الدليل العملي للتعافي من الكوارث/خطط استمرارية العمل لعمليات نطاقات المستوى الأعلى

الإصدار 1.0.2

3 ديسمبر 2019

قائمة المحتويات

المحتويات

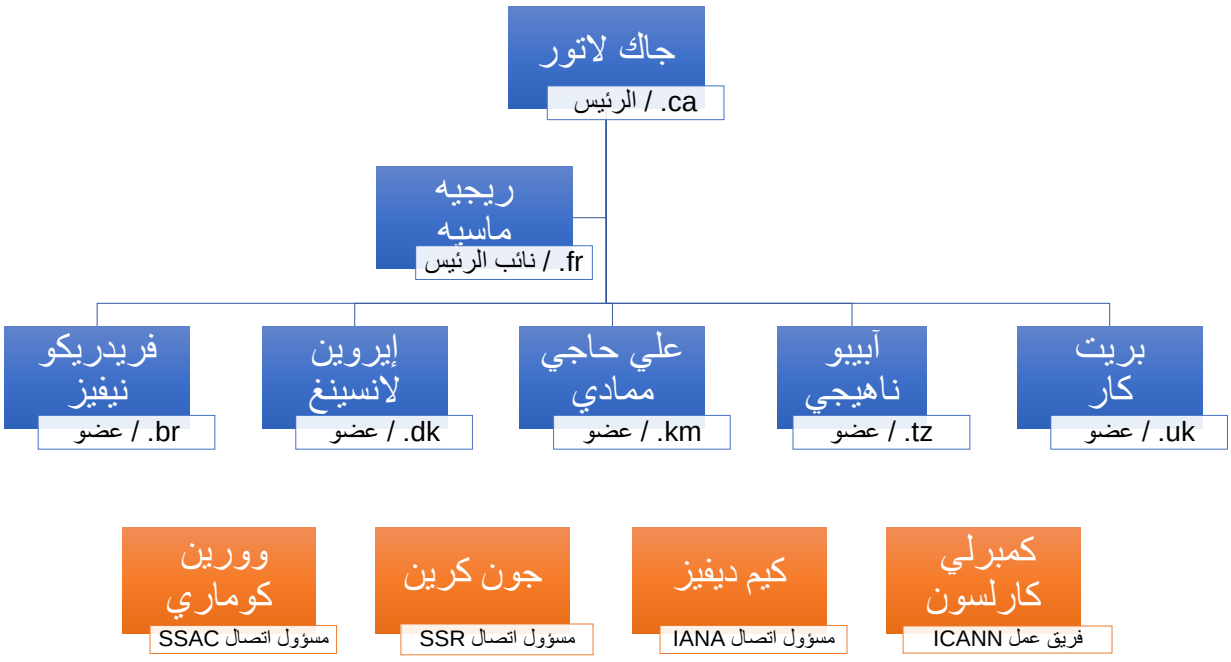
المقدمة

حول عمليات نطاقات المستوى الأعلى: أمن واستقرار ccTLD معًا

إن عمليات نطاقات المستوى الأعلى TLD-OPS عبارة عن مجتمع الاستجابة للحوادث لنطاقات ccTLD وبمعرفتها كما يقوم بتجميع المسئولين عن الأمن والاستقرار التشغيلي لنطاقات ccTLD الخاصة بهم. ويتمثل هدف مجتمع TLD-OPS في تمكين مشغلي نطاقات ccTLD على مستوى العالم من اكتشاف والحد من الحوادث التي قد تؤثر على أمن واستقرار خدمات ccTLD، مثل هجوم حجب الخدمة الموزعة DDoS، وحالات الإصابة بالبرامج الضارة وهجوم التصيّد. كما يتمثل الهدف من عمليات نطاقات المستوى الأعلى في مزيد من توسيع نطاق هياكل وعمليات وأدوات الرد والاستجابة للحوادث الحالية للأعضاء وليس استبدالها. كما أن مجتمع TLD-OPS منفتح على كل نطاق ccTLD، بصرف النظر عن عضوية منظمة دعم أسماء رموز البلدان ccNSO.

نبذة: https://ccnso.icann.org/en/resources/tld-ops-secure-communication.htm

أتوجه بالشكر الخاص للسيد دريك جومبيرتز، مدير الأمن من شركة EURid لإسهاماته البارزة في هذه الوثيقة والمشروع.



لجنة TLD-OPS الدائمة

كيفية استخدام هذه الوثيقة

يهدف كتيب المبادئ هذا إلى تقديم إرشادات عملية لكل من يريد تطبيق استراتيجية استمرارية الأعمال ضمن مشغل سجل أصغر. الجمهور المستهدف موجه نحو الإدارة العليا والوسطى أو أيهما. وهو يفترض أن مشغل السجل لديه الالتزام والرعاية والمهمة الموكلة إليه من الهيئة المشرفة عليه (سواء كان ذلك مجلس إدارة أو تمثيلًا حكوميًا أو أي شكل آخر) لتطوير المرونة ضد الأحداث التخريبية في شكل خطة لاستمرارية الأعمال.

نظرًا لأن هذه الوثيقة تحاول أن تكون عملية قدر الإمكان، فهي تحتوي على عدد من جداول الأمثلة العملية التي يمكن نسخها واستخدامها في المراحل المختلفة لكل من التطوير والتنفيذ.

كما يحتوي أيضًا على بعض الأمثلة التي يمكن استخدامها في صورة قوالب أو مصدر إلهام لوضع خطط استمرارية العمل/التعافي من الكوارث.

أخيرًا، سيجد القارئ "مربعات إجراءات" من حين لآخر في المستند تحتوي على اقتراحات ونصائح قابلة للتنفيذ: وصف صغير لأي نشاط ومن يجب عليه تنفيذه.

ما المقصود باستمرارية الأعمال؟

استمرارية الأعمال هي قدرة المؤسسة على مواصلة تنفيذ أو تسليم المنتجات أو الخدمات التي تعتبر هامة لشركة وأعمال مشغل سجل ccTLD وفقًا لمستويات مقبولة ومحددة مسبقًا بعد وقوع حادث مسبب للتعطل.

لاحظ أن استمرارية الأعمال لا تركز بالضرورة على الحوادث المسببة للتعطل من الناحية الفنية فقط. حيث يمكن أن تؤدي أي حادثة تخريبية ذات تأثير على الجاهزية التشغيلية لأي مؤسسة إلى إطلاق خطط استمرارية الأعمال. لذلك من المهم أن تحقق المنظمة فهمًا لما يمكن أن يعوق الجاهزية التشغيلية.

استمرار الأعمال في مقابل التعافي من الكوارث

ثمة ارتباط بين خطط استمرارية العمل (BCP) وخطط التعافي من الكوارث (DRP) ولكن لا يمكن لأي منهما أن يحل محل الآخر على الرغم من أن المرء سيجد أوجه تشابه عند البحث عن القوالب عبر Google، على سبيل المثال، تتكون الأولى من خطة عمل تركز على تقديم أعمال منتظمة أثناء الأزمات؛ أما الأخير فهو عبارة عن مجموعة فرعية ويتضمن إجراءات لتعافي الأنظمة الحيوية في أقصر وقت ممكن تتطلبه الأعمال.

وبمعنى آخر، سوف تحتوي أي خطة لاستمرارية الأعمال على إشارات إلى عدد من خطط التعافي من الكوارث. لأغراض هذا المستند، سنقوم بوضع خطط لاستمرارية الأعمال تضم خطة إجرائية من أجل سيناريو محدد.

كيف يمكن تحقيق هذا الهدف؟

يمكن للمرء من خلال استخدام بعض إرشادات المعيار ISO 22301 بشأن استمرارية الأعمال أن ينشئ إطار عمل عالمي يساعد في إنشاء خطط استمرارية الأعمال وإدارتها وتحسينها.

نظرًا لأن المهمة التشغيلية لمديري النطاقات متطابقة في الغالب في عالم نطاقات ccTLD، يمكن استخدام نهج مبسط مشترك يركز على التطبيق العملي بدلاً من التقنيات المعقدة والمستهلكة للوقت وأحيانًا المجردة لوضع خطط استمرارية العمل الصحيحة.

