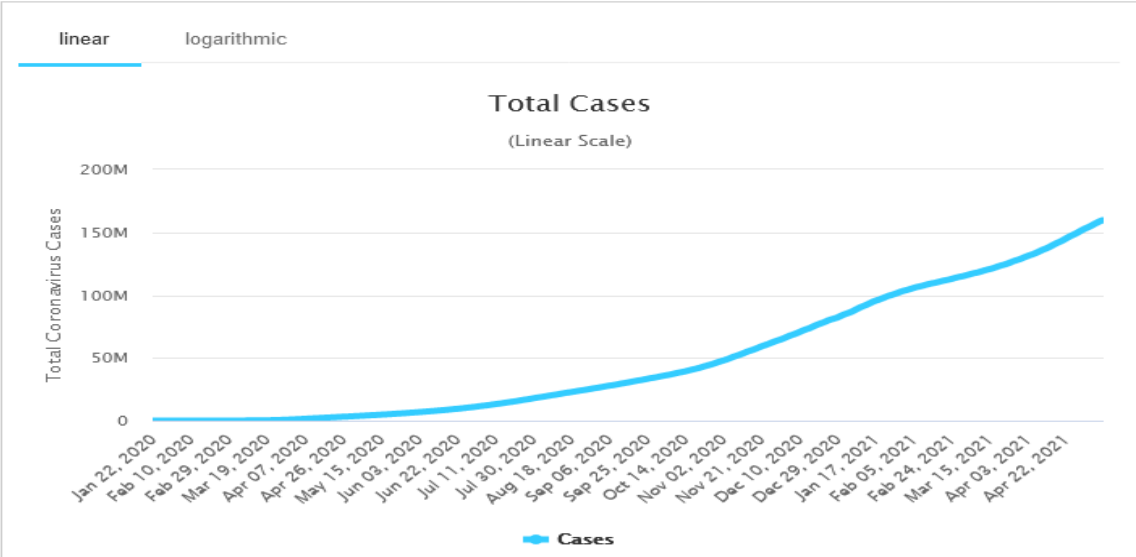
– **انفلونزا الخنازير**:انتشر وباء إنفلونزا الخنازير في عام 2009، وقد اكتشف أولا في المكسيك في شهر أفريل من ذلك العام، قبل أن ينتشر في العديد من دول العالم. ووفقا لمنظمة الصحة العالمية، فإن إنفلونزا الخنازير من أكثر الفيروسات خطورة حيث يتمتع بقدرة تغير سريعة، هربا من تكوين مضادات له في الأجسام التي يستهدفها، وقد أعلنت منظمة الصحة العالمية في عام 2010 عن وفاة 18 ألف شخص جراء الوباء.

– **أيبولا**:في ديسمبر 2013، ظهر هذا الوباء في غينيا وانتشر إلى ليبيريا وسيراليون المجاورتين، ليعرف بعدها باسم "فيروس إيبولا في غرب أفريقيا"، الأمر الذي كاد يتسبب بانهيار اقتصادات البلدان الثلاثة، وتوفي حوالي 6 آلاف شخص بسببه. وفي عام 2018، ضرب إيبولا مجددا جمهورية الكونغو الديمقراطية حيث فقد أكثر من 2200 شخص حياتهم.

– **كوفيد–19**:يعتبر كوفيد–19 هو المرض الناجم عن فيروس كورونا المستجد المسمى فيروس كورونا–سارس– 2. وقد اكتشفت المنظمة هذا الفيروس المستجد لأول مرة في 31 ديسمبر 2019، بعد الإبلاغ عن مجموعة من حالات الالتهاب الرئوي الفيروسي في يوهان بجمهورية الصين الشعبية.

وقد تجاوزت عدد حالات الإصابة بهذا الفيروس عتبة 160 مليون شخص عبر العالم حسب آخر الإحصائيات، وفي الشكل التالي مخطط بياني يوضح تطور عدد حالات الإصابة بالفيروس في العالم خلال الفترة من 01 جانفي 2020 إلى 22 أفريل 2021.

