

مخطط استئناف/استمرارية النشاط ضرورة حتمية لحماية الأنظمة المعلوماتية في حالة الأزمة

Business Recovery/continuity Plan is an imperative to protect information systems in the event of a crisis

فيلالي أسماء
جامعة أوبكر بلقايد بتلمسان (الجزائر)
filaliasma@outlook.fr

تاريخ الاستلام: 2020-04-26 تاريخ القبول للنشر: 2020-11-22

ملخص:

تهدف هذه الدراسة إلى توضيح كيفية مواجهة المؤسسة للأزمات التي تتعرض لها أنظمتها المعلوماتية، وذلك بالاعتماد على مخطط استئناف/استمرارية النشاط، والخطوات الصحيحة الواجب اتباعها للنجاح في ذلك.

وتوصلت الدراسة إلى أن مخطط استئناف/استمرارية النشاط ضرورة حتمية على كل مؤسسة اعتمادها من أجل مواجهة الأزمات التي تتعرض لها الأنظمة المعلوماتية، والخروج بأقل الخسائر، وذلك من خلال دراسة احتمالات الأزمات الممكن حدوثها ودرجة الخطورة المصاحبة لكل أزمة والخروج بسيناريوهات متعددة والتي تقود إلى تحضير حلول مناسبة لكل سيناريو ممكن، من أجل المباشرة في تطبيق المخطط فور حدوث الأزمة لتجنب الخسائر أو على الأقل تخفيضها، لكن مثل هذه المخططات ليست موحدة وصالحة للجميع، إنما على كل مؤسسة تحضير مخطط خاص بها حسب معطياتها وطبيعة وحجم أنظمتها المعلوماتية.

الكلمات المفتاحية: مخطط، استمرارية النشاط، استئناف النشاط، الأنظمة المعلوماتية، الأزمة.

Abstract:

This study aims to clarify how the organization addresses the crises to which its information systems are exposed, by relying on the Business Recovery/continuity Plan, and the correct steps to be followed to succeed in this.

The study concluded that the Business Recovery/continuity Plan is imperative for each institution to adopt in order to face the crises to which

information systems are exposed, and to get out of them with the least losses, by studying the potential for crises that may occur and the degree of risk associated with each crisis, and coming up with multiple scenarios that lead to the preparation Suitable solutions for every possible scenario, in order to start implementing the scheme as soon as the crisis occurs, in order to avoid losses or at least reduce them, but such schemes are not uniform and valid for all, but each institution has to prepare its own scheme according to its data and the nature and size of its information systems.

key words: Schemes, Business Recovery Plan, Business continuity Plan, Information Systems, Crisis.

مقدمة:

أثر التطور التكنولوجي الكبير في مجال ادارة الأعمال بشكل مباشر على الحياة المؤسسية، حيث أصبحت جميع المؤسسات تعتمد في تسيير أعمالها على أنظمة معلوماتية متطورة، ومتكونة من حواسيب، خوادم وشبكات، وبطبيعة الحال أفراد أكفاء لادارتها، ورغم أن هذه الأنظمة المعلوماتية ساهمت في تطور المؤسسات، وساعدت في تسريع الأعمال واختصار الجهد والوقت، إلا أن الأخطار التي تتعرض لها كبيرة وقد تكون مدمرة، فقد تتعرض الأنظمة إلى مخاطر وأزمات تدمر الأنظمة جزئياً، ومخاطر أخرى قد تدمرها كلياً، وتنقسم هذه المخاطر إلى مخاطر مادية منها ما يكون متعمد كالتكسير والسرقة، ومنها ما يكون نتيجة كوارث طبيعية كالفيضانات والزلازل والحرائق، وهناك مخاطر برمجية كالإصابة بالبرامج الضارة أو التعرض للهجمات المعلوماتية الناتجة عن القرصنة باستغلال ثغرات النظام.

ورغم اعتماد المؤسسات على طرق حماية مادية ككاميرات المراقبة وأجهزة الإنذار، وأخرى برمجية كمضادات الفيروس والجدران النارية إلا أنها لا تجدي نفعا عند التعرض لأزمات وكوارث كبيرة، ومن هنا ظهرت ضرورة التفكير في إيجاد حلول لاستعادة نشاط المؤسسة عموماً ونشاط الأنظمة خصوصاً بعد أي أزمة، وكان مخطط استئناف/استمرارية النشاط أفضل حل لذلك، وهو عبارة عن مخطط تحضره المؤسسة مسبقاً لمواجهة أي كارثة محتملة، ويكون على ثلاث مراحل: قبل الأزمة، خلال الأزمة، بعد الأزمة، حيث تقوم المؤسسة بتحديد البنية التحتية لنظامها، وتحديد ثغراته والمخاطر المحتملة وأثرها عليه، وبعد ذلك تشكيل خلية أزمة تتكون من أفراد أكفاء من أجل ادارة الأزمة عند حدوثها واتخاذ أفضل القرارات وتقييم الوضع بعد ذلك، واستنتاج الدروس وبالتالي تغيير ما يجب تغييره وإضافة ما يجب إضافته.

ونظرا لحساسية الأنظمة المعلوماتية وضرورتها في استمرارية المؤسسة، وكثرة المخاطر التي قد تتعرض لها، والعجز عن مواجهتها تم طرح الاشكالية التالية:

كيف يساعد مخطط استئناف/استمرارية النشاط في حماية الأنظمة المعلوماتية في حال الأزمة؟

للإجابة على هذه الاشكالية وجب الاجابة على مجموعة من التساؤلات:

- ما هي الأزمات التي قد تتعرض لها الأنظمة المعلوماتية؟
 - ما هو مخطط استئناف/استمرارية النشاط؟ وكيف يتم اعداده وتنفيذه؟
 - هل يعتبر مخطط استئناف/استمرارية النشاط ضروري لحماية المؤسسة؟
 - هل مخطط استئناف/استمرارية النشاط عبارة عن وثيقة أو خطة جاهزة تستطيع أي مؤسسة اعتمادها؟ أم يختلف باختلاف المؤسسات وطبيعة أنظمتها المعلوماتية؟
 - كيف يساهم المخطط في حماية الأنظمة المعلوماتية؟
- لدراسة الموضوع تم الاعتماد على الفرضيات التالية:
- الفرضية الأولى: مخطط استئناف النشاط ضرورة حتمية لاستمرارية المؤسسة وأنظمتها المعلوماتية.
 - الفرضية الثانية: مخطط استئناف/استمرارية النشاط يختلف حسب حجم الأنظمة المعلوماتية.
 - الفرضية الثالثة: مخطط استئناف/استمرارية النشاط يختلف حسب حساسية الأنظمة المعلوماتية.

أهداف الدراسة

نسعى من خلال هذه الدراسة إلى تحقيق الأهداف التالية:

- إلقاء الضوء على أهم المخاطر التي قد تتعرض لها الأنظمة المعلوماتية والتي تضع المؤسسة في موقف الأزمة.
- التعريف بمخطط استئناف/استمرارية النشاط وأهميته، وضرورة تواجده في كل مؤسسة.
- توضيح خطوات تحضير المخطط وكيفية تنفيذه خلال الأزمة، وطريقة استخلاص الدروس بعد الأزمة عن طريق اتباع استراتيجية تقييم فعالة تساعد المؤسسة في اكتشاف نقاط ضعف مخططها والعمل على تحسينها.

منهج التحليل

تم في هذه الدراسة الاعتماد على المنهج الوصفي التحليلي لوصف حالات الأزمة التي تتعرض لها الأنظمة المعلوماتية ومدى تأثيرها على سيرورة النشاط، والتعريف بمخطط استئناف/استمرارية النشاط وأهميته، وتحليل مدى تأثير المخطط بطبيعة حجم وحساسية الأنظمة المعلوماتية.

للإجابة على الاشكالية المطروحة والأسئلة المرافقة لها تم تقسيم البحث إلى مبحثين أساسيين:

- المبحث الأول: أزمات الأنظمة المعلوماتية.
- المبحث الثاني: عملية استئناف/استمرارية نشاط الأنظمة المعلوماتية خلال الأزمة.

المبحث الأول: أزمات الأنظمة المعلوماتية

تعتبر الأنظمة المعلوماتية الوتر الحساس في المؤسسة، إذ أصبح اعتماد هذه الأخيرة في تسيير أعمالها مرتكزا على الأنظمة المعلوماتية والشبكات، لكن هذه الأنظمة معرضة للعديد من الأخطار من كل الأنواع، ما قد يؤدي أحيانا إلى تلفها وفقدان المعلومات والبيانات التي تضمها وهذا ما يسمى بالأزمة، ويختلف أثر التهديدات حسب شدة هذه الأخيرة ونسبة الاستعداد لها من طرف المؤسسة، ومن خلال هذا المبحث سنتعرف على مفهوم الأزمة وسماتها، ومختلف الأزمات التي قد تقع فيها الأنظمة المعلوماتية، مع توضيح أهمية الاجتهاد في توفير حماية للمعلومات وأنظمتها.