العاقة مع المعيار ISO/IEC 27001:2013

يركز المعيار ISO 27001 على أمن المعلومات والذي يتلخص في تطوير وتنفيذ ومراقبة وتحسين ضوابط للحفاظ على مستويات السرية والنزاهة والتوافر - والمختصرة باسم CIA. أما بالنسبة لشركات خدمات تكنولوجيا المعلومات، فإنها تشترك في قدر من التداخل مع استمرارية الأعمال.

وثمة فارق على الرغم من ذلك: حيث يركز المعيار ISO/IEC 27001 على تحقيق مستويات السرية والنزاهة والتوافر المطلوبة أثناء العمليات العادية ويتنبأ بالتخفيف الضروري من خلال التكنولوجيا والإجراءات؛ ويركز المعيار ISO 22301 على الحوادث التخريبية التي تعيق المؤسسة ويتنبأ بالخطط اللازمة للتعامل مع هذه الحوادث.

لفهم الفارق بين نظام إدارة أمن المعلومات (ISMS) ونظام إدارة استمرارية الأعمال (BCMS)، قد تكون من المفيد طرح بعض الأمثلة للتوضيح:

- يتم طرح التخزين الزائد مع حماية وتكرار RAID لزيادة النزاهة والتوفر (ISO/IEC 27001).
- تم تنظيم تمرينات تدريبات الحرائق للتأكد من أن الخسائر البشرية في حدها الأدنى في حالة نشوب حريق حقيقي (ISO 22301).
- يتم نشر حماية النقاط النهائية من الفيروسات لحماية أجهزة الكمبيوتر المحمولة وأجهزة سطح المكتب والأجهزة المحمولة من تهديدات الإنترنت (ISO/IEC 27001).
- تعتبر الإجراءات التي تمت تجربتها في حالة حدوث هجوم ناجح للفدية جزءًا من خطط استمرارية الأعمال من ناحية أخرى (ISO 22301).

النطاق (لهذه الوثيقة)

تستخدم هذه الوثيقة بمثابة إرشادات في تنفيذ أساس استمرارية الأعمال واستعادة القدرة على العمل بعد الكوارث ضمن مشغل سجل صغير.

ويجب أن تساعد هذه الوثيقة في الإجابة على الأسئلة التالية:

- كيف يمكن تحديد نطاق استمرارية العمل؟
- كيف يمكن تحديد المخاطر؟
- كيف يمكن تضمين استمرارية الأعمال في مبادئ عمل الشركة؟
- ما المطلوب لاستراتيجية فعالة لاستمرارية العمل؟
- ما المواد الحيوية؟
- كيف يمكن صياغة خطة استمرارية العمل أو خطة التعافي من الكوارث؟
- كيف يمكن لقيام بممارسات استمرارية الأعمال؟
- كيف يمكن التحسين؟

المراجع المعيارية

تقوم هذه الوثيقة على ما يلي:

- ISO 22301:2012 - الأمن المجتمعي - أنظمة إدارة استمرارية الأعمال - المتطلبات.
- ISO 31000:2009 - إدارة المخاطر - المبادئ والإرشادات.
- ISO/IEC 27001:2013 - تكنولوجيا المعلومات -- تقنيات الأمن -- نظم إدارة أمن المعلومات -- المتطلبات

الأحكام والشروط

انظر ISO 22301:2012 للاطلاع على المصطلحات والتعاريف المستخدمة في هذا المستند.

انظر RFC2119 لفهم مستويات المتطلبات.

سياق المؤسسة

على الرغم من أن معظم نطاقات ccTLD لديها مجموعة خدمات ومهمة متشابهة للغاية، إلا أن هناك دائمًا فرق كبير من شأنه إعطاء التوجيه لاستراتيجية استمرارية الأعمال. وبشكل عام، يمكن القول أن المهمة التشغيلية لمعظم نطاقات ccTLD هي:

- إدارة البنية التحتية لخادم الاسم لنطاق TLD الخاص بها.
- إدارة الخدمات العامة الضرورية لأي نطاق ccTLD. وبشكل أكثر تحديدًا، من المفترض أن يكون هذا موقع ويب للشركة وخدمة بحث إدارية مثل WHOIS أو RDAP.
- إدارة نوع ما من خدمات التسجيل التي تسمح بالتسجيل المباشر أو غير المباشر لأسماء النطاقات. قد تكون هذه واجهة بشرية مثل موقع ويب أو واجهة مخصصة من آلة إلى آلة مثل بروتوكول التزويد المرن EPP.
- وأخيرًا وليس آخرًا، سيدير السجلُ عددًا من أنظمة دعم الشركات التجارية التي قد لا يكون لها قدر كبير من الرؤية الخارجية، ولكنها ضرورية لكي تعمل المؤسسة (مثل البريد الإلكتروني والإنترانت وخادم الملفات، إلخ...)

يتمثل الغرض من هذه الخطوة الأولى في فهم من الذي يعتمد على المؤسسة، وبالتالي لديه بعض التوقعات التي يجب الوفاء بها خلال حادثة تخريبية ومن الذي تطالبه المؤسسة بالوفاء بمهمتها.

فهم المؤسسة وسياقها

إن أول خطوة رفيعة المستوى في بناء استراتيجية فعالة في استمرارية الأعمال تتمثل في الفهم الدقيق والشامل للأعمال وأصحاب المصلحة فيها. فسوف يكون للمساهمين وأصحاب المصلحة توقعات خاصة ومتطلبات من أجل صياغة الالتزامات التي يتعين وضعها في الاعتبار ضمان النطاق. ومن ثم، دائمًا ما يكون من الممارسات الجيدة إدراج أصحاب المصلحة ووصف طبيعتهم وفي النهاية مراجعة واستعراض توقعاتهم فيما يخص المرونة التشغيلية واستمرارية الأعمال. ويفضل القيام بهذا النشاط من خلال الإدارة من أجل الاستحواذ على التعقيبات والآراء المناسبة. يسرد العمود "الصلة باستمرارية الأعمال" علاقة التوقع باستمرارية الأعمال. بعض التوقعات قد لا تكون ذات صلة؛ في حين قد يتم اعتبار البعض الآخر هامة للغاية. وإلى هذا الحد، يمكن للمرء استخدام "مرتفع" أو "متوسط" أو "منخفض" أو "بدون" للإشارة إلى مدى الصلة. مثال: إذا ما تم اعتبار أحد التوقعات ذات صلة كبيرة باستمرارية الأعمال، فهذا يعني بشكل أساسي أن صاحب المصلحة لديه توقعات كبيرة - وعلى وجه الخصوص، قد يتوقع صاحب المصلحة أنها "مفيدة دائمًا"، بما يعني أن نظام أسماء النطاقات دائمًا في وضع تشغيل، فتكون صلة عندئذ عالية.

القائمة التالية عبارة عن قائمة غير شاملة تضم بعض **الأمثلة** التي يمكن استخدامها من أجل المساعدة في هذا التدريب. من الناحية العملية، يُنصح في البداية بمراجعة وتحديث القائمة وتحديد أصحاب المصلحة وتسميتهم (من أجل المقابلات الشخصية)، والتفكير في صياغة التوقعات في عبارات قصيرة وفي النهاية إجراء تقييم لمدى صلتها باستمرارية الأعمال.