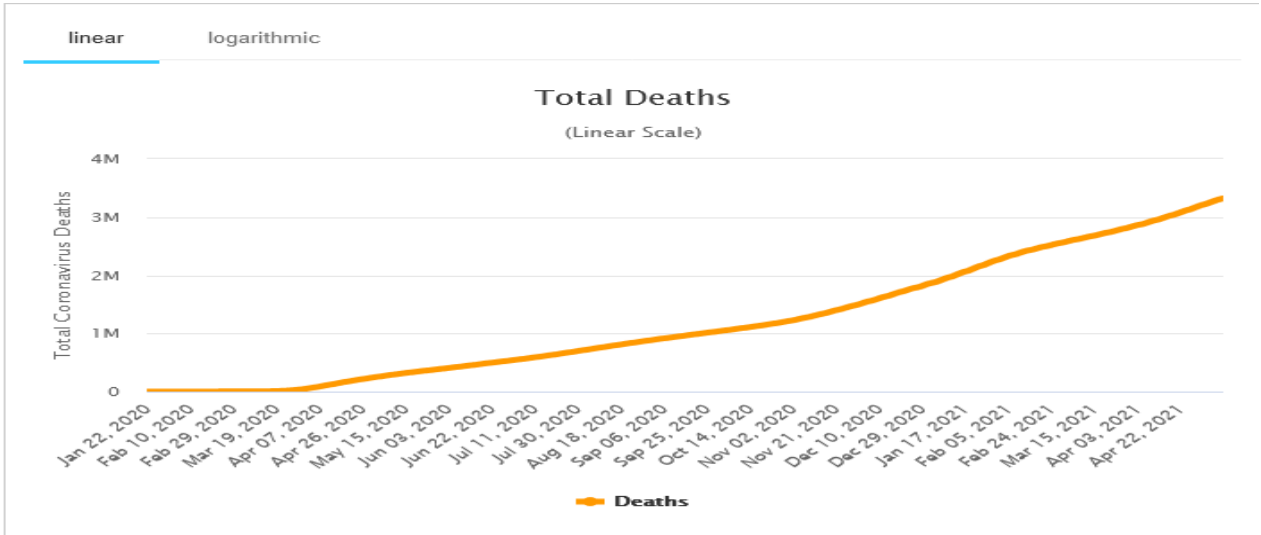
الشكل 01 :تطور حالات الإصابة بفيروس كوفيد-19 في العالم.



المصدر: https://www.worldometers.info/coronavirus/worldwide-graphs

كما أن عدد الوفيات قد تفاوتت من دولة إلى أخرى، وقد تجاوزت في مجموعها الثلاثة ملايين حالة وفاة، وهو ما يبينه الشكل التالي عن تطور عدد الوفيات في العالم خلال نفس الفترة:

الشكل 02 : تطور حالات الوفيات جراء فيروس كوفيد-19 في العالم.



المصدر: https://www.worldometers.info/coronavirus/worldwide-graphs

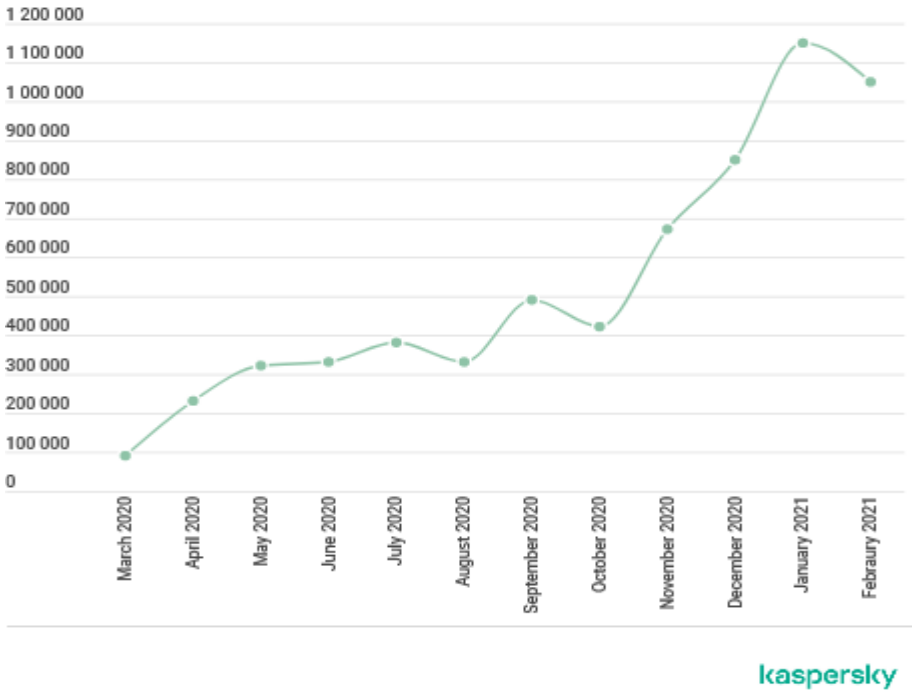
2-III إحصائيات ومعطيات ميدانية : تم انجاز هذا البحث الميداني في الفترة ما بين 2020/01/01 إلى غاية 2021/04/30.