المطلب الأول: ماهية الأزمة

تتعرض أنظمة المعلومات إلى العديد من التهديدات منها ما يمكن تداركه ويكون بسيطا، ومنها ما يؤدي إلى أزمة حقيقة تؤدي إلى توقف عمل الأنظمة، وقد يتطور الأمر إلى توقف المؤسسة ككل، ومن خلال هذا المطلب سنتعرف على أنواع الأزمات والسمات والمؤشرات الحقيقية التي تدل على أن المؤسسة في حالة أزمة.

الفرع الأول: تعريف الأزمة

نستطيع القول أننا في حالة أزمة عند حدوث حدث استثنائي يعطل بصفة كبيرة العمل المعتاد للعمليات المهمة للزبائن الداخليين والخارجيين، هذا الحدث إن لم يحل ينتج عنه تأثيرات مباشرة أو غير مباشرة كبيرة.¹

كما تتمثل وضعية الأزمة في الأثر السلبي المهم والمستمر على النتائج المالية للمؤسسة، على العلامات وعلى صورتها، إضافة إلى علاقاتها مع الشركاء الأساسيين.²

وتعرف على أنها فترة حرجة أو حالة غير مستقرة يترتب عليها حدوث نتيجة مؤثرة.³ إذا الأزمة هي عبارة عن كشف الاختلالات ما يدفع المؤسسة إلى إعادة التفكير، فالأزمة تضع الإدارة في وضعية حساسة تفرض عليها أخذ معايير فورية وجذرية، وتقاس شدة الأزمة بمستوى ضياع نشاط المؤسسة.⁴

كل التعاريف السابقة استندت في تعريفها للأزمة على عامل التأثير والنتيجة المترتبة، متناسين عنصر المفاجأة، والذي نجده في التعاريف التالية:

الأزمة هي إدراك لحدث غير متوقع، يؤثر على أداء المؤسسة، يفضي إلى نتائج غالبا ما تكون سلبية تهدد توقعات المؤسسة.⁵

وتعرف على أنها حدث مفاجئ فيه إثارة وعنف ومدته الزمنية قد تكون قصيرة أو ممتدة لعد أشهر.⁶

كما تعرف على أنها لحظة حاسمة حرجة أو قد تكون تزايد وتراكم مستمر لعدة أحداث وأمور غير متوقع حدوثها في وقتها وتتعلق بمصير الكيان الإداري أو قد تتعلق بجزء من النظام أو على مستوى النظام بأكمله، وتمثل مشكلة ذات صعوبة أمام متخذ القرار.⁷

إذا الأزمة هي عبارة عن حالة أو حدث تتعرض له المؤسسة فجأة، يؤثر بشكل كبير على سير العمليات، ويحدث نتائج وتأثيرات جسيمة قد تصل أحيانا إلى إيقاف النشاط بصفة مستمرة أو مؤقتة، قد تمس الأزمة كيان المؤسسة ككل، أو نظام المؤسسة أو جزء من النظام كنظام المعلومات.

الفرع الثاني: سمات الأزمة

اختلف الباحثون في تقديم تعريف محدد للأزمة، لذا من الضروري إعطاء مجموعة من السمات التي تميز جميع الأزمات منها:⁸

- المفاجأة: فهي حدث غير متوقع سريع وغامض، أو موقف مفاجئ.
- جسامه التهديد: إذ تؤدي الأزمة إلى خسائر هائلة تهدد الاستقرار وتصل أحيانا إلى القضاء على كيان المؤسسة.
- الارباك: فالأزمة حالة تحدث ارباكا داخل المؤسسة، وتخلق حالة من القلق والتوتر، وعدم يقين في البدائل المتاحة.

- ضيق وقت المواجهة: فالأحداث تقع وتتصاعد بشكل متسارع وحاد، الأمر الذي يتطلب اتخاذ قرارات حاسمة في وقت محدود ما يخلق نوعاً من الضغط وفقد السيطرة أحياناً. بالنسبة لسمة المفاجأة فقد أو ضحت العديد من الدراسات أن الأزمة لها مؤشرات تسبقها، إذ بين موقع معهد إدارة الأزمات بأنه في 34% من المؤسسات ظهرت الأزمة فجأة، بينما في 66% من المؤسسات كانت هناك مؤشرات لموقف الأزمة واشتعلت فجأة، وهذا يعني أن ما يقارب ثلثي الحالات التي تعتقد فيها المؤسسات أنها تعرضت لأزمة فجائية كانت هناك مؤشرات لها ولكن المؤسسة أهملتها.⁹

وعليه فعلى مسيري المؤسسات التمتع بقدر عال من اليقظة الاستراتيجية والتفطن لحدوث الأزمات قبل حدوثها، الأمر الذي يساعد في عملية التحضير والاستعداد الجيد لها.

المطلب الثاني: أزمات أنظمة المعلومات

تتعرض المؤسسة ككل إلى العديد من الأزمات، لكن خلال هذا البحث سنركز على أزمات الأنظمة المعلوماتية خصوصاً، فما هي مختلف الأزمات التي تتعرض لها الأنظمة المعلوماتية؟ وما الفائدة من صرف أموال ومجهودات من أجل حماية الأنظمة والمعلومات؟

تتعرض أنظمة معلومات المؤسسة إلى العديد من التهديدات والأزمات، تختلف هذه الأخيرة حسب حجم الأضرار التي تخلفها، كما يمكن تقسيمها إلى أزمات مادية وأزمات برمجية.

الفرع الأول: أزمات أنظمة المعلومات المادية

1. تدمير البنية أو جزء منها

ويكون ذلك غالباً نتيجة الكوارث الطبيعية، التي قد تعرض أحياناً مجتمعاً بأكمله إلى أخطار شديدة وخسائر فادحة، ومن أشهر الكوارث: الزلازل والأعاصير والفيضانات والحرائق، إضافة إلى درجة الحرارة العالية أو الرطوبة العالية التي تلحق الضرر بالحواسيب والأجهزة الإلكترونية.

الخسائر الناتجة عن هذه الكوارث ليست سوى جزءاً من نتائج الكارثة، فالتكاليف غير المباشرة مثل توقف الانتاج، اغلاق المؤسسة وفقدان العمل قد يكون لها آثار طويلة الأجل على المؤسسة وعلى الاقتصاد ككل، وأفضل حل هو العودة السريعة للسوق.¹⁰

العديد من المناطق في العالم تكون أكثر عرضة لهذه الكوارث من غيرها، الأمر الذي يؤدي إلى تدمير مراكز البيانات والمدن بأكملها، لذا وفي الولايات المتحدة قامت SUN* بتطوير مفهوم مهم للجابة على هذا النوع من الكوارث: الصندوق الأسود (Blackbox) عبارة عن مركز

بيانات متحرك حقيقي يعمل على ضمان استمرارية خدمات تكنولوجيا المعلومات عقب أي كارثة كبيرة.¹¹

وتعتبر هذه الأزمة من أكبر وأخطر الأزمات التي قد تتعرض لها المؤسسات.

2. تدمير مركز البيانات

ضياح وتدمير مركز بيانات يعتبر حدث خطير جدا، مركز البيانات غالبا ما يكون محمي ضد الكوارث كالفيضانات، انقطاع التيار، الحرائق والأعاصير، ولكن هناك العديد من السيناريوهات التي لا يتم تغطيتها كالاختلاس الداخلي، الهجمات الارهابية، انتشار الأمراض المعدية.... فضياح مركز بيانات يؤثر بدوره على العديد من الزبائن وله عواقب وخيمة.¹²

3. توقف عمل أنظمة المعلومات

ويعني ذلك توقف عمل أنظمة المعلومات لفترات ما يسبب خسائر كبيرة للمؤسسة، وغالبا ما يكون ذلك بسبب الأعطال التقنية كانقطاع التيار الكهربائي، انقطاع الانترنت أو حدوث أعطال في مكونات النظام أو تلف أجهزة الاعلام الآلي بسبب تقادمها.

كل هذه الأزمات ناتجة عن تهديدات مادية تمس الأجهزة، وهي مدمرة جدا وتضع المؤسسة في مواقف حرجية، لكن مع التطور التكنولوجي اليوم أصبح من السهل تدارك مثل هذه الأزمات بالنسبة للأنظمة المعلوماتية، وذلك عن طريق الافتراضية أو توفير موقع بديل.