المساهم أو صاحب المصلحة	التوقعات	الصلة باستمرارية الأعمال
الحكومة	توافر نظام أسماء النطاقات بنسبة 100% تكامل دقة السجل توافر نظام السجل مركز الخبرات في نظام أسماء النطاقات البحث والتطوير في نظام أسماء النطاقات إساءة استخدام أسماء النطاقات	عالية عالية عالية لا يوجد لا يوجد لا يوجد

ICANN	تسجيل لنطاقات ccTLD في IANA	لا يوجد
مجلس الإدارة	توافر نظام أسماء النطاقات بنسبة 100% تكامل دقة السجل توافر نظام الشركات	عالية عالية متوسطة
عامة الناس	توافر نظام أسماء النطاقات توافر تسجيل النطاقات	عالية عالية
معايير c-CERT	معلومات الأمن الولوج إلى بيانات المسجلين	منخفضة لا يوجد
الموظفين	توافر نظام الشركات	عالية
جهات إنفاذ القانون	تكامل تسجيل النطاقات	منخفضة
أمناء السجلات	توافر تسجيل النطاقات	متوسطة
المشتركون	توافر حل النطاقات تكامل تسجيل النطاقات	منخفضة منخفضة
مزود خدمة إنترنت محلي	حل النطاقات دعم الامتدادات الأمنية لنظام أسماء النطاقات	عالية لا يوجد
مجتمع وحدة حل التصديق	الوصول إلى ملف المنطقة	لا يوجد

جدول 1

هذه القائمة سوف تساعدك في تحديد الأولويات عالية المستوى فيما يخص استمرارية الأعمال.

سلسلة التوريد

في الشركات الكبرى الحديثة، تعتمد المؤسسات على عدد من الشركاء والمورّدين وموفري الخدمات إلخ... ولهذه الجهات بشكل واضح تأثير هام على استراتيجية استمرارية الأعمال ومن ثم يجب على المرء فهم اعتمادية المؤسسة على سلسلة التوريد. ومن الأنشطة والممارسات ذات القيمة العالية والتي لا يمكن الاستغناء عنها إدراج جميع المورّدين ممن لهم تأثير على المهمة التشغيلية للمؤسسة.

ومن الطرق العملية في إنشاء القائمة مطالبة إدارة التمويل بإعداد قائمة بجميع المورّدين، مع وصف قصير لما يقومون بتوريده في حقيقة الأمر. ومن خلال تلك القائمة، يمكن للمرء أن يحدد أيّ المورّدين له تأثير فعلي على المرونة التشغيلية. مثال: سوف يكون لموفر مركز البيانات بشكل واضح صلة عالية باستمرارية الأعمال؛ أما موفر الأثاثات مثل "إيكيا" على الجانب الآخر فسيكون له صلة أقل.

واعتمادًا على تأثير أي حادثة مع المورّد، فإننا نستخدم تسمية مختلفة للتأثير:

التأثير	الأثر
خطير	متوسط
تأثير كبير	في غضون أسبوع أو 7 أيام
تأثير متوسط	في غضون شهر أو 30 يومًا
تأثير منخفض	أطول من شهر أو 30 يومًا

جدول 2

الجدول التالي عبارة عن **مثال** على المساعدة في إنشاء هذه القائمة من المورّدين:

المورّد (الاسم)	الوصف	الصلة باستمرارية الأعمال	التأثير
ISP	مزود خدمة الإنترنت	عالية	خطير
معالج بطاقات الائتمان	عبارة عن كيان يقوم بتسهيل الاتصال بين التاجر وبنك حامل البطاقة.	متوسط - مرتفع	تأثير كبير
شركة هواتف	موفر خطوط الهاتف الأرضي	متوسطة	تأثير متوسط
خدمة البريد	موفر (البريد) الخدمة البريدية	منخفضة	منخفضة
شركة الكهرباء	استعادة الكهرباء		
شركة تسديد الرواتب	سداد الرواتب للموظفين		
شركة خدمات الكمبيوتر	شراء أجهزة الكمبيوتر للموظفين والخوادم من أجل توفير الخدمات		
موفري الشبكات/مزودي خدمة الإنترنت			
مشغلو شبكات المحمول			
شركة التأمين			

جدول 3

تحديد نطاق استمرارية الأعمال

الاستمرارية التشغيلية باعتبارها حجر الزاوية في استراتيجية استمرارية الأعمال

تشمل الاستمرارية التشغيلية جميع الأنشطة اللازمة من أجل إدارة "شركة الأعمال كالمعتاد". وهو ما ينطوي على دعم أصحاب المصلحة مثل أمناء السجلات والمسجلين والجمهور العام من منظور فني وتجاري وقانوني. كما ينطوي على تشغيل جميع الخدمات الفنية من أجل تسجيل وإدارة أسماء النطاقات ودعم الأسماء وأخيرًا وليس آخرًا التأكد من إتاحة وتوافر مساحة أسماء TLD أمام الجميع على الإنترنت.

ويجب التعامل مع قسم كبير من التأثيرات التكنولوجية من خلال الممارسات الهندسية المعيارية ولذلك ركز استمرارية الأعمال على تقييم مجموع الحوادث المعطلة ونتائجها المفترضة والمقدرة على الجاهزية التشغيلية. وهي تحدد عملية التخفيف من وطأة التأثيرات من خلال وضع السياسات والإجراءات، وأيضًا التكنولوجيا إذا لزم الأمر.

ومن ثم، يمكن تلخيص استمرارية الأعمال على النحو التالي

إدارة الإجراءات **الوقائية** وأيضًا **التصحيحية** من خلال السياسات والإجراءات والاختبارات والتكنولوجيا من أجل ضمان **الجاهزية التشغيلية والاستمرارية** في مواجهة الأحداث**المسببة للأعطال** ذات الطبيعة **الفنية** والطبيعة **غير الفنية** على السواء.

القيادة

إن وضع استراتيجية فعالة لاستمرارية الأعمال والحفاظ عليها يعد جهدًا وعملاً مستمرًا يتطلب الدعم من أعلى مستويات الإدارة. ومن ثم فإن أفضل مكان لإيواء ودعم المبادرات ذات الصلة باستمرارية الأعمال هو فريق الإدارة أو حتى مجلس الإدارة.

وعلى الرغم من الحاجة إلى إجراء مراجعات منتظمة للإبقاء على الخطط حديثة وذات صلة، يجب على الإدارة أيضًا أخذ زمام المبادرة من أجل تضمين استمرارية الأعمال في جميع طبقات العمليات (التكنولوجيا والهندسة والمشتريات والعمليات إلخ...).

الإجراء: تنفيذ ومراقبة دورة مراجعة سنوية على أقل تقدير من خلال فريق المراجعة.

التخطيط

يجب هذا القسم عن السؤال الخاص بكيفية وضع الخطط العملية لاستمرارية الأعمال بحيث تضع في الاعتبار التهديدات ونقاط الضعف ذات الصلة بالنسبة لمشغل السجل وأيضًا التأثير على المرونة التشغيلية للمؤسسة.

وسوف نبدأ أولاً بعملية إنشاء سجل للتهديدات/المخاطر وهو ما سوف يساعدنا في تحديد وتعريف النواحي التي يجب فيها التعامل مع استمرارية الأعمال. لاحظ أن بعض التهديدات تمتاز بصعوبة الحد منها أو الجاهزية للتصدي لها، إن يكن ذلك مستحيلاً. ومن الجدير التحري عن التهديدات وتقييم الخيارات الاستراتيجية. وقد لا تتجلى هذه الأشياء في صورة خطة لاستمرارية الأعمال، ولكن إلى خيارات استراتيجية[1]على المدى الطويل.

ولتحويل التهديدات والمخاطرات إلى مخاطر فعلية، يتعين علينا فهم تأثير الجاهزية والمرونة التشغيلية. ويمكن استخدام منهجية مبسطة لتقييم المخاطر من أجل المساعدة في الوقوف على السيناريوهات التي ينبغي التعامل معها. ومن خلال هذا التقييم، سوف تتم ترجمة عدد من هذه السيناريوهات إلى خطط تكتيكية لاستمرارية الأعمال في حين سوف تؤدي سيناريوهات أخرى إلى استراتيجية لاستمرارية الأعمال والتي يمكن استخدامها في صورة تعقيبات وملاحظات لهيئة الإشراف ولدعم القرارات الاستراتيجية.

[1] وقد تكون من الأمثلة النموذجية على ذلك "عدم الاستقرار السياسي" وهو ما قد يكون من الصعب جدًا الحد منه، كما هو الحال بالنسبة لنطاق ccTLD، فمن المهم وضع هذ الأمر في الاعتبار في استراتيجية استمرارية الأعمال الكلية.