وقد قمنا برصد بعض الإحصائيات من موقع الشركة الرائدة في أمن المعلومات كاسبرسكي(Kaspersky)، وذلك للاطلاع على مدى تطور الهجمات الإلكترونية خلال فترة الدراسة، وذلك بسبب زيادة الإصابات بفيروس كوفيد-19.

– **الفيروسات** :تم تخصيص جزء كبير من الوقت الذي يقضيه المستخدمون على الإنترنت للاجتماع والتعاون افتراضيًا. لهذا السبب أصبحت تطبيقات الاجتماعات والمراسلة ، مثل Zoom و Teams ، إغراءً شائعًا لتوزيع التهديدات الإلكترونية.

عند فحص تطبيقات الاجتماعات ومؤتمرات الفيديو الشائعة ، بما في ذلك Zoom و Webex و MS Teams ، لاحظ باحثو Kaspersky عددًا متزايدًا من الملفات الضارة المنتشرة تحت ستار أسماء هذه التطبيقات، وهذا ما يبينه الشكل التالي :

الشكل 03 : تطور عدد الفيروسات التي قامت شركة كاسبرسكي بحضرها.

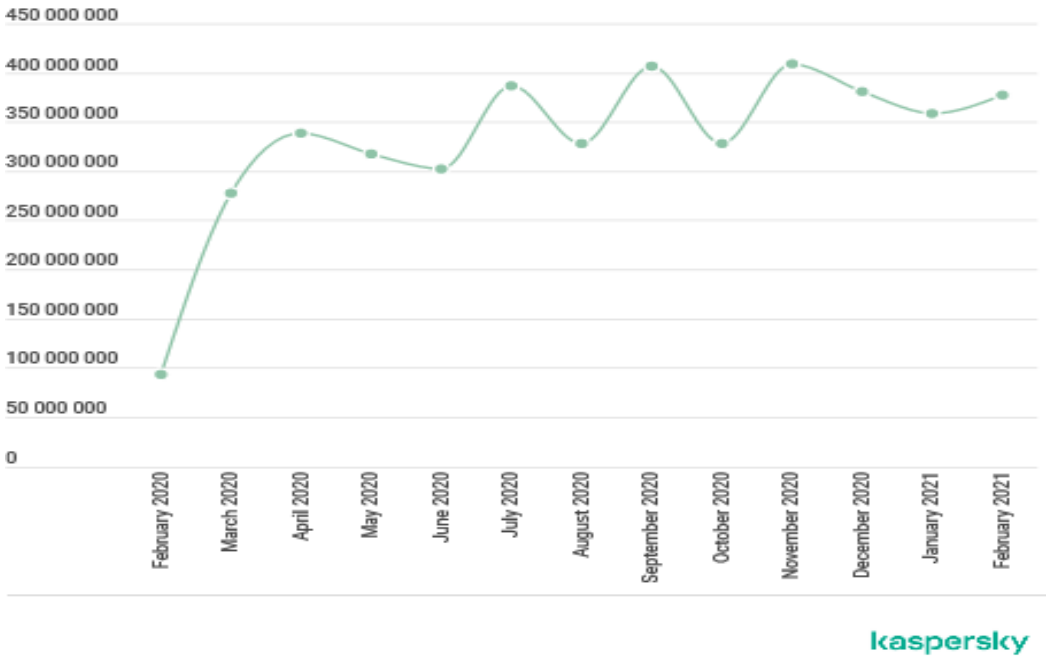


المصدر :https://securelist.com/covid-19-examining-the-threat-landscape-a-year-later/101154