الفرع الثاني: أزمات أنظمة المعلومات البرمجية

1. إصابة أنظمة المعلومات

غالبا ما يحدث هذا في جميع المؤسسات بجميع أنواعها، ويظهر أثر الإصابة كبيرا كلما كانت البيانات التي تضمها الأنظمة حساسة واستراتيجية، ويكون السبب في إصابة الأنظمة البرامج الضارة مثل:

أ. الفيروسات: تعرف الفيروسات على أنها: برمجيات خبيثة بطبيعتها، تؤثر سلبا في الحواسيب بشكل مباشر، وفي غير الحواسيب بشكل غير مباشر، فالفيروس عندما يحذف ملفات مهمة للعملاء فإن التأثير يتعدى الحاسوب إلى العملاء وسمعة الشركة، والفيروسات لها تأثيرات منها ما يقوم بحذف ملفات أو برامج أو تعطيلها عن العمل، ومنها ما يقوم بزراعة برامج خبيثة أخرى قد تكون تجسسية، ومنها ما يعطل الجهاز بالكلية، وهناك أنواع للفيروسات منها ما يكون مكون من أجزاء متعددة، ومنها ما تتغير صفاته بشكل دوري، ومنها ما يكون متخفيا حتى من برامج مكافحة الفيروسات.¹³

ب. الديدان المعلوماتية: الديدان عبارة عن برامج مستقلة تنتقل من حاسب لآخر داخل الشبكة دون الحاجة لتدخلات بشرية، وتنتشر بسرعة أكبر من الفيروس، ويمكن أن تخفي معطيات وبرامج واتلافها، وإعاقة عمل شبكة معلوماتية¹⁴، عملها ليس ضار بصفة مباشرة ولكن سرعة تكاثرها وانتقالها السريعان يؤثران سلبا في فعالية الحاسوب وشبكة المعلومات. وبالنسبة لتحقيق الدودة فهو أمر صعب ولكن بمجرد النجاح في ذلك تحدث خسائر كارثية، وأكبر دليل هو الدودة المعروفة تحت اسم Slammer وهي أشهر دودة عبر التاريخ، ففي 25 جانفي 2003 انتشرت الدودة عبر الانترنت وأصابا أكثر من 90% من أنظمة المعلومات العالمية في 10 دقائق.¹⁵

ت. القنابل المنطقية: القنبلة المنطقية هي برنامج خبيث، يستقر في النظام وينتظر حدث معين (تاريخ، نشاط، معلومة معينة ...) وهذا مل يسمى بالزناد لينفذ نشاطه الهجومي.¹⁶ ولمعرفة خطورة هذا الرمز فقد قام "تيموتي آلن ليود" إطلاق قنبلة الكترونية ألغت كافة التصاميم وبرامج الانتاج لأحد أكبر مصانع التقنية العالمية في نيوجرسي التي تعمل لحساب وكالة الفضاء NASA والبحرية الأمريكية.¹⁷

ويوجد برامج ضارة أخرى غير التي تم ذكرها مثل برنامج حصان طروادة التجسسي، لكن عمله ليس تعطيل النظام وإنما التجسس بمختلف الطرق وبالتالي تظهر نتائجه بصفة تدريجية وليس بصفة مفاجئة، أما البرامج المذكورة فنتيجتها تكون مفاجئة والمفاجأة هي أهم سمة للأزمة.

2. اجتياح النظام

غالبا ما يتم اجتياح النظام عن طريق هجمة رفض الخدمة وهي نشاط خبيث يترجم بانشغال أو عدم اتاحة مؤقت أو دائم لعدة مكونات نظام الاتصال عن بعد.¹⁸ وتتم بعدة طرق منها:

أ. استهلاك موارد النظام: الحواسيب قدرتها لا تحمل إلا موارد محددة: قدرة الأقراص الصلبة، مساحة الذاكرة، قدرة عناصر الشبكة...¹⁹ وعن طريق استهلاك المعتدي أكبر جزء ممكن من

هذه الموارد فإن هذا سيحدث خنق وقطع لعمل التطبيق²⁰، فتعبئة منطقة التخزين يؤدي إلى مرحلة يصبح لا يمكن استعمالها.

ب. اجتياح النظم والضغط عليها:

- اجتياح خادم الشبكة: فاجتياح خادم الشبكة أو خادم الويب بطلبات خاطئة يثير عطل الشبكة²¹، فكل خادم لا يستطيع ضمان الخدمة إلا في نطاق محدد، والضغط بمعنى عدد الطلبات بوحدة الزمن يجب أن تبقى في إطار الحدود ما يمثل واحد من خصائص الخادم.²²

- اجتياح خادم الرسائل: هذا النوع من التعدي يستعمل خادم الرسائل لموقع ما من أجل ارسال رسائل غالبا تكون إخبارية وغير مرغوب فيها لعدد كبير من الجهات عن طريق إخفاء هويته، إلى غاية تعبئة البريد بالرسائل الإلكترونية، وبالتالي تعطيل خدمة رسائل الموقع.²³

ت. فيروس bot: هذا الفيروس لا يعمل سوى أنه ينتشر، ولكن في ساعة محددة أو إشارة معطاة آلاف أو ملايين الآلات المصابة تتصل بنفس الخادم المستهدف وتثير انهياره.²⁴

هجمة رفض الخدمة حتى وإن كانت لا تستطيع تدمير المعلومة أو الوصول إلى مناطق ممنوعة داخل نظام معلومات المؤسسة، إلا أنها يمكن أن تؤدي إلى إغلاق موقع الويب، فمثلا بالنسبة لمواقع التجارة الإلكترونية، هذه الهجمات هي جد ضارة، لأن المستهلكين لا يمكنهم القيام بعملية الشراء بما أن الموقع خارج الخدمة²⁵، وكذلك إذا كان هناك مثلا موقع ويب لمزايدة إذا أصبح غير متاح بسبب هجمة رفض الخدمة فالموقع يمكن أن يضيع جزء مهم من المداخيل.²⁶

وعليه فإن هذه الهجمة مضرّة بالنسبة للمستعملين الذين يعتمدون على تطبيقات أو مواقع أو أنظمة عليها العمل باستمرار، والتي قد يؤدي تعطيلها ولو لمدة معينة إلى خسارة مداخيل، خسارة سمعة، تضییع زبائن، تضییع مصالح...

المبحث الثاني: عملية استئناف/استمرارية نشاط الأنظمة المعلوماتية

خلال الأزمة

كل مؤسسة مهما كان نوعها أو حجمها أو مجال نشاطها، فهي معرضة في أي لحظة لحصول كارثة أو أزمة على مستوى أنظمة معلوماتها، الأمر الذي قد يعرضها إلى خسائر جمة، لذا من الضروري التفكير في وضع مخططات تساعد على استمرارية أو حتى استئناف نشاطها خلال حدوث الكارثة.

المطلب الأول: ماهية مخطط استئناف/استمرارية النشاط

من خلال هذا المطلب سنتعرف على مفهوم مخطط استمرارية النشاط ومخطط استئناف النشاط والفرق بينهما، وأهم المبادئ التي يتم احترامها عند إعدادة.

الفرع الأول: تعريف مخطط استئناف/استمرارية النشاط

1. مخطط استمرارية النشاط (PCA):

مخطط استمرارية النشاط (PCA) يحدد مجموع النشاطات التي تضمن استمرارية المؤسسة بعد وقوع كارثة، يجب أن يُرافق بتدابير الطوارئ، فهو مخطط على المدى القصير، يسمح بتحديد كمية الاحتياجات من أجل استمرارية النشاط حتى في حالة التدهور بعد الانقطاع القصير من بعض الثواني إلى بعض عشرات الدقائق²⁷.

2. مخطط استئناف النشاط (PRA)

مخطط استئناف النشاط هو مجموع الاجراءات التي تسمح باستئناف النشاط على موقع النجدة بعد الكارثة، الانقطاع هنا يعد من بعض الساعات إلى بعض الأيام، تطبيق مخطط الاستمرارية هنا يظهر مستحيلا. كل ممثل نظام وكل نشاط في المؤسسة له اجراءات استئناف خاصة. يمكن أن يكون هناك مخطط استئناف النشاط حسب النظام، حسب المحيط، حسب التطبيق، حسب مجال النشاط أو حسب الموقع، حسب السياسة الأمنية المحددة²⁸

وهناك فرق بين مخطط استئناف النشاط ومخطط استمرارية النشاط، فهذا الأخير مرتبط بمفهوم الاتاحة العالية، وهدفه ضمان اتاحة المعلومات مهما كان المشكل، في حين أن مخطط الاستئناف لا يسمح باتاحة كلية على مستوى المعلومات، وإنما يسمح فقط بضمان أن النشاطات يمكن استرجاعها خلال وقت محدد مسبقا، فالفرق بينهما ضئيل، وهما مرتبطان ببعضهما، إذ يتدخل مخطط الاستئناف عندما يواجه مخطط الاستمرارية سيناريو خطير أو كارثة²⁹.