ومتى ما أصبح واضحًا ماهية التهديدات/المخاطرات التي تحتاج لخطة فعلية لاستمرارية العمل، فيمكن وضع الخطة استنادًا إلى نموذج عام وشامل. ويجب حينئذ استخدم هذا النموذج في صورة إرشادات توجيهية لجميع الأقسام من أجل إعداد الإجراءات متى لزم ذلك.

وضع سجل بالتهديدات/المخاطرات

يعد سجل التهديدات/المخاطرات قائمة عالية القيمة تضم مصادر الكوارث التي قد يكون لها تأثير كبير على المرونة التشغيلية للمؤسسة. وقائمة التهديدات التالية تستند إلى الكتاب "إدارة استمرارية الأعمال" (الإصدار الرابع) - الرقم الدولي الموحد للكتاب 978-1-931332-35-4 وتم توسيعها بالأحداث الأخيرة الناشئة.

وعند تقييم هذه التهديدات، يجب على المؤسسة تقدير احتمالية الحدث استنادًا إلى البيانات الإحصائية المتاحة. إن احتمالية (أرجحية) الحدوث تُقاس على النحو التالي:

1. احتمالية كبيرة: حدث يقع سنويًا أو بوتيرة أكبر
2. محتمل: حدث يقع كل ثلاث سنوات في المتوسط
3. نادر: حدث يقع كل عشر سنوات
4. غير محتمل: حدث يقع مرة كل 50 سنة أو أكثر
5. خارج النطاق: خارج النطاق - لا يتم الالتفات إلى هذه الأحداث في استمرارية الأعمال

والاحتمالية لا تستند إلى الإحصائيات الداخلية ولكن على الإحصائيات ذات الصلة لكل من المنطقة والبلد والأعمال والبيئة[2]. ومن المهم الإشارة إلى أنه يتعين على الناس تحديد نقاط الاحتمالية (الجدول رقم 7 ورقم 8) وأيضًا تأثير المخاطر (الجدول 6) مع تفعيل الضوابط الأمنية الحالية. وتستند التهديدات إلى الإحصائيات؛ دون تفعيل أي ضوابط محددة.

فئة التهديد	التهديد	مطابق	الاحتمالية
الكوارث الطبيعية	الحريق	☐	_____
	الفيضان	☐	_____
	الإعصار/الزوبعة/العاصفة	☐	_____
	الطقس المناوئ	☐	_____
	الزلزال	☐	_____
	الانزلاق الأرضي/الانهيار الجليدي	☐	_____
	النشاط البركاني	☐	_____
	تسونامي	☐	_____
	ضربات البرق الهبوط	☐	_____
	الأرضي التلوث	☐	_____
	انتشار الحشرات	☐	_____
	القوارض	☐	_____
	_____	☐	_____
الموارد البشرية والجانب الطبي	خسارة فريق العمل الرئيسي	☐	_____
	المرض الوبائي	☐	_____
	نقص المهارات/العاملين	☐	_____
	المسائل الأسرية	☐	_____
	السطو	☐	_____
	التلف الضار (التخريب)	☐	_____
	الابتزاز	☐	_____
	_____	☐	_____

[2] وقد يكون أحد الأمثلة النموذجية على الأحداث ذات الصلة بالطقس مثل الأعاصير وثيق الصلة للغاية بأجزاء من الولايات المتحدة، لكنه غير ذي صلة تمامًا بالأجزاء الأخرى من نفس الدولة.

الجانب الإلكتروني	هجوم حجب الخدمة الموزعة DDOS	☐	_____
	القراصنة	☐	_____
	فقد البيانات	☐	_____
	فيروسات الفدية	☐	_____
	الأنشطة ذات الصلة بالحرب الإلكترونية	☐	_____
	_____	☐	_____
خارجي	الكساد	☐	_____
	العصيان المدني	☐	_____
	النشاط الإرهابي	☐	_____
	الحرب/الغزو	☐	_____
	التدخل السياسي/تغييرات السياسات	☐	_____
	السطو	☐	_____
	التغييرات/الصلة التكنولوجية	☐	_____
	_____	☐	_____
الجوانب المالية	مشكلات التدفقات النقدية/السيولة	☐	_____
	نضوب رأس المال	☐	_____
	المخالفات المالية	☐	_____
	الديون المعدومة	☐	_____
	مخاطر الفائدة	☐	_____
	خطر سعر الصرف	☐	_____
	مخاطر الخزانة	☐	_____
	_____	☐	_____
التكنولوجيا والبنية التحتية	فشل الشبكة - عالمي	☐	_____
	الكهرباء - حالات فشل الشبكة	☐	_____
	حالات فشل التيار المتردد	☐	_____
	حالات فشل مركز البيانات	☐	_____
	حالات فشل المكونات[3]	☐	_____
	_____	☐	_____
فشل التوريد	فشل مستوى الخدمة	☐	_____
	عيوب الجودة	☐	_____
	خسارة الخدمات المقدمة	☐	_____
	حالات فشل التوريد من الخارج/نفاد مخزون	☐	_____
	التعاقد على التوريد	☐	_____
	خسارة الأصول الأساسية الأخرى	☐	_____
	التقيد بمورّدين معينين	☐	_____
	_____	☐	_____

جدول 4

ليس هناك من سبب يدعو أي مشغل سجل إلى التركيز على التهديدات ذات الصلة لمنطقته/منطقتها وسياق الأعمال؛ فالقائمة غير الحصرية سالفة الذكر تعد مثالاً على ذلك. ومن الممكن أيضًا البدء بمجموعة من التهديدات/المخاطرات والتوسع فيها لاحقًا.

[3] حالات فشل المكونات عبارة عن مظلة جامعة تشير إلى قصور الأداء الوظيفي لأنظمة الكمبيوتر ووحدات تزويد الطاقة وذاكرة الكمبيوتر والأقراص إلخ... يمكن للمرء أن يقرر وضع هذه الأشياء في نطاق استمرارية الأعمال أو افتراض التخفيف من ذلك في تصميم وهندسة البنية التحتية بشكل افتراضي (أي وحدات تزويد الطاقة المكررة أو أنظمة أقراص RAID أو ذاكرة ECC في الخوادم، إلخ...).

الإجراء: قد ينبغي على منسق أو مدير استمرارية الأعمال التركيز على التهديدات و/أو المخاطر والتوسع من هناك في دورة المراجعة الاعتيادية.

تقييم وإدارة المخاطر

ما المقصود بالخطر؟ أنواع الخطر

الخطر، كما هو محدد في المعيار ISO 31000 عبارة عن: ""تأثير عدم اليقين على الأشياء" وهو تعريق عام للغاية ورفيع المستوى ومجرد. وعند ترجمة الخطر إلى استمرارية الأعمال والمرونة التشغيلية والاستمرارية، فإنه يكون "تأثير الحدث المسبب للتعطل على المهمة التشغيلية لمشغل سجل ccTLD".

فإذا ما اقتنع أحد بإجراء تقييم رسمي ومبسط في الوقت ذاته للمخاطر، فيمكنه استخدام القائمة التالية:

الخطر	الوصف
الجوانب المالية	الحدث يتسبب في تكبد المؤسسة لتكاليف مباشرة وغير مباشرة. اعتمادًا على الاستقرار المالي للمؤسسة، تكون هناك خسائر مالية مقبولة.
الجانب التشغيلي	يَحول الحدث دون تنفيذ المؤسسة لمهمتها التشغيلية (أي يحدث انقطاع لخدمات أسماء النطاقات).
على مستوى السمعة	قد يتسبب الحدث في ضرر على مستوى السمعة ويكون له تأثير مباشر أو غير مباشر على المهمة التشغيلية.
الجانب القانوني	يتسبب الحدث في تحديات قانونية قد تؤدي إلى عقوبات أو حتى إدانات جنائية.
الحوكمة	يتسبب الحدث في عواقب سياسات وعدم امتثال وهو ما قد يؤدي إلى إنهاء عقد امتياز أو تدخل سياسي.
الجانب الإنساني	يتسبب الحدث في ضرر مادي للموظفين (أو لأسرهم).