– **العمل عن بعد وظهور هجمات القوة الغاشمة (Brute Force)**:مع إجبار العديد من الشركات على إغلاق أبوابها دون سابق إنذار، لم يكن لدى القليل منهم الوقت لاتخاذ الإجراءات الأمنية المناسبة. وكانت النتيجة أن العديد أصبحوا عرضة لمجموعة من الهجمات الجديدة حيث بدأ موظفوهم في تسجيل الدخول إلى موارد الشركة من الأجهزة الشخصية وعلى الشبكات غير الآمنة.

وهذا مما ساهم في تزايد هجمات القوة الغاشمة (Brute Force) بشكل كبير خلال نفس الفترة، وهذا ما يبينه الشكل التالي :

الشكل 04 :تطور عدد هجمات القوة الغاشمة.



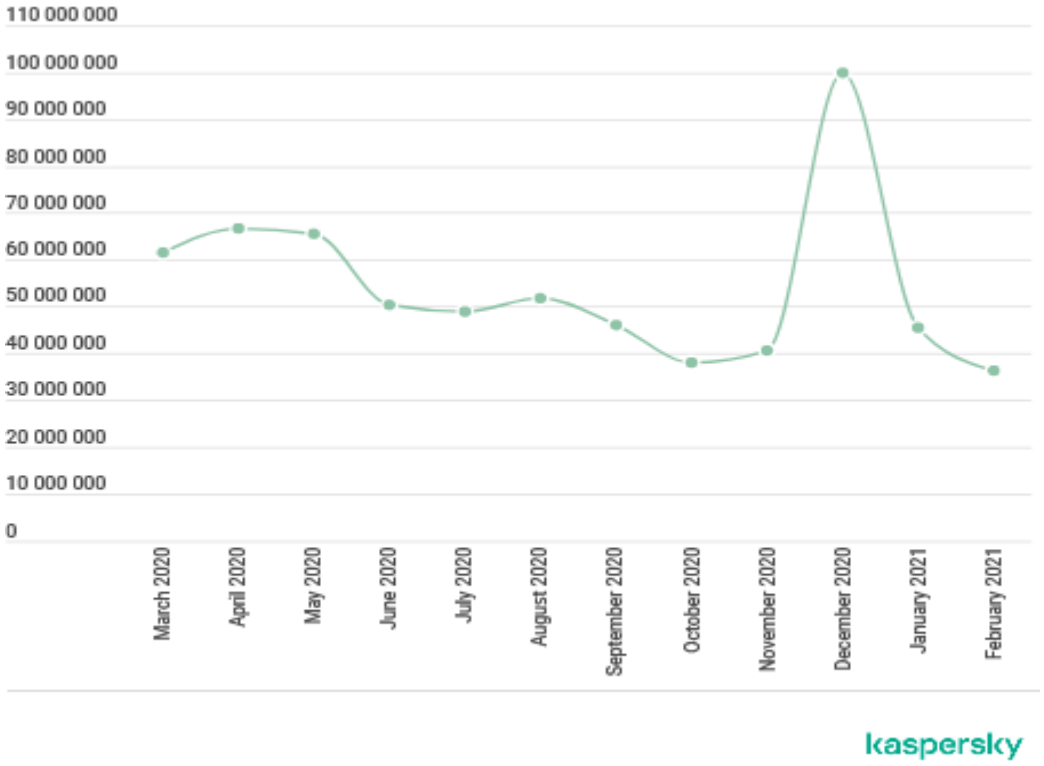
المصدر :https://securelist.com/covid-19-examining-the-threat-landscape-a-year-later/101154/

– منصات الاتصالات الافتراضية تتعرض للهجوم :مع إغلاق العالم جراء تزايد الإصابات بفيروس كورونا المستجد، وصل الطلب على الإنترنت إلى مستويات غير مسبوقة، حيث اضطرت الشركات الكبيرة من Facebook إلى Netflix إلى YouTube إلى تقليل جودة الفيديو من أجل مواكبة الطلب. وكل هؤلاء المستخدمين الإضافيين يعني مجموعة من الأهداف الجديدة للمجرمين.