مخطط استئناف النشاط هو مخطط طوارئ يهدف إلى استئناف نشاط الانتاج التجاري في أقرب وقت ممكن، يمكنه تحمل إعادة إنتاج الحد الأدنى من الكفاف في الانتاج، بينما مخطط استمرارية النشاط يتطلب الشفافية الكاملة للمستخدمين في حالة وقوع كارثة، وبالتالي يتطلب هذا المخطط الحصول على نفس المعدات في جميع المواقع لضمان تناسقية الانتاج (الموقع الأصلي والمواقع الاحتياطية) لذلك يعتبر مخطط استمرارية النشاط أكثر تكلفة من مخطط استئناف النشاط³⁰.

ونجد في العديد من المراجع استخدام مصطلحي الاستئناف والاستمرارية لنفس المعنى وهذا خطأ، فرغم أن المفهومين يتماشيان ويعملان معا إلا أن الفرق بينها واضح فمخطط الاستمرارية يعني عدم الانقطاع عن العمل وبالتالي تكلفته تكون عالية، في حين مخطط الاستئناف يعني الانقطاع لمدة معينة وتكلفته تكون أقل من المخطط السابق، إلا أنه في العديد من الحالات الاختيار بينهما لا يكون متاحا وإنما مفروضا، فقد تقع المؤسسة في أزمة كبيرة جدا يستحيل فيها استمرارية النشاط ويتدخل هنا مخطط الاستئناف من أجل استعادة النشاط في أقل وقت ممكن، أي أن الاستمرارية تكون مستحيلة.

الفرع الثاني: أهمية مخطط استئناف/استمرارية النشاط

في الوقت الحاضر، تعتبر كمية البيانات التي تنتجها المؤسسة في يوم واحد محيرة للعقل، ولا يمكن التفكير أبدا في انقطاع الوصول إلى البيانات، من هنا برزت أهمية المخططات التي تضمن استمرارية أو حتى استئناف الوصول إلى البيانات ومتابعة النشاط.

أصبحت هذه المخططات قضية أساسية لنظم المعلومات، فمجرد الحفظ البسيط لم يعد كافيا خصوصا في حال الكوارث الكبرى، وبما أن نظم المعلومات أصبح عنصر حساس وحرص للمؤسسة فعليه دائما أن يكون متاحا، وكما يشير مسؤولي مخططات استئناف النشاط: "لكي تكون مستعدا لجميع الاحتمالات عليك أن تتخيل الأسوأ"³¹.

كما يوجد مجموعة من الاحصائيات الناتجة عن منتدى أمن المعلومات الفرنسي (CLUSIF) تسمح بفهم مدى أهمية وضع مخطط استئناف/استمرارية النشاط:³²

- 95% من عمال المؤسسات صرحوا أنهم فقدوا ملفات معلوماتية تمثل ساعة إلى عدة أيام من العمل.

- 20% من الحواسب المحمولة تعرضت لكارثة (تكسير أو سرقة).

- 70% من المؤسسات الصغيرة والمتوسطة لا تقوم بحفظ معطياتها.

- 60% من المؤسسات الصغيرة والمتوسطة والتي تعرضت لأزمة معلوماتية اختفت في غضون 5 سنوات.

- 98% من المؤسسات ذات الأكثر من 200 عامل لديهم اعتماد معتدل إلى قوي على المعلوماتية.

- 42% من المؤسسات ذات الأكثر من 200 عامل ليس لديهم عملية رسمية لتسيير استمرارية النشاط.

وبالنظر لهذه الاحصائيات يتم التأكد من أهمية مثل هذه المخططات، فنتائج الاهمال والتجاهل قد تؤدي إلى اختفاء المؤسسة، لأن العالم اليوم أصبح غير آمن والمسير اليقظ عليه أن يسير بعقلية توقع حصول الأسوأ دائما من أجل تشديد الاحترازا، والتأهب الدائم لمواجهة السيناريوهات الكارثية، ومخططات الاستئناف/الاستمرارية تجعل عملية حفظ المعلومات والمحافظة على الأنظمة المعلوماتية عملية ممنهجة ورسمية تفرض مجموعة من الاجراءات و الممارسات الضرورية لتحقيق الأمن.

المطلب الثاني: مراحل عملية استئناف/استمرارية النشاط في ظل الأزمة

عملية استئناف/استمرارية النشاط عبارة عن عملية متكاملة، وليست حلول فورية يتم تطبيقها عند حدوث الأزمة، وتمر هذه العملية بثلاث مراحل، مرحلة ما قبل الأزمة، مرحلة الأزمة، مرحلة ما بعد الأزمة.

الفرع الأول: مرحلة التخطيط والاعداد(مرحلة ما قبل الأزمة)

استعدادا للأزمة هناك عدة ترتيبات من الضروري تحضيرها مسبقا، وهي:

■ مخطط الأزمة(التوثيق)

يجب أن يكون مخطط الأزمة كاملا وجاهزا مسبقا، ففي يوم الكارثة فرق التدخل ليس لها وقت لتضيقه في التفكير والتفسير، وإنما عليهم الاعتماد على إجراءات مكتوبة ومفصلة³³، لذا على مسؤول استمرارية النشاط تحضير وثيقة بيداغوجية تعمل على تقديم استراتيجية استمرارية الخدمة .

ويتمثل مخطط الأزمة في مخطط المأوى(الزبائن، العمال، المعدات، المخزون، المعطيات...)، مخطط استمرارية النشاط، مخطط اتصالات الأزمة(داخلي وخارجي، حلول تكنولوجية لاتصالات الأزمة)، مخطط العودة للحالة الطبيعية.³⁴

ويجب الإشارة إلى أنه لا يوجد أزمة مشابهة لأخرى بسبب اختلاف الأسباب وأنواع المؤسسات، لذا من غير الممكن تحضير مخطط نموذجي، ولا يمكن الاستفادة من بعض مبادئ مخطط آخر.³⁵

وإنما يتم تحضير المخطط حسب السيناريو المتوقع، وبما أن السيناريوهات متعددة فعلى المؤسسة تحضير مخططات متعددة.

■ تحديد النطاق وتوثيق البنية التحتية الحالية

وضع مخطط استئناف النشاط يمر قبل كل شيء بمعرفة جيدة للمحيط وتوثيق البنية التحتية، وهذا ما يسمح بتسليط الضوء على أي تبعيات قد تكون موجودة بين مختلف عناصر البنية التحتية وبدون معرفة هذه التبعيات فتقريباً من المستحيل وضع مخطط استئناف فعال وموثوق³⁶ لذا يجب إحصاء مجموع الموارد التي تحتاجها المؤسسة من أجل أن تعمل خاصة الموارد والمعلومات الاستراتيجية، فبمجرد تعريفها يجب الأخذ بعين الاعتبار احتمالية وقوع دمار تام، سواء كان سببه حادثي أو إجرامي، لذا في نظام مثالي المعطيات الاستراتيجية تكون مرتبة حسب أهميتها، ومأرشفة بطريقة تجعلها دائماً متاحة³⁷، وعند تعريف البنية التحتية لا يكفي معرفة 99% من الأجهزة والبرامج الخاصة بالمؤسسة لأن 1% الذي بقي يمكن أن يكون أصل ثغرة أمنية كبيرة.³⁸

وعليه من الضروري تحديد التطبيقات والتجهيزات والبرامج والملفات المهمة والحساسة حسب معايير التكيف للمؤسسة حيث ستركز جهود استعادة النشاط عليها.

■ فحص ثغرات الجهاز الأمني

من أجل تحضير مخطط استئناف/استمرارية فعال من الضروري القيام بفحص عام لجهاز أمن نظم المعلومات ومعرفة كل الثغرات الموجودة به، ومن أهم ما يجب فحصه:³⁹

- تنظيم عملية الأمن.
- التغطية التأمينية المتعلقة بالمخاطر المعلوماتية.
- الأمن العام (المحيط، الوصول المادي، أمن الحرائق وكوارث الماء، التعليمات الأمنية).
- وسائل النجدة الموضوعة أو المخطط لها (الخوادم، الشبكة، الحواسيب، التغذية الكهربائية، التهوية، التجهيزات والامدادات، العمال...).
- وسائل حماية المعلومات المخزنة.
- التحويلات المعلوماتية: النسخ الاحتياطية، الأرشفة.
- التحويلات الورقية: الوثائق، الملفات، الأرشفة.
- الوسائل الموضوعة لضمان أمن التبادلات الخارجية (حماية الشبكة).
- عقود صيانة الأجهزة والبرامج (التحقق من درجة مشاركة مزودي الخدمات).
- عقود الموردين للموارد الحساسة (ضمان استعادة الخدمات في حال الانقطاع).
- وسائل الادارة واستغلال الأنظمة (فحص ثغرات الأنظمة، متابعة الانذار..).