جدول 5

لكل خطر مستوياته المختلفة بشكل واضح ويمكن للمرء اعتمادًا على المستوى أن يقرر إدراجه ضمن خطط استمرارية الأعمال أم لا. بعض الأمثلة:

- قد تؤدي الخسارة المالية بقيمة مليون يورو إلى إفلاس حقيقي لمشغل السجل.
- وأي حدث يؤدي إلى إدانة جنائية للأفراد قد لا يكون مقبولاً بالنسبة لمشغل السجل.
- وأي حدث يتسبب في ضرر بدني للموظفين قبل لا يكون مقبولاً.

القائمة غير حصرية ويمكن لمشغل السجل ما يجب استخدامه في أي من المستويات. توضح القائمة التالية المستويات الخمسة للمخاطر حسب نوع الخطورة. ويعود إلى مشغل السجل مسألة تقرير مدى انطباق هذه المستويات والقيم الحقيقية.

النوع	بدون أو لا يوجد	منخفضة	متوسطة	عالية	خطير
الجوانب المالية	الخطر غير موجود أو غير منطبق	أقل من 1.000 دولار أمريكي	أقل من 10.000 دولار أمريكي	أقل من 100.000 دولار أمريكي	أكبر من 100.000 دولار أمريكي
الجانب التشغيلي		يؤثر على الفرد	يؤثر على الإدارة	يؤثر على السجل	يؤثر على الجمهور

على مستوى السمعة		على المستوى الداخلي	مجموعات المستخدمين (ICANN أو CENTR)	الجمهور	الوسائط / السياسية
الجانب القانوني		العقوبة الإدارية	غرامة أقل من 10.000 دولار أمريكي	غرامة أقل من 100.000 دولار أمريكي	غرامة أكبر من 100.000 دولار أمريكي، المسئولية الشخصية أو الإدارة الجنائية
الحوكمة[4]		مجلس الإدارة	الحكومة المحلية	التدقيق السياسي	إنهاء السجل
الجانب الإنساني		المستوى غير مستخدم	المستوى غير مستخدم	أسرة زملاء العمل	الإصابة الشخصية

جدول 6

من المستحسن تمييز المستويات المختلفة بالألوان حيث يمكن استخدام ذلك لاحقًا في إنشاء تمثيل بياني مرئي لجميع المخاطر المنطبقة في مقابل المخاطر المحققة.

تقييم بسيط للمخاطر / تقييم تأثير الأعمال التجارية

إن إضافة المخاطر المختلفة وفقًا لما هو مذكور أعلاه إلى مصفوفة التهديدات/المخاطرات يوفر أداة بسيطة في النظر إلى تأثير الأعمال.

ولنتناول مثالاً من أجل توضيح ذلك. السيناريو عبارة عن عمليات هجوم حجب الخدمة الموزعة DDoS على البنية الأساسية التشغيلية لنطاقات ccTLD (والتي تشمل على سبيل المثال لا الحصر خادم اسم النطاق لنطاق tld. بالإضافة إلى خدمات التسجيل؛ ونحن نفترض أن لمشغل السجل تأثير صغير من حيث البنية التحتية حيث تكون جميع الخدمات موحدة وعدم استخدام أي موفر لخدمات "التوجيه متعدد الاتجاهات - anycast" لنظام DNS).

فئة التهديد	**التهديد**	**منطبق (نعم/لا)**	**الاحتمالية**
الجانب الإلكتروني	هجوم حجب الخدمة الموزعة DDOS	نعم	مرجح بشكل كبير
المخاطر	**المستوى**		
الجوانب المالية	متوسطة	لا تتسبب هجمات حجب الخدمة الموزعة DDoS في أي تكاليف مباشرة حيث لا تتسبب في أي تدمير مادي للممتلكات. بل إن التكلفة الأكبر هي تعامل الناس مع الحادثة. وبالطبع هناك تكلفة غير مباشرة تحدث لعدم وجود أي أسماء نطاقات يتم تسجيلها أثناء التعرض للهجوم.	
الجانب التشغيلي	خطير	ولا يتوفر نطاق TLD. بالكامل أو أنه يتوفر على فترات متقطعة. ويكون لهذا تأثير تشغيلي كبير على الإنترنت. وبالمثل، تتأثر خدمات أخرى مثل موقع الشركة على الويب، وخدمة نظام WHOIS العامة وخدمات التسجيل الأخرى.	

[4] ربما تكون مخاطر الحوكمة الأكثر صعوبة وفي الوقت ذاته هي الأكثر تحديدًا من بين أنواع المخاطر. بالنسبة لبعض السجلات قد لا يكون الخطر موجود من الأساس. وهذا يستلزم من الإدارة إجراء وصف وتحديد واضحين لكيفية اعتماد السجل على التأثيرات الخارجية.

على مستوى السمعة	عالية/خطيرة	سوف يلاحظ الحادثة أي شخص على الإنترنت.
الجانب القانوني	عالية	وفي أعقاب الحادثة، قد يتقدم المسجلون وأمناء السجلات بشكاوى بسبب خسارة العوائد. (وهذا يعتمد على أحكام وشروط السجل بالإضافة إلى الاختصاص القضائي الخاص بالسجل).
الحوكمة	عالية	حيث إن غالبية نطاقات ccTLD يمكن اعتبارها شركات مختصة بتشغيل الخدمات الأساسية (وفقًا لوصف توجيه EU NIS)؛ من الآمن افتراض وجود بعض الاستعلامات من جهة الحكومة.
الجانب الإنساني	لا يوجد	لن يتأثر الموظفون بشكل مباشر أو غير مباشر
هدف وقت الاستعادة	بالنسبة لنظام DNS فإنه صفر؛ حيث ينبغي ألا تتعطل الخدمة أبدًا. وجميع الخدمات الأخرى التي تتأثر بهجمات DDoS يجب أن تكون متاحة في غضون يوم عمل واحد.	
هدف نقطة الاستعادة	إن تردي الخدمات إلى نسبة 50% من سعة خادم الاسم مقبولة؛ ويجب أن يكون من الممكن الوصول إلى جميع الخدمات الأخرى بالكامل، كما أن تردي السعة يكون مقبولاً حتى نسبة 50% كحد أقصى.	

جدول 7

ويحدد RTO أو هدف وقت الاستعادة السرعة التي ينبغي استعادة الخدمة وفقًا لها. وهذا يعكس توقع أصحاب المصلحة و/أو الالتزامات القانونية أو التعاقدية. لاحظ أن أهداف وقت الاستعادة المختلفة يمكن تعريفها لتهديد أو خطر واحد حيث يعتمد ذلك على الخدمات المتأثرة.

أما RPO أو هدف نقطة الاستعادة فيصف المستوى الذي يجب استعادة الخدمات عنده. وقد يتخذ ذلك العديد من الأشكال مثل انخفاض السعة (توافر أقل لخوادم الاسم على سبيل المثال؛ أو انخفاض سعة الخادم على سبيل المثال؛ إلخ)، تأخر الخدمات أو استعادة البيانات حتى نقطة محددة، إلخ...

ويجب أن يستند كل من فريق المراجعة وRPO تمامًا إلى مدخلات الأعمال وألا يعتمدا على "ما هو ممكن" عند وقوع الحوادث.

ويوفر هذا التقييم إشارة جيدة إلى أن التهديد يجب وضعه في الاعتبار وأنه يلزم إجراء معالجة للمخاطر.

الميل للمخاطر والمعالجة

ثمة 5 طرق تقريبًا للتعامل مع المخاطر:

1. قبول الخطر (عدم القيام بأي شيء).
2. تجنب الخطر (التوصل إلى خطة بديلة).
3. الحد من الخطر (تغيير المعادلة).
4. احتواء الخطر (التخفيف من التأثير).
5. تحويل الخطر (إعطائه لشخص آخر، التأمين).

تتعلق خطط استمرارية العمل بالكامل بالخيار 4، حيث يتم التصدي من خلال إجراءات محددة مسبقًا للتأثير وتتم استعادة المهمة التشغيلية إلى مستوى محدد مسبقًا.

كما يجب أخذ نتيجة تقييم تأثير الأعمال التجارية من الناحية الأخرى في الحسبان حيث قد يؤدي ذلك إلى خطوات أولية (الخطوة 3، تخفيف الخطر) وإجراءات من أجل تقليل مستوى الخطر والوصول إلى RTO وRPO.