بحلول شهر ماي من عام 2020، ارتفع متوسط العدد اليومي للهجمات المحظورة بواسطة Kaspersky Web Anti-Virus بنسبة 25٪، ووصل عدد هجمات الويب ، بعد أن ظهر انخفاضًا في صيف 2020 ، إلى ذروة جديدة في ديسمبر حيث كان معظم العالم يواجه موجة ثانية من الوباء.

هذه الهجمات رصدتها إحصائيات شركة كاسبرسكي في الشكل الموالي:

الشكل 05 :عدد الهجمات على الويب التي تم حظرها بواسطة برنامج مكافحة الفيروسات من كاسبرسكي.



المصدر :https://securelist.com/covid-19-examining-the-threat-landscape-a-year-later/101154/

III–3أهمية الأمن الإلكتروني في ظل الأزمات الصحية:

في ظل الأزمات الصحية تزداد أهمية تدابير الأمن الإلكترونيلمواجهة المخاطر الرقمية أكثر من أي وقت مضى، وفيما يلي بعض هذه التأثيرات وأسبابها: (www.weforum.org, 2020)

–زيادة الاعتماد على البنية التحتية الرقمية يزيد من تكلفة الفشل: عند تفشي الفيروسات والأوبئة بشكل كبير، يتزايد الاعتماد على الاتصالات الرقمية، وتقدم الشركات ومنظمات القطاع العام بشكل متزايد سياسات "العمل من المنزل" أو تفرضها، وتقتصر التفاعلات الاجتماعية بسرعة على مكالمات الفيديو ومشاركات وسائل التواصل الاجتماعي وبرامج الدردشة، وتقوم العديد من الحكومات بنشر المعلومات عبر الوسائل الرقمية؛ في هذا السياق، يمكن أن يكون الهجوم الإلكتروني الذي يحرم المنظمات أو العائلات من الوصول إلى أجهزتهم أو بياناتهم أو الإنترنت مدمرًا أو حتى مميتًافي أسوأ السيناريوهات، حيث يمكن أن تتسبب الهجمات الإلكترونية واسعة النطاق في فشل البنية التحتية على نطاق واسع والتي تأخذ مجتمعات بأكملها أو مدنا خارج الإنترنت، مما يعيق مقدمي الرعاية الصحية والأنظمة والشبكات العامة.

– تستغل الجريمة الإلكترونية الخوف وعدم اليقين:يستغل مجرمو الإنترنت الضعف البشري لاختراق الدفاعات النظاميةفي حالة الأزمات، خاصة إذا طال أمدها، حيث يميل الناس إلى ارتكاب أخطاء ما كانوا ليرتكبوها لولا ذلك، إذ يعتبر مجرمو الإنترنت مبدعين للغاية في ابتكار طرق جديدة لاستغلال المستخدمين والتكنولوجيا للوصول إلى كلمات المرور والشبكات والبيانات، وغالبًا ما يستفيدون من الموضوعات والاتجاهات الشائعة لإغراء المستخدمين إلى السلوك غير الآمن عبر الإنترنت، كأن يدفعوا المستخدمين إلى اتخاذ إجراءات يمكن اعتبارها غير منطقية في ظروف أخرى.

– يمكن أن يؤدي المزيد من الوقت عبر الإنترنت إلى سلوك أكثر خطورة:يزيد سلوك الإنترنت المحفوف بالمخاطر عن غير قصد مع زيادة الوقت الذي يقضيه المستخدمون على الإنترنت خاصة عند فرض الحجر المنزلي، على سبيل المثاليمكن أن يلجأ المستخدمون إلى الوصول "المجاني" إلى مواقع الويب أو البرامج المقرصنة غير الواضحة، مما يفتح الباب أمام البرامج الضارة والهجمات المحتملة. وبالمثل، قد تكون هناك مخاطر خفية في طلبات الحصول على معلومات بطاقة الائتمان أو تثبيت تطبيقات عرض متخصصة وخاصة أثناء انتشار الوباء، يمكن أن يكون النقر على الرابط الخاطئ أو توسيع عادات تصفح الإنترنت أمرًا خطيرًا ومكلفًا للغاية.