هذا الفحص يجب أن يكون دوري فلا يعني سلامة عنصر ما من عناصر النظام عند إجراء الفحص أن الأمر مستمر وكل شيء على مايرام، فما هو آمن اليوم يمكن أن يكون غير ذلك في الغد، كما أنه من الضروري معالجة كل الثغرات المكتشفة أثناء الفحص بسرعة كبيرة تفاديا لاستغلالها بأي شكل من الأشكال.

■ تشخيص وتحليل المخاطر

تشخيص المخاطر وتحليلها هدفه ترتيب المخاطر التي تؤدي إلى عدم الاتاحة الكلية أو الجزئية للنظام، ووضع الأولويات في معالجتها، ويكون ذلك عن طريق دراسة عنصري الخطر الأساسيين:

- التكرار: ويسمى باحتمالية الحدوث وفي هذا التقييم نجد مدرستين: ⁴⁰ إما بالاعتماد على تحقيق فحص شامل للنظام ومختلف عناصره وإما انطلاقا من قواعد المعارف الموجودة والمعرفة مسبقا.

فالمخاطر المتكررة والتي تحدث بانتظام ولكن بنتائج محدودة فإن المقاربة التاريخية بتعريف قوانين الاحتمال للتكرار والخطورة تسمح بتقييم الخطر. ⁴¹ وفي هذا التقييم، فإن تاريخ الحوادث المفهرس للنظام وتجارب الأفراد يمكن أن يحمل دلائل مهمة، والاعتماد كذلك على احصائيات الحوادث الأمنية الحادثة مسبقا.

أما بالنسبة للمخاطر الاستثنائية فالأمر يختلف، ولا يمكن تحديد فرص التكرار إلا بالاعتماد الحقيقي على قياس درجة التنبؤ بحصول هذه الحوادث.

- الخطورة: وتسمى أيضا الأثر المالي للحوادث، وقد يكون هذا الأثر مقبولا وأحيانا غير مقبول إذا قام بتخريب قوي لعنصر مهم من عناصر العملية العملية.

ومن أجل تقييم أثر الحوادث المعرفة يجب تخيل "سيناريوهات كوارث"، وهذا في حال المخاطر الكبيرة التي تتعرض لها المؤسسة مثل: حريق، زلزال، فيضان، انفجار فيجب التفكير عن طريق السيناريو من أجل تحديد شروط البقاء تحت ما يسمى اليوم في المؤسسات المالية "قيمة الخطر"، فتقييم الخطورة تهدف في أسوأ الحالات إلى تحديد أهمية نزيف الخزينة، والتي يمكن أن تؤثر على المنظمة، وهذا التحليل يجب إعادة النظر فيه سنويا، وإعطاء الاعتبار للخسائر الثانوية وليس فقط الفورية ⁴²

إذا تقدير مستوى الخطر عن طريق (الاحتمال، الخطورة) يسمح بحساب الخطر، ونتاج التقارير التي تحمل قائمة المخاطر وأولوياتها بعلاقة مع سيناريوهات الحوادث الممكنة.

■ توفير موقع بديل

لحماية نظم المعلومات لابد من توفير موقع بديل يسمى قاعة النجدة، يتم اللجوء إليه حالة حدوث الكارثة، والمؤسسة أمام خيارات منها: إقامة هذا الموقع داخل المؤسسة وهذا في حالة المنشآت الكبيرة، اتفاقيات التعاون المتبادل بين مؤسستين حيث تحول المنظمة المضيفة نظامها إلى نمط التشغيل في حال الطوارئ لمساعدة المؤسسة الأخرى على معالجة بياناتها المهمة، المواقع الباردة وهي عبارة عن بنايات خارج المؤسسة فارغة وتكون جاهزة لاستيعاب الأجهزة اللازمة لمعالجة البيانات بشكل مؤقت، والمواقع الساخنة وتختلف عن الباردة بأنها مجهزة بكافة الأجهزة والحواسيب اللازمة لاستعادة النشاط خلال فترة قصيرة من وقوع الأزمة⁴³.

وفي هذا الصدد ظهر اليوم ما يسمى بالافتراضية، والتي تسمح بخلق مخططات استئناف نشاط بطريقة أكثر بساطة وبترشيد التكاليف، إذ أن أغلب مخططات الاستئناف تعتبر أن الأنشطة يجب استئنافها على موقع ثاني والذي يجب أن يكون قادرا على استقبال جزء أو كل خوادم الموقع الأول، إذ يجب على الأغلب الاستثمار في الأجهزة والتي قد لا يتم استخدامها أبدا، فإذا كانت الخوادم افتراضية، يكون الاستثمار في الأجهزة جد منخفض، لأن الافتراضية تبسط عملية النسخ بتخزين الأجهزة الافتراضية على خزان تخزين تحمل النسخ المتماثل وغير المتماثل، إضافة إلى أن محطات التشغيل أيضا يمكن أن تكون افتراضية، يكفي فقط نهايات "خاملة" على الموقع الثاني من أجل أن تستطيع مجموعة كبيرة من العمال الاستمرار في العمل⁴⁴.

وعليه نستنتج أنه لا يمكن استئناف النشاط بعد الأزمة إلا بتوفير مواقع أخرى لنشاط الأنظمة المعلوماتية سواء كانت هذه المواقع حقيقية أو افتراضية.

■ تعيين خلية أزمة

من الضروري في التخطيط لمواجهة الأزمات أن يتم اعداد فريق أو خلية أزمة وتقديره على الورق سواء حدثت الأزمة أم لم تحدث، يتميز أفراد هذه الخلية بمجموعة من الخصائص والخبرات التي تؤهلهم لإدارة الأزمة بدءا من استشعار الأزمة قبل حدوثها حتى مواجهة آثارها عند الحدث واستخلاص الدروس المستفادة منها⁴⁵.

وعليه فإن مواجهة الأزمة تتطلب كفاءات بشرية تُحدد مهامها مسبقا، كل حسب تخصصه، وأهم شخص في هذا الفريق هو مسؤول مخطط الاستمرارية أو مخطط النجدة

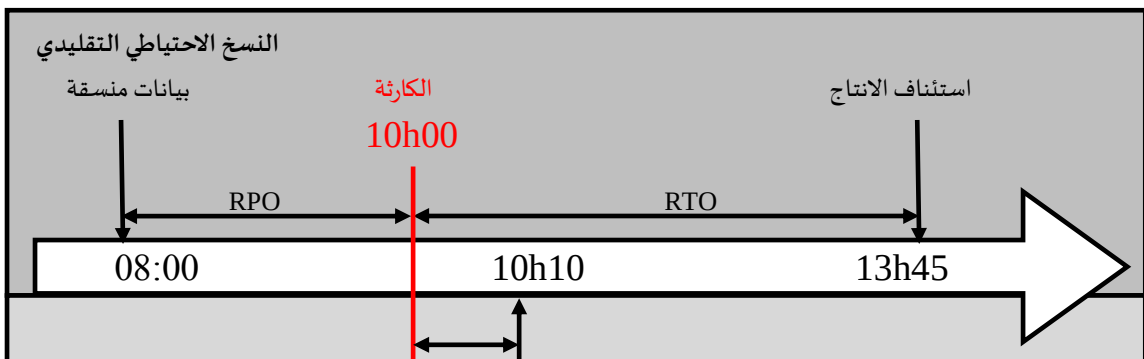
وهو المسؤول عن عملية التخطيط لتسيير الأزمة ويكون إما تحت إشراف المدير العام أو مدير نظم المعلومات أو مسؤول أمن نظم المعلومات، مدير مخطط الاستمرارية هو المسؤول الأول عن اتخاذ القرارات وتنفيذها وتسيير العمليات خلال وقوع الكارثة، ولكن ليس بمفرده بل بمساعدة فريق عمل أو ما يسمى أحيانا بخلية تسيير الأزمة.