لنعد مرة أخرى إلى المثال السابق ونتحرى عن ما يمكن القيام به من أجل الحد من الخطر إلى مستوى مقبول.

في هذه الحالة الخاصة، من الواضح أن نظام أسماء النطاقات لديه أولوية مطلقة، أما الخدمات العامة مثل موقع الشركة على الويب ووظيفة نظام WHOIS العامة فتأتي في المرتبة الثانية وأخيرًا وليس آخرًا خدمات التسجيل.

فئة التهديد	التهديد	منطبق (نعم/لا)	الاحتمالية
الجانب الإلكتروني	هجوم حجب الخدمة الموزعة DDOS	نعم	مرجح بشكل كبير
تخفيف المخاطر			
قبول الخطر	غير منطبق		
تجنب الخطر	مستحيل، يتم إطلاق هجمات حجب الخدمة الموزعة DDoS من خلال خصوم غير معروفين.		
الحد من الخطر	لن تكون للبنية التحتية الحالية القدرة على ضمان متطلبات RTO/RPO المتوقعة. من الحلول الممكنة استخدام حل "التوجيه متعدد الاتجاهات - anycast" لنظام نظام أسماء النطاقات و/أو خدمات الإجلاء للخدمات الأخرى.		
احتواء الخطر	وضع خطة لاستمرارية الأعمال من هجوم حجب الخدمة الموزعة DDoS (استخدام دليل الحد من هجوم حجب الخدمة الموزعة DDoS في منظمة دعم أسماء رموز البلدان مرجعًا) بما في ذلك التدابير الفنية الإضافية (مثل التغيير المؤقت لمقع بعض الخدمات) وخدمة الاتصالات وخطة للدعم		
نقل الخطر	غير منطبق		

جدول 8

سوف تحتوي خطة معالجة المخاطر بعد ذلك على إجراءات مختلفة يتم استخلاصها من القائمة السابقة. ويمكن تنفيذ البعض على الفور، وقد تتطلب غيرها ميزانية إضافية بالإضافة إلى موافقة وتخطيط آخرين.

خطة معالجة المخاطر

عند إجراء تقييم أولي للمخاطر/تقييم لتأثير الأعمال، سوف يؤدي عدد من السيناريوهات إلى مستويات غير مقبولة من الخطر أو إلى توقعات ومتطلبات من حيث RTO/RPO لا يمكن ضمانها في الوقت الحالي.

ويمكن سد هذه الفجوة من خلال إجراءات نوعية للحد من المخاطر. ويجب تسجيل هذه التدابير ووضعها في خطة، وهي ما يطلق عليه اسم خطة معالجة المخاطر. علمًا بأن خطة معالجة المخاطر ليست جزءًا من خطة استمرارية الأعمال، لكنها موجودة بشكلٍ متوازٍ. وهي تتألف من تحريات إضافية وإعادة هندسة الخدمات الحالية و/أو البنية التحتية والحصول على بعض الأنشطة من مصادر خارجية، إلخ...

خطة استمرارية الأعمال

قبل أن نتمكن من صياغة الخطة، قد تكون بعض المصطلحات بحاجة لتفسير. وفقًا لما ذكرنا من قبل، يمكن استخدام خطة استمرارية الأعمال في صورة دليل إرشادي وخطة إجرائية من أجل إدارة الأزمات عند وقوع أي أحداث مسببة للتعطل.

وعندما يكون المستوى مرتفع، يمكن دائمًا التعامل مع الأزمات بنفس الطريقة:

1. تقييم الموقف
2. احتواء الحدث
3. التعافي إلى المستويات المحددة مسبقًا ضمن RTO (هدف وقت الاستعادة) وRPO (هدف نقطة الاستعادة)
4. الاحتواء

لاحظ أن نهاية أي أزمة التي تأتي في أعقاب إلغاء الخدمة لا يعني ضمنًا أن المؤسسة قد عادت لحالة "ما قبل الحادثة". يقصد بلفظ "الاحتواء" أن فريق الأزمات يعتبر الأزمة تحت السيطرة، وأن الخدمة تمت استعادتها، وأن بإمكان المؤسسة تنفيذ مهمتها التشغيلية. ولا يشير ذلك ضمنًا إلى أن جميع الأضرار تم إصلاحها.

ويمكننا استخدام مثال لمزيد من التوضيح والبيان: خلال العطلة الأسبوعية، قام المخربون بتدمير ونهب المقر الرئيسي للسجل. وتمت سرقة معدات تقنية المعلومات وتم تدمير الأثاث، ولا يمكن للمؤسسة بشكل أساسي العمل من المقر بسبب الأضرار، كما أن التحقيقات جارية. يتم تنشيط خطة استمرارية الأعمال وتفيد الخطة بأنه عندما لا يكون من الممكن الوصول إلى المقر، يتم إعادة توجيه الهواتف إلى الخدمات المحمولة، ويتم إبلاغ الموظفين بالمكوث في بيوتهم والعمل من المنزل حتى إشعار آخر (وهذا ينطوي على أن العمل عن بعد ليست به مشكلة). يتناول فريق الأزمات الاتصال الأولي بجهات إنفاذ القانون والتأمينات وغيرها من الجهات ويتأكد من تنفيذ خطة استمرارية العمل سالفة الذكر. وبمجرد الانتهاء من ذلك، سوف تتم استعادة الخدمة إلى مستوى مقبول ويمكن للمؤسسة مواصلة مهمتها التشغيلية. ويقوم فريق الأزمات بتخصيص الموارد للتعامل أكثر مع الحالة ويعيد المقر إلى حالته السابقة. وفي ذلك الوقت يحتوي فريق الأزمات المشكلة ويستأنف دوره التشغيلي الطبيعي. وبشكل واضح، سوف يكون في المؤسسات الصغيرة تداخل بسبب توافر الموارد المحدودة في العادة.

المواد الحيوية عبارة عن مجموعة من المعلومات (رقمية و/أو مادية) لازمة بشكل مطلق من أجل إدارة الحادثة. ويمكن أن تكون هذه المعلومات عقود أو معلومات جهات اتصال لخدمات نوعية (على سبيل المثال؛ موفري الخدمات، وخدمات الإجلاء والتصفية والمالك والهيئات، إلخ....) وعمليات تسجيل الدخول وكلمات المرور، والأصول المادية مثل المفاتيح، إلخ... ولا تنس توفير الحماية الملائمة لهذه المواد الحساسة مع الحفاظ في الوقت ذاته على إمكانية الوصول إليها خلال الأزمات.

خطة استمرارية الأعمال: بمجرد تحديد السيناريوهات ذات المخاطر الأعلى، يحين وقت صياغة الخطط. ويمكن لأي أحد أن يقرر كتابة وتدوين خطة تفصيلية تحتوي على كل خطوة فردية للتنفيذ خلال أي كارثة. وفي حين أن هذا الأمر ممكن تمامًا، تنحو الكوارث إلى التسبب في أحداث جانبية غير متوقعة وهو ما يجعل من الصعب تدوين كل خطوة فردية يجب القيام بها. فمن واقع الخبرة، من المفيد استخدام إرشادات إجمالية تعيد تكرار الخطوات الأساسية خلال التعامل مع الأزمات. ويمكن استخدام تلك الخطة بعد ذلك خلال التدريب والاختبار والمحاكاة.

كما يجب على المرء أن ينظر في تأثير وأثر السيناريو. ومن غير المعقول تدوين العديد من خطط استمرارية الأعمال قد يكون لها في نهاية المطاف سيناريوهات مختلفة، لكنها تؤدي إلى نفس الخطة. من الأمثلة النموذجية على ذلك الحوادث التي تجعل مقر العمل غير متاح/لا يمكن الوصول إليه. ومهما كان السبب (حريق أو إضراب أو انقطاع الكهرباء أو فيضان أو جمعة سوداء) ولم يكن ذا صلة حقيقية، فإن النتيجة واحدة. ويمكن ترجمة ذلك بعدها إلى خطة واحدة لاستمرارية الأعمال.