– انتشار المواقع المضللة: والتي تدعي توفير لقاحات أو أدوية أو معدات لمواجهة الأزمات الصحية، وهي في الحقيقة تقوم بنشر برمجيات خبيثة أو تقوم بهجومات إلكترونية مثل هجوم الفدية أو سرقة البيانات الشخصية.

III–4إجراءات الحد من أثر الأزمات الصحية في زيادة المخاطر الرقمية:

وللحد من أثر الأزمات الصحية في زيادة المخاطر الرقمية،تنتهج الدول والمؤسسات إجراءات احترازية للحد من أثر الأزمات الصحية في زيادة المخاطر الرقمية، نذكر منها:(www.weforum.org، 2020)

–تعزيز معايير النظافة الإلكترونية: بالإضافة إلى غسل اليدين بعد كل اتصال جسدي لمنع انتشار الفيروسات، واستخدام محلول تنظيف مناسب قائم على الكحولعلى الهاتف ولوحة المفاتيح وأجهزة التحكم في الألعاب وأجهزة التحكم عن بعد، لا بد من تخصيصبعض الوقت لمراجعة عادات النظافة الرقمية، مثل التحقق من أن كلماتالمرور المستخدمة للوصول إلى مختلف المواقع والخدمات على شبكة الإنترنت طويلة ومعقدة، وأن جدران حماية النظام نشطة، واستخدم شبكة VPN موثوقةللوصول إلى الإنترنت حيثما أمكن ذلك.

– اليقظة والحذر: لا بد من الحذر أكثر من المعتاد عند تثبيت البرنامج وإعطاء أي معلومات شخصية على شبكة الإنترنت، عدم النقر على الروابط من البريد الإلكتروني، عند الاشتراك في خدمات جديدة يجب التحقق من مصدر كل عنوان URL والتأكد من أن البرامج أو التطبيقات التي يتم تثبيتها هي الإصدارات الأصلية من مصدر موثوق به، لأن الفيروسات الرقمية منتشرة مثل الفيروسات المادية أو أكثر، ويمكن لأي خطأ محتمل عبر الإنترنت أن يطال الآخرين في المؤسسة أو دفتر العناوين أو المجتمع ككل.

– اتباع التحديثات الرسمية:تمامًا كما يجبالاهتمامبمصادر البيانات الموثوقة حول انتشار وتأثير الفيروسات، لا بد منالتأكد من تحديث برامج النظام والتطبيقات بانتظام لتصحيح أي نقاط ضعف قد يتم استغلالها من طرف أطراف تسعى للقيام بهجمات إلكترونية.

IV. الطريقة والأدوات :

لقد قمنا باستخدام المنهج التحليلي، وذلك بالاعتماد على الاحصائيات المجمعة من مواقع بعض الشركات العالمية الرائدة في مجال حلول الأمن الإلكتروني، وإحصائيات منظمة الصحة العالمية في مجال تطور وانتشار فيروس كوفيد-19 المستجد، ومن ثم محاولة دراسة الارتباط بين الظاهرتين، وإسقاطها على المؤسسات الاقتصادية في الجزائر.

V. النتائج ومناقشتها :

لقد خلصت هذه الدراسة إلى النتائج التالية:

– يؤدي تدهور صحة المواطنين ونفسياتهم جراء الأزمات الصحية إلى عدم تمكن الموظفين في قسم أمن المعلومات بالمؤسسات الاقتصادية من أداء مهامهم بكفاءة عالية، مما يؤدي إلى زيادة إمكانية حدوث المخاطر الرقمية بها.

– تفشي الوباء بصورة كبيرة يؤدي إلى فرض الحجر الصحي للسكان، وهذا ما يؤدي بالمؤسسات إلى تقليص عدد العمال أو تسريحهم، بما فيهم موظفي أمن المعلومات، وهذا ما يزيد من احتمالية تعرض المؤسسات إلى الهجمات الإلكترونية.
– تقوم الدولة بخفض ميزانية الأمن المعلوماتي لصالح قطاعات أكثر أهمية خلال الأزمات الصحية مثل الصحة والغذاء.
– الحجر الصحي يؤدي إلى زيادة الضغط على مواقع الإنترنت، مما يزيد من قابلية اختراقها.
– خلال الأزمات الصحية العالمية، يقوم مجرمو الإنترنت باستغلال فترات الحجر الصحي لتكثيف جهودهم خاصة مع لجوء الكثير من المؤسسات إلى الاعتماد على نموذج العمل عن بعد.
– إغلاق الأسواق العالمية والحد من حركة التجارة العالمية يؤدي إلى صعوبة التموين بمعدات وبرامج الأمن الإلكتروني.