■ النسخ الاحتياطي

إن نهج مسؤولي مخططات استئناف النشاط يتمثل حاليا في تصور العديد من السيناريوهات الكارثية المثبتة في أقصى الحالات، وأحسن نهج حاليا يتمثل في اتباع توصيات معهد التعافي من الكوارث (DRI)، إذ يجب تمييز عنصرين جد مهمين في كل مخطط استئناف نشاط وهما RTO^{**} و RPO^{***} .⁴⁶

يعد هدف وقت الاسترداد (RTO) وهدف نقطة الاسترداد (RPO) عاملين رئيسيين في خطة التعافي من الكوارث، إذ يشير RTO إلى الحد الأقصى لوقت التوقف قبل أن يعمل التطبيق بعد وقوع كارثة، ويشير RPO إلى أقصى قدر من فقدان البيانات الأخيرة من حيث الوقت قبل أن يعمل التطبيق بعد وقوع الكارثة.⁴⁷

بمجرد تحديد RTO و RPO لكل نظام ونوع كارثة تأتي الحاجة إلى الاتفاق على الوقت الذي يمكن فيه اجراء نسخ احتياطي للنظام، والمدة التي يمكن أخذها احتياطيا، ومدى القدرة على التأثير على نظام الانتاج بينما يتم عمل نسخة احتياطية منه، إذ تعتبر بعض التطبيقات حاسمة للغاية بالنسبة للأعمال لدرجة أن أصحابها لن يقبلوا ببساطة أي وقت تعطل أو فقدان البيانات.⁴⁸ لذا يجب التفكير والعمل على الحماية المستمرة، وهي نسخة احتياطية مستمرة تشبه أليتها النسخ المتماثل في الوقت الحقيقي (يضمن النسخ المتماثل مطابقة مثالية في جميع الأوقات بين المصدر والبيانات المنسوخة)، وتتمثل التقنية في التقاط كل تغيير عن طريق نسخه تلقائيا إلى وحدة تخزين أخرى، وبالتالي يسمح باستعادة فورية في أي وقت، ويطلق عليها النسخ الاحتياطي المستمر مما يسمح بالاسترداد في أي وقت ولها عدة مزايا منها: هدف نقطة الاسترداد قريب من الصفر، الاستعادة الفورية، نقل النسخ الاحتياطي إلى موقع آخر.⁴⁹



Source: Cédric Georgeot, op.cit, p81.

يوضح الرسم البياني الفرق بين النسخ أو الحفظ التقليدي والمستمر، في البنية التقليدية لدينا فقدان البيانات ساعتين من RPO بين النسخ الاحتياطي الأخير والوقت الذي حدثت فيه الكارثة، بعد هذه الكارثة من الضروري استعادة البيانات من الأشرطة والتي يمكن أن تستغرق وقتاً طويلاً (3:45 ساعات من RTO) حسب الحجم، في حين يفترض أن يوفر النسخ الاحتياطي المستمر صفر RPO ووقت الاستعادة شبه فوري أو يمكن أن يستغرق بضع لحظات حسب الحجم إذا كان من الضروري استرداد اللقطة من خليج آخر، ففي مثالنا توقف الانتاج لمدة 10 دقائق (RTO=10 دقائق).⁵⁰

إذن النسخ الاحتياطي ضروري وعلى كل مؤسسة أن تحاول الوصول إلى الحالة المثالية التي تتمثل في عدم فقدان أي بيانات (RPO قريب من الصفر)، وتوقف الانتاج قصير قدر الامكان (قيمة RTO قريبة من الصفر).

وكما ذكرنا سابقاً ليست كل التطبيقات والبيانات بنفس الدرجة من الأهمية والحساسية، فهناك ما يكون ضياعها ليوم كامل أمر عادي، وهناك من لا تحتمل لحظة ضياع واحدة، لذا عند انشاء خطة الاستئناف/الاستمرارية يجب العمل على فهم مدى أهمية وحرية كل تطبيق وتحديد RTO و RPO، والجدول الموالي يعتبر مثالاً لتحديد RTO و RPO بناء على مستوى حرية التطبيق.

الجدول رقم (1): تحديد RTO و RPO بناء على مستوى حرية التطبيق

الحرية	RTO	RPO
عالية	> ساعة	قريب من الصفر
متوسطة	بين ساعة و4 ساعات	> 2 ساعات
منخفضة	بين 4 ساعات و12 ساعة	> 8 ساعات
منعدمة	< 12 ساعة	< 8 ساعات

Source: Paolo Bruni&al, Managing DB2 for z/OS Utilities with DB2 Tools Solution Packs, Redbooks, 2013, p57.

من خلال الجدول نلاحظ أنه يمكن تحديد مدة RPO و RTO حسب حرجية التطبيق، فالتطبيق الاستراتيجي ذو الحرجية العالية لا يتحمل ضياع أي معطيات ولا يمكن أن يتحمل توقف نشاطه لأكثر من ساعة، في حين التطبيق غير المهم وغير الاستراتيجي يمكن أن يتحمل وقت استرداد لأكثر من 12 ساعة ونقطة استرداد لأكثر من 8 ساعات. لكن قد يقول قائل لماذا لا يتم توفير RPO و RTO قريب من الصفر لكل التطبيقات، لأنه ببساطة يتعلق الأمر بالتكاليف، فكلما كان RPO و RTO منخفض كلما كان وضع الحلول مكلفا، ويظهر ذلك من خلال الجدول التالي:

الجدول رقم(2): تكاليف الحلول حسب مستوى RPO و RTO

المستوى	RPO	RTO	التكلفة
1	فوري	فوري	€€€
2	24 ساعة أو أكثر	48 ساعة أو أكثر	€€
3	7 أيام أو أكثر	5 أيام أو أكثر	€

Source: Eric Maillé, VMware vSphere4-Mise en place d'une infrastructure virtuelle-, Editions Eni, 2010, p332.

فمن خلال الجدول نلاحظ أن كلما اقترب هدف نقطة الاسترداد RPO وهدف وقت الاسترداد RTO من الصفر وكان الاسترجاع فوريا كلما كانت تكلفة وضع الحلول مرتفعة، وكلما زادت مدة الاسترجاع كلما كانت التكلفة منخفضة، ويكون الاختيار طبعا حسب أهمية وحرجية النظام أو التطبيق أو المعطيات.

الفرع الثاني: مرحلة التنفيذ(مرحلة الأزمة)

واحدة من الصعوبات التي تواجه تسيير الأزمة تتمثل أساسا في فهم الظاهرة وتعريف الوقت الذي يجب اطلاق عملية التسيير فيه وتبدأ بإجراءات محدودة في الوقت والهدف، وهنا يجب إعطاء ملاحظة لمن له فرصة النجاح، المخطط يجب أن يفعل بسرعة منذ الاشارات الأولى للكارثة إن أمكن، بمعنى قبل ظهور الاضطراب وهي وظيفة العملياتيتين، وفي الحالات الأكثر خطورة يمكن البدء بمرحلة الانقاذ التي تهدف في حالة الطوارئ إلى حماية الأشخاص، السمعة والممتلكات. المهم هو التنظيم بطريقة مختلفة من أجل السماح بمواصلة الإنتاج بأقل وقت توقف ممكن.⁵¹

ومن الصعوبات التي يواجهها المسؤولون أيضا في حالة الأزمة هي التحكم في الأعصاب، فالتحكم الجيد في الأزمة هو قبل كل شيء نتيجة قرارات المدير الذي يجب أن يكون له القدرة

على فرز المعلومات حسب درجة أهميتها، والإبتعاد تماما عن جانب المشاعر (الغضب، الغيرة، الغرور.....) لأنها الخطر الأول الذي يواجه المقرر.⁵²

وعليه يتم التفكير والاستنتاج إذا كان من الممكن، أو من المفيد والمهم العودة إلى الوضعية الأولى، واختيار الاستراتيجية المناسبة إما بالعودة إلى الوضعية الأولى أو العمل على تطوير المؤسسة.⁵³

ومن خلال التعرض لمرحلة التحضير ومرحلة التنفيذ يظهر لنا جليا مدى أهمية مرحلة التحضير والاعداد، بل تعتبر تقريبا كل شيء من أجل مواجهة الأزمة، أما مرحلة التنفيذ فهي مجرد تطبيق لما تم التخطيط له، فاذا كان هذا الأخير جيدا غالبا ما يتم مواجهة الأزمة بطريقة جيدة والعكس صحيح، لذا فان الاستثمار الأكبر في مخطط استئناف/استمرارية النشاط يكون في التحضير الجيد لمراحل مواجهة الأزمة.

الفرع الثالث: مرحلة التقييم(مرحلة ما بعد الأزمة)

بعد أي أزمة أو كارثة تتعرض لها المؤسسة بصفة عامة أو أنظمة المعلومات بصفة خاصة، تجد المؤسسة نفسها في وضعية تقييم، حيث تقوم المؤسسة بتقييم أثر الأزمة على نشاط أنظمة المعلومات وذلك بالتطرق للنقاط التالية:⁵⁴

- تحليل التكاليف المالية.
- تعريف التطبيقات الحساسة.
- تحديد مدة الاستئناف الضرورية.
- تفصيل البنية التحتية لنظام المعلومات.
- قائمة المستخدمين الحرجين.