القالب التالي مختصر كما أنه يكرر جميع الخطوات سالفة النقاش من أجل التعامل مع الكوارث. كما أنها تساعد في تحديد بعد المهام التحضيرية. **لاحظ أن الارتجال أثناء الكوارث هو أسوأ النتائج المحتملة.** وهذا القالب في نهاية المطاف ليس إلا ملاحظات مختصرة لمساعدة فريق الكوارث في التعامل مع الموقف وأن يكون على استعداد.

خطة استمرارية الأعمال (القالب)			
المرجع:	[المرجع]	نوع التهديد	تأثر الأصول
السيناريو:	يصف الظروف التي أدت إلى إطلاق الخطة. ويمكن أن يكون ذلك حدثًا أو وقتًا أو ظرفًا خاصًا، إلخ...		
التنشيط:	متى يتم تنشيط الخطة؟ يمكن أن يكون ذلك أثناء التحريات أو بعد وقوع الحادثة بعدة ساعات.		
RTO:	هدف وقت الاستعادة		
RPO:	هدف نقطة الاستعادة		
فريق الأزمات:	من هو فريق الأزمات؟ من الذي يتعامل فعليًا مع الحادثة؟ استخدم أسماء الموظفين والشركات والمورّدين من أجل إزالة الغموض.		
الأولويات:	ما هي الأولويات؟ يجب ترجمة ذلك إلى قائمة متتابعة.		
التقييم:	المرحلة الأولى في التعامل مع أي حادثة مسببة للتعطل تكون بتقييم مدى ونطاق الحادثة. صِف العوامل التي يجب وضعها في الاعتبار.		
الاحتواء:	صِف المسار الإجرائي الذي يجب اتباعه من أجل منع ازدياد الموقف سوءًا.		
التعافي:	صِف المسار الإجرائي الذي يجب اتباعه من أجل استعادة الحد الأدنى من الجاهزية التشغيلية، مع الأخذ في الاعتبار الأولويات سالفة الذكر.		
الاحتواء:	وبمجرد استعادة العمليات مرة أخرى، يترك فريق الأزمات الأمر ويترك تعليمات من أجل مزيد من الإجراءات للعودة إلى حالة ما قبل الحادثة.		
التواصل:	حدد المراسلات الداخلية والخارجية، والتي تشمل الرسائل بالإضافة إلى قائمة التوزيع وأيضًا الوسائل اللازمة لذلك. ابدأ دائمًا بالمراسلات الداخلية.		

المواد الحيوية:	قائمة المصادر اللازمة من أجل التعامل مع الحادثة. وهو جزء من مرحلة التحضير. لا تحتوي الخطة على محتوى فعلي، لكنها مقتصرة على مراجع (ويتحمل قادة و/أو شركاء الإدارات المختلفة المسئولية عن الحفاظ على هذا المحتوى، وتحديثه ودقته والقدرة على نقله متى أمكن)
السجلات:	ما السجلات التي يجب تقديمها خلال الأزمة وبعدها. تفيد هذه السجلات من أجل جمع الأدلة والدروس المستفادة وتعقب الحوادث الفعلية.

جدول 9

وثمة بعض الأمثلة على خطط استمرارية العمل في الملحق.

الدعم

المصادر

قد كون الجهد الأولي المبذول في إعداد نظام (إدارة) استمرارية الأعمال مستهلكاً للوقت إلى حد ما، إلا أن الطريقة السابقة يجب أن تجعل هذا الأمر عمليًا وقابلاً للتطبيق بالنسبة للمؤسسات الصغيرة.

وبمجرد صياغة عمليات الجرد والقوائم، يصبح الجهد أكثر استدامة حيث إن هناك حاجة لإجراء مراجعات كل سنة فقط من أجل تحديث الخطط مع الأخذ في الاعتبار المشهد المتغير للتهديدات والمخاطر، على سبيل المثال؛ كانت غالبية عمليات الهجوم الإلكتروني في عالم الخيال العلمي في بداية القرن الحادي والعشرين؛ أما اليوم يجب النظر إليها على اعتبار أنها مخاطر واضحة وحاضرة.

أما في المنظمات الصغيرة، فإن أفضل مكان لإدارة وإرشاد التطوير الناجح لخطط استمرارية الأعمال فهو في مستوى الإدارة ويجب إعطاء المشروع ما يكفي من دعم وتركيز.

وليس ثمة حاجة فعلية لتعيين مدير مخصص لاستمرارية الأعمال، ففي بعض الحالات قد تكون استراتيجية استمرارية الأعمال أكثر فاعلية عند تضمين ذلك في مسئوليات المنظمة بالكامل.

الوعي

تتطلب استراتيجية استمرارية الأعمال الناجحة وعيًا في جميع قطاعات المؤسسة بالكامل بالإضافة إلى إدراك أنها يجب أن تكون محور اهتمام الجميع.

ومن ثم فإن جلسات الوعي الاعتيادية ضرورة مطلقة.

المراسلات

وفقًا لما يوضحه النموذج ومثال خطط استمرارية الأعمال، تلعب المراسلات (الداخلية والخارجية) دورًا هامًا للغاية في إدارة الأزمات.

ومن ثم من الضروري للغاية:

1. تحديد وسائل الاتصالات التي يجب استخدامها. مثال: الهاتف والرسائل النصية والرسائل العادية وتويتر والبريد الإلكتروني، إلخ...
2. إعداد قوالب الاتصالات (يمكن أن تؤدي المرسلات الارتجالية إلى نسف مصداقية أي مؤسسة خلال أي أزمة).
3. التحديد المسبق والتحضير لمن سيتم إرسال المراسلات له، على سبيل المثال؛ "أمناء السجلات التابعين لنا" ليس تعريفًا قابلاً للإجراء. بل الإشارة إلى قائمة عناوين البريد الإلكتروني التي يتم الحفاظ على تحديثها هي التعريف القابل للإجراء.

4. إعداد الأولويات والجداول من أجل المراسلات (على سبيل المثال؛ التغريد بتحديث كل 60 دقيقة، وإرسال بريد إلكتروني في بداية ونهاية الحادثة).
5. تقييم الحاجة للاستعانة باستشاري مراسلات خارجي للأزمات من أجل المساعدة في إعداد استراتيجية وخطط المراسلات، ولكن أيضًا لتدريب الأشخاص المتعاملين مع الصحافة.

التشغيل

بمجرد صياغة خطة استمرارية العمل؛ يجب تضمينها في الأعمال اليومية والعمليات الاسمية. وهذا يعني أن استمرارية الأعمال يجب أن تلعب دورًا في جميع الأعمال الهندسية والتجارية وتدفقات العمليات.

وهذا ينطوي على أن استمرارية الأعمال تلعب دورًا في مختلف النواحي مثل: المشتريات والقطاع القانوني والهندسي والعمليات والاتصالات.

بعض الأمثلة لتوضيح ذلك:

- يتم شراء بعض الخوادم ومعدات الشبكات. طلب تقديم العروض (RFP) الذي يتم إرساله إلى المورّدين يشير إلى **زيادة توريدات الطاقة** وأيضًا **بطاقات واجهة الشبكة** الثنائية من أجل أقصى وفرة وتكرار.
- يتم الحصول على خدمة من **مصدر خارجي**، يشير طلب تقديم العروض صراحة إلى هو متوقع من تدابير لاستمرارية الأعمال المتوقعة من موفر الخدمة.

ممارسات استمرارية الأعمال

لا بأس بوضع خطط من أجل التماهي مع سيناريو خاص للكوارث، ولكن بدون أي اختبار أو تدريب، وتظل الخطة حبرًا على ورق.

ولذلك فإن اختبار وتجربة خطط استمرارية الأعمال من المكونات الأساسية في أي استراتيجية فعالة لاستمرارية الأعمال. تمامًا مثل رجال الإطفاء فهم يتدربون على إطفاء الحرائق؛ ويجب على فريق الأزمات تمضية بعض الوقت في إجراء الاختبارات والتجارب الفعلية على الخطط.

وثمة طريقتان للقيام بذلك. هناك ما يطلق عليه اسم تمرين المحاكاة أو TTX والمحاكاة الفعلية المنضبطة.