VI. الخلاصة :

إن الانتقال نحو الاقتصاد الرقمي الذي انتهجته أغلب المؤسسات الاقتصادية في جميع دول العالم نتجت عنه مخاطر وصفت بالمخاطر الرقمية، والتي أثرت سلبا على أداء هذه المؤسسات وربحيتها وقدرتها على نموها وتحقيق أهدافها، ومما يزيد من خطورة الوضع هو تزامن ذلك مع ظهور أزمات صحية عالمية مثل التي يشهدها العالم ابتداء من الأشهر الأخيرة من سنة 2019 إلى يومنا هذا، وهو ما عرف بجائحة Covid-19، لذلك حاولنا من خلال هذا البحث إلى تقصي أثر الأزمات الصحية في زيادة المخاطر الرقمية استنادا إلى الإحصائيات المتوفرة على شبكة الإنترنت.

كما خرجت الدراسة ببعض التوصيات للمؤسسات الاقتصادية وصناع القرار سواء في القطاع الحكومي أو الخاص، والمتمثلة فيما يلي:

- استدعاء الموظفين الأكثر كفاءة قدر الإمكان لضمان الحد الأدنى من سيرورة العمل بصفة عامة، وعمال الأمن الإلكتروني بصفة خاصة.
- تدريب الموظفين على الأمن الإلكتروني، وتكوينهم في الخارج للاستفادة من تجارب الدول المتقدمة في هذا المجال، وذلك لمجابهة المخاطر الرقمية المتوقعة مستقبلا.
- استخدام برامج وأنظمة عمل عن بعد أكثر أمانا وموثوقية للحد من هذه المخاطر.
- تخصيص مؤونة الأخطار الرقمية لمواجهة المخاطر التي تنجم عن الأزمات الصحية غير المتوقعة.
- الاعتماد على البرامج مفتوحة المصدر والمجانية لمجابهة نقص ميزانية اقتناء برامج الأمن المعلوماتي مثل برامج مكافحة الفيروسات والجدار الناري.
- نشر الوعي لدى المواطنين بضرورة الاعتماد على مصادر الأخبار الموثوقة مثل القنوات التلفزيونية الحكومية، والمواقع الموثوقة مثل موقع منظمة الصحة العالمية، من أجل تجنب المواقع المضللة ومجرمي الإنترنت.

VII. المراجع :

- BBC. (2021). Récupéré sur https://www.bbc.com/arabic/science-and-tech-51675634
- Bernard Barthélémy .(2000) .Gestion des risques .Paris: Edition d'Organisations.
- Oliveira, D. d. (2021, 01 21). Digital Risk: What It Is And How to Manage It in Your Org. Récupéré sur https://www.plutora.com/blog/digital-risk
- www.weforum.org. (2020). Récupéré sur www.weforum.org
- البورصة نيوز. (2020). Récupéré sur https://alborsaanews.com/
- جبريل بن الحسن العريشي، و محمد حسن الشلهوب. (2016). أمن المعلومات. الأردن: الدار المنهجية للنشر والتوزيع.
- سمير ,ب .(2017) .الأمن السيبراني في الجزائر :السياسات والمؤسسات .المجلة الجزائرية للأمن الإنساني.
- طارق عبد العال حماد. (2003). إدارة المخاطر. مصر: الدار الجامعية.
- فاطمة الزهراء محمد طاهري. (2014). إدارة المخاطر الزراعية. الأردن: دار أسامة للنشر والتوزيع.
- ليتيم ,ن .ل .(2015) .الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة .مجلة الفكر.
- هاني جزاع أرتيمية و سامر محمد عكور. (2010). إدارة الخطر والتأمين من منظور إداري كمي وإسلامي . عمان، الأردن: دار الحامد للنشر والتوزيع.
- ويكيبيديا/https://ar.wikipedia.org/wiki .(2021) .أزمة_صحية