هذا التقييم يسهل عملية اتخاذ القرارات التي غالبا ما تكون صعبة بعد الكارثة، ويمكن تكملته ب:⁵⁵

- حلول النجدة وإطلاقها.
- تكوين خلية أزمة مختصة إن لم تكن موجودة من قبل، وتطويرها وتحسينها إن وجدت، أو إضفاء بعض التغييرات إن تطلب الأمر.
- وضع مخطط استئناف/استمرارية النشاط إن لم يكن، وتعديله وتحسينه إن كان.

كما يجب القيام باختبارات منتظمة من أجل التحقق من التنفيذ الجيد للمخطط وتصحيح الأعطال الممكنة، إضافة إلى أن اختبار وتكوين وتحقيق عمليات يسمح بتعريف الفجوات من أجل تحضير الأفراد المشاركين في تفعيل مخططات النجدة وتحسين فعالية المخططات.

هذه المرحلة لا تقل أهمية عن سابقتها في الأساس الذي تُبنى عليه عملية التحسين المستمر لمخططات استئناف/استمرارية النشاط، فبعد كل مرحلة تقييم -بعد أي أزمة- يتم اكتشاف ثغرات في المخططات يتم اصلاحها وملاحظات مهمة يجب أخذها بعين الاعتبار، وممارسات يجب تطبيقها في الأزمات القادمة، وقرارات حاسمة وضرورية يجب اتخاذها، وبهذه الطريقة تكتسب المؤسسة خبرات عالية في مواجهة الأزمات، وتحسن بذلك من أدائها وفرص بقاءها واستمراريتها.

خاتمة:

من خلال هذه الدراسة تم معالجة اشكالية كيفية مساهمة مخطط استئناف/استمرارية النشاط في حماية الأنظمة المعلوماتية واسترداد نشاطها عند مواجهة أي أزمة أو كارثة، وتم التوصل إلى النتائج التالية:

- إن المخاطر التي تتعرض لها الأنظمة المعلوماتية والتي قد تضعها موضع أزمة حقيقية عديدة ولا يمكن حصرها أو تحديدها أو حتى توقعها، لذا فإن سبل الحماية التقليدية ككاميرات المراقبة وأجهزة الانذار وبرامج الحماية أصبحت لا تجدي نفعا في حال مواجهة المؤسسة والأنظمة لكوارث كبيرة، وأصبحت عملية التخطيط للأزمات عملية ضرورية من خلال تحضير مخطط لاستئناف أو استمرارية النشاط في حال حدوث ذلك.

- المعلومات اليوم تعتبر رأس مال العديد من المؤسسات والتي قد يؤدي ضياعها ولو لفترة وجيزة إلى خسارة كبيرة للمؤسسة لذا فإن مخطط استئناف/استمرارية النشاط مخطط ضروري يسعى لضمان اتاحة المعلومات حتى في حالات الأزمات الكبيرة والمفاجئة.

- مخطط استئناف/استمرارية النشاط ليس بمخطط مطاط وموحد يصلح لجميع المؤسسات، بل هو خاص، ويختلف من مؤسسة لأخرى حسب حجم الأنظمة المعلوماتية وحساسيتها، ولا يمكن ولا في أي حال من الأحوال الاستعانة بمخطط مؤسسة أخرى

وتطبيقه، لأن لكل واحدة بنية تحتية وكفاءات بشرية خاصة بها، كما أنه لا يمكن استخدام مخطط نموذجي لجميع الأزمات، لأنه لكل أزمة خصائص مختلفة عن غيرها.

- مخطط استئناف/استمرارية النشاط وإن لم يحقق الاستئناف الكامل أو الاستمرارية الكاملة لنشاط الأنظمة المعلوماتية، فعلى الأقل يخرجها من الأزمة بأقل الخسائر الممكنة.

- مخطط استئناف/استمرارية النشاط عبارة عن منهجية متكاملة تتكون من ثلاث مراحل: مرحلة التخطيط قبل الأزمة، مرحلة التنفيذ خلال الأزمة ومرحلة التقييم بعد الأزمة، كل مرحلة من هذه المراحل مهمة وضرورية، لكن حصة الأسد تكون لمرحلة التخطيط والتحضير والاعداد، فاذا كان التحضير جيدا كان التنفيذ ناجحا والعكس صحيح.

- أفضل تحقيق لاستئناف/استمرارية النشاط عندما يكون هدف وقت الاسترداد RTO قريب من الصفر، وهدف نقطة الاسترداد RPO قريب من الصفر، بمعنى أن عملية النسخ الاحتياطي عملية مستمرة، وعند حدوث الكارثة لا يكون هناك أي ضياع للبيانات، وبالتالي لا يتم خسارة الوقت في عملية الاسترداد.

التوصيات

- باعتبار أن المؤسسات اليوم تعمل في عالم معلوماتي سمته الأساسية هي المخاطر والتهديدات المختلفة فمُحْتَم على هذه المؤسسات مواكبة هذا العالم والتحصن ضد مخاطره غير المتوقعة التي تضع المؤسسة في حالة الأزمة، ومن هنا أصبح تحضير مخطط استئناف/استمرارية النشاط ضرورة حتمية لاستمرارية المؤسسات، وذلك من خلال انشاء خلية في المؤسسة تسمى بخلية الأزمات تقوم بدراسة أنواع الأزمات الممكن حدوثها واحتمالية تكرارها ودرجة الخطورة المصاحبة لها ل يتم الاستعداد لها عن طريق المخطط المذكور واعطاء هذه الخلية اهتماما خاصا وتزويدها بكل المعدات والكفاءات اللازمة.

- على المؤسسات التحضير الجيد والجدي لمخطط استئناف/استمرارية النشاط، وبذل كل الأموال والمجهودات لذلك، فمرحلة التحضير أهم مرحلة والتي بدونها لا يمكن المرور للمراحل اللاحقة، ففي حالة الأزمة لا يمكن التفكير في حلول وإنما التطبيق فقط.

- لنجاح المؤسسات في تخطي الأزمات بأقل الأضرار عليها إما جلب الكفاءات البشرية في مجال الأنظمة المعلوماتية أو الاتصال بمختصين في هذا المجال للاستفادة من الاستشارات اللازمة في حال أي خطورة ومواكبة المستجدات في مجال المعلوماتية.

الهوامش:

- ¹ Bernard Foray, la Fonction RSSI «guide des pratiques et retours d'expériences», ED Dunod, Paris, 2010, p251.
- ² Jean Paul Louisot, gestion des risques (100 question pour comprendre et agir), ED AFNOR, 2010, p127.
- ³ عبد الكريم أحمد جميل، إدارة الأزمات و الكوارث، الجنادرية للنشر و التوزيع، 2016، ص14؛
- ⁴ Nicolas Moinet, la boite à outils de la sécurité économique, ED Dunod , Paris, 2015, pp 100-101
- ⁵ صلاح عبد الحميد، الإعلام و إدارة الأزمات، مؤسسة طيبة للنشر و التوزيع، الطبعة 1، 2013، ص191؛
- ⁶ محمد عبد المنعم شعيب، ادارة المستشفيات:منظور تطبيقي:الادارة المعاصرة:نظم المعلومات:نظم اقتصاديات الصحة:نظم الادارة الموقفية، دار النشر للجامعات، 2014، ص254؛
- ⁷ نفس المرجع، ص254؛
- ⁸ عبد الكريم أحمد جميل، مرجع سابق، ص15؛
- ⁹ صلاح عبد الحميد، مرجع سابق، ص193؛
- ¹⁰ OCDE, Etude de l'OCDE sur la gestion des risques d'inondation :Bassin de la Loire, OCDE, France, 2010, p105.
- * SUN: Stanford University Network, Sun Microsystems est un constructeur de matériel informatique et éditeur de logiciels américain.
- ¹¹ Philippe Gillet, Virtualisation des systèmes d'information avec VMware-Architecture, projet, sécurité et retours d'expérience, ED ENI, 2009, p202.
- ¹² Ibid, p202.
- ¹³ خالد بن سليمان الغثير، مهندس محمد بن عبد الله القحطاني، أمن المعلومات بلغة ميسرة، مكتبة الملك فهد الوطنية، الرياض، الطبعة الأولى، 2009، ص ص 65-66؛
- ¹⁴ Kenneth Laudon et Jane Laudon , Management des systèmes d'information, ED Pearson, 9^{ème} édition, France, 2006, p352
- ¹⁵ George Sadowsky, James x.Dempsey, Alan greenberg, Barbara J.Mack, Alan Schwartz, Information Technology Security Handbook , the International Bank for Reconstruction and Development, Washington, 2003, p22.
- ¹⁶ Eric Filiol, «les virus informatiques: théorie, pratique et applications», Springer, deuxième éditions, Paris, 2009, p127
- ¹⁷ أسامة سمير حسين، الاحتيال الالكتروني - الأسباب و الحلول -، الجنادرية للنشر و التوزيع، الطبعة الأولى، 2011، ص 101؛
- ¹⁸ Michel Lafitte, Sécurité des systèmes d'information et maitrise des risques, ED Revue Banque, 2003, p88.
- ¹⁹ Eric Léopold, Serge Lhoste, la sécurité informatique, ED Puf, 3^{ème} édition, Aout, 2007, p56.
- ²⁰ Tom Gallagher, Bryan Jeffries, Lawrence Landauer, Chasser les failles de sécurité, les meilleures pratiques pour tester la sécurité de vos logiciels, ED microsoft, Janvier 2007, p376.
- ²¹ Kenneth Laudon et Jane Laudon, 2006, op cit, p354
- ²² André Vaucamps, CISCO: Sécurité des routeurs et contrôles du trafic réseau, ED ENI, 2010, p14.
- ²³ Robert Longeon, Jean-luc Archimbaud, guide de la sécurité des systèmes d'information à l'usage des directeurs, Centre National de la Recherche Scientifique(CNRS), Paris, 1999, p13.
- ²⁴ André Vaucamps, op cit, p14.
- ²⁵ Kenneth Laudon et Jane Laudon , 2006, op cit , p355
- ²⁶ Tom Gallagher, et autres, op cit, p377

- ²⁷ Philippe Atelin, Réseaux informatiques-notions fondamentales-, ED ENI, troisième édition, France, 2009, p47.
- ²⁸ Ibid, p47.
- ²⁹ Philippe Gillet, op.cit, p 200.
- ³⁰ Cédric Georgeot, Bonnes pratiques, planification et dimensionnement des infrastructures de stockage et de serveur en environnement virtuel, MVP Microsoft, ED Books On Demand, Paris, 2011, p96.
- ³¹ Philippe Gillet, op.cit, p199.
- ³² Ibid, p 200.
- ³³ Patrick Boulet, Management de la sécurité de système d'information, ED Lavoisier, Paris, 2007, p197
- ³⁴ Ocde, op.cit, p107
- ³⁵ Nicolas Moinet, op.cit, p101.
- ³⁶ Marc Benisty, Microsoft SharePoint Server2007(MOSS2007) Déploiement et Administration, ED ENI, France, 2010, p299
- ³⁷ Eric Léopold, op.cit, pp107-108
- ³⁸ Jean-Marc Royer, Sécurisé l'informatique de l'entreprise: enjeux, menaces, prévention et parade, ED ENI, 2004, p33.
- ³⁹ Philippe Gillet, op.cit, p 207
- ⁴⁰ Nicolas Mayer, Jean philippe Humbert, la gestion des risques pour les systèmes d'information, centre de recherche public Henri Tudor , Article paru dans le magasin MISC n24, 2006, p4
- ⁴¹ Jean Paul Louisot, op.cit , p38
- ⁴² Ibid , p38.
- ⁴³ تركي راجي الحمود و آخرون، "التخطيط لمواجهة الطوارئ الخاصة بأنظمة المعلومات المحاسبية في المصارف التجارية الأردنية"، مجلة جامعة الملك عبد العزيز: الاقتصاد و الادارة، الأردن، العدد 2، 2017، ص ص 186-187؛
- ⁴⁴ Philippe Gillet, op.cit, pp 210-211.
- ⁴⁵ غادة البطريق، العلاقات العامة وفن ادارة الأزمات، أطلس للنشر والانتاج العلمي، 2017، ص 74.
- ^{**} RTO: Recovery Time Objective.
- ^{***} RPO: Recovery Point Objective.
- ⁴⁶ Philippe Gillet, op.cit, p 204.
- ⁴⁷ Michael Collier, Robin Shahan, Fundamentals of Azure-Microsoft Azure Essentials-, Microsoft Press, 2015, p167.
- ⁴⁸ W.Curtis Preston, Backup & Recovery, O'Reilly, United States of America, 2007, p209.
- ⁴⁹ Cédric Georgeot, op.cit, pp 80-81.
- ⁵⁰ Ibid, p81.
- ⁵¹ Jean Paul Louisot , op.cit , p125.
- ⁵² Nicolas Moinet ,op.cit, p102.
- ⁵³ Ibid , p101.
- ⁵⁴ Philippe atelin, op.cit, p46.
- ⁵⁵ Ibid, p47.

المراجع:

أ. باللغة العربية:

1. أسامة سمير حسين، الاحتيال الالكتروني - الأسباب و الحلول -، الجندرية للنشر و التوزيع، الطبعة الأولى، 2011؛

2. تركي راجي الحمود و آخرون، "التخطيط لمواجهة الطوارئ الخاصة بأنظمة المعلومات المحاسبية في المصارف التجارية الأردنية"، مجلة جامعة الملك عبد العزيز : الاقتصاد و الادارة، الأردن، العدد 2، 2017؛
3. خالد بن سليمان الغثير، مهندس محمد بن عبد الله القحطاني، أمن المعلومات بلغة ميسرة، مكتبة الملك فهد الوطنية، الرياض، الطبعة الأولى، 2009؛
4. صلاح عبد الحميد، الإعلام و إدارة الأزمات، مؤسسة طيبة للنشر و التوزيع، الطبعة 1، 2013؛
5. عبد الكريم أحمد جميل، إدارة الأزمات و الكوارث، الجنادرية للنشر و التوزيع، 2016؛
6. غادة البطريق، العلاقات العامة وفن ادارة الأزمات، أطلس للنشر والانتاج العلمي، 2017؛
7. محمد عبد المنعم شعيب، ادارة المستشفيات: منظور تطبيقي: الادارة المعاصرة: نظم المعلومات: نظم اقتصاديات الصحة: نظم الادارة الموقفية، دار النشر للجامعات، 2014.

ب. باللغة الفرنسية

1. André Vaucamps, CISCO: Sécurité des routeurs et contrôles du trafic réseau, ED ENI, 2010.
2. Bernard Foray, la Fonction RSSI«guide des pratiques et retours d'expériences», ED Dunod, Paris, 2010.
3. Cédric Georgeot, Bonnes pratiques, planification et dimensionnement des infrastructures de stockage et de serveur en environnement virtuel, MVP Microsoft, ED Books On Demand, Paris, 2011.
4. Eric Filiol, «les virus informatiques: théorie, pratique et applications», Springer, deuxième éditions, Paris, 2009.
5. Eric Léopold, Serge Lhoste, la sécurité informatique, ED Puf, 3^{ème} édition, Aout, 2007.
6. Eric Maillé, VMware vSphere4-Mise en place d'une infrastructure virtuelle-, ED Eni, 2010.
7. Jean-Marc Royer , Sécurisé l'informatique de l'entreprise: enjeux , menaces, prévention et parade, ED ENI,2004.
8. Jean Paul Louisot, gestion des risques(100 question pour comprendre et agir), ED AFNOR, 2010.
9. Kenneth Laudon et Jane Laudon, Management des systèmes d'information, ED Pearson, 9^{ème} édition, France, 2006.
10. Marc Benisty, Microsoft SharePoint Server2007(MOSS2007) Déploiement et Administration, ED ENI, France, 2010.
11. Michel Lafitte, Sécurité des systèmes d'information et maitrise des risques, ED Revue Banque, 2003.
12. Nicolas Mayer, Jean philippe Humbert, la gestion des risques pour les systèmes d'information, centre de recherche public Henri Tudor, Article paru dans le magasin MISC n24, 2006.
13. Nicolas Moinet, la boîte à outils de la sécurité économique, ED Dunod , Paris, 2015.

14. OCDE, Etude de l'OCDE sur la gestion des risques d'inondation :Bassin de la Loire, OCDE, France, 2010.
15. Patrick Boulet, Management de la sécurité de système d'information, ED Lavoisier, Paris, 2007.
16. Philippe Atelin, Réseaux informatiques-notions fondamentales-, ED ENI, troisième édition, France, 2009.
17. Philippe Gillet, Virtualisation des systèmes d'information avec VMware-Architecture, projet, sécurité et retours d'expérience, ED ENI, 2009.
18. Robert Longeon ,Jean-luc Archimbaud, guide de la sécurité des systèmes d'information à l'usage des directeurs, Centre National de la Recherche Scientifique(CNRS), Paris, 1999.
19. Tom Gallagher, Bryan Jeffries, Lawrence Landauer, Chasser les failles de sécurité, les meilleures pratiques pour tester la sécurité de vos logiciels, ED microsoft, Janvier 2007.

ت. باللغة الانجليزية

1. Michael Collier, Robin Shahan, Fundamentals of Azure-Microsoft Azure Essentials-, Microsoft Press, 2015.
2. Paolo Bruni&al, Managing DB2 for z/OS Utilities with DB2 Tools Solution Packs, Redbooks, 2013
3. W.Curtis Preston, Backup & Recovery, O'Reilly, United States of America, 2007.