تمرينات المحاكاة (TTX)

هذه الممارسات "الصورية أو الورقية" تهدف إلى مراجعة الإجراءات وهي مفيدة للغاية من أجل تدريب فرق العمل. وهي تستلزم القليل من الاستعداد النسبي.

ويمكن أن تكون تمرينات المحاكاة من الممارسات التي تلعب دورًا هامًا حيث تجلس جميع الأطراف المعنية حول الطاولة ويؤدي كلٌ دوره. **وسوف ترشد وثيقة "رئيس التشريفات"** فريق العمل عبر خطوات السيناريو المختلفة، والتي تتداخل مع الأحداث الإضافية العرضية غير المتوقعة.

ومن العيوب الرئيسية في تمرينات المحاكاة صعوبة إيصال معنى العجلة والإلحاح والواقعية للمشاركين.

الإجراء: من الضروري أن تستعرض المنظمة بالكامل خطط استمرارية الأعمال مرة واحدة سنويًا على الأقل مع إلقاء نظرة ناقدة على مدى الجدوى. إن خطط استمرارية الأعمال عبارة عن مستندات حية سوف تكون بحاجة لمواءمتها مع أي بيئة متغيرة.

عمليات المحاكاة

يتم في العادة اختبار خطط استمرارية العمل في ضوء عمليات المحاكاة في الحياة الواقعية. وخلال عمليات المحاكاة المشار إليها، فإن استجابة فرق العمل أو الشركاء المختلفين يتم فحصها من أجل توثيق فاعلية فرق العمل بالإضافة إلى جدوى الخطط.

ومن خلال تجربة واختبار الخطط المختلفة، سوف تعتاد فرق العمل على ما يتوجب عليها القيام به عندما تقع الأحداث فعليًا.

وبشكل واضح، ليس من السهل دائمًا إجراء محاكاة فعلية للحوادث (على سبيل المثال؛ انقطاع الكهرباء في مركز البيانات)؛ ولكن يمكن اقتراح سيناريوهات واقعية.

بعض الأمثلة:

- اندلاع فيروسات الفدية. يقوم المستخدم بالاتصال بمكتب الدعم من أجل السؤال عن ما يجب القيام به حيث تدعي الشاشة بأن الكمبيوتر المحمول تم الاستحواذ عليه مع طلب الحصول على بعض عملات البيتكوين في مقابل إلغاء قفل الكمبيوتر. ويتمثل الغرض من هذا التمرين في اختبار استجابة فريق الدعم.
- لا يمكن الوصول إلى مقر الأعمال بسبب تفشي الجرزان. من الواضح عدم وجود أي جرزان، لكن الغرض يتمثل في اختبار مستوى التواصل مع الموظفين.

التحسين

من الضروري بالنسبة لأي استراتيجية فعالة لاستمرارية الأعمال مراجعة الخطط وتقييم المخاطر وسرد أصحاب المصلحة وسرد التهديدات والمخاطر إلخ... على الأقل مرة سنويًا أو في حالة حدوث تغييرات كبيرة.

ويتم البدء في هذه التغييرات بشكل نموذجي من خلال عدد من الإجراءات:

- التشريعات الناشئة
- الحصول على الموارد الخارجية
- عمليات الدمج والاستحواذ
- الخدمات الجديدة
- تغييرات أصحاب المصلحة
- التقنيات الناشئة
- تغير المشهد العام للتهديدات
- حادثة
- ...

الملحق: موجز المهام

يمثل هذا الملحق تلخيصًا لمختلف المهام المذكورة في الوثيقة. ويمكن استخدام ذلك في صورة قائمة فحص للمساعدة في التنفيذ.

1. عمل جرد لجميع **أصحاب المصلحة** وتوقعاتهم، وتحديد التوقعات ذات الصلة باستمرارية الأعمال (الجدول 1)
2. عمل جرد لجميع **المورّدين**، ووصف ما يقومون بتوريده وتحديد الصلة باستمرارية الأعمال والتأثير (الجدول 3)
3. استخدام الجدول 4 من أجل إنشاء **سجل بالتهديدات والمخاطر**، وتمييز ما ينطبق منها وماهية الاحتمالية
4. استخدام الجدول 5 من أجل تحديد **المخاطر** التي تنطبق على المؤسسة؛ واستخدام الجدول 6 من أجل تحديد المستويات المختلفة حسب كل خطر
5. تناول سجل التهديدات والمخاطر (الجدول 4) ونسخ التهديدات والمخاطر المنطبقة في **تقييم تأثيرات الأعمال** (الجدول 7). ويمكننا تلخيص هذه الجداول في تمثيل بياني حيث يتم تمييز مستويات المخاطر بألوان مميزة وفقًا لما هو موضح في المثال أدناه:

فئة التهديد	التهديد	الجوانب المالية	الجانب التشغيلي	على مستوى السمعة	الجانب القانوني	الحوكمة	الجانب الإنساني
الجانب الإلكتروني	هجوم حجب الخدمة الموزعة DDOS	متوسطة	خطير	عالية/ خطير	عالية	عالية	لا يوجد

6. قم بتوسيع الجدول 7 الذي تم استخدامه لتقييم تأثير الأعمال البسيط وأضف **معالجة المخاطر** إليه (الجدول 8). سوف يكون هناك عدد من التهديدات التي يتأتى عنها خطر غير مقبول ما لم يتم الحد منه؛ ومن ثم ينجم عن معالجة الخطر خطة لمعالجة الخطر تحتوي على إجراءات لتقليل المخاطر. ولا يشير ذلك ضمنًا إلى أن المخاطر تتم السيطرة عليها بعد ذلك، بل يشير إلى أن المخاطر يتم التخفيف منها.
7. قم بإنشاء **خطط استمرارية العمل** مستخدمًا الجدول 9 لتكون بمثابة قالب ونموذج لتلك التهديدات والمخاطر التي تعتبر تهديدًا حقيقيًا وذات تأثير كبير على المؤسسة.

الملحق: نموذج لخطة استمرارية الأعمال

خطة استمرارية الأعمال (القالب)			
المرجع:	[المرجع]	نوع التهديد	تأثر الأصول
السيناريو:	يصف الظروف التي أدت إلى إطلاق الخطة. ويمكن أن يكون ذلك حدثًا أو وقتًا أو ظرفًا خاصًا، إلخ...		
التنشيط:	متى يتم تنشيط الخطة؟ يمكن أن يكون ذلك أثناء التحريات أو بعد وقوع الحادثة بعدة ساعات.		
RTO:	هدف وقت الاستعادة		
RPO:	هدف نقطة الاستعادة		
فريق الأزمات:	من هو فريق الأزمات؟ من الذي يتعامل فعليًا مع الحادثة؟ استخدم أسماء الموظفين والشركات والمورّدين من أجل إزالة الغموض.		
الأولويات:	ما هي الأولويات؟ يجب ترجمة ذلك إلى قائمة متتابعة.		
التقييم:	المرحلة الأولى في التعامل مع أي حادثة مسببة للتعطل تكون بتقييم مدى ونطاق الحادثة. صِف العوامل التي يجب وضعها في الاعتبار.		
الاحتواء:	صِف المسار الإجرائي الذي يجب اتباعه من أجل منع ازدياد الموقف سوءًا.		
التعافي:	صِف المسار الإجرائي الذي يجب اتباعه من أجل استعادة الحد الأدنى من الجاهزية التشغيلية، مع الأخذ في الاعتبار الأولويات سالفة الذكر.		

الاحتواء:	وبمجرد استعادة العمليات مرة أخرى، يترك فريق الأزمات الأمر ويترك تعليمات من أجل مزيد من الإجراءات للعودة إلى حالة ما قبل الحادثة.
التواصل:	حدد المراسلات الداخلية والخارجية، والتي تشمل الرسائل بالإضافة إلى قائمة التوزيع وأيضًا الوسائل اللازمة لذلك. ابدأ دائمًا بالمراسلات الداخلية.
المواد الحيوية:	قائمة المصادر اللازمة من أجل التعامل مع الحادثة. وهو جزء من مرحلة التحضير. لا تحتوي الخطة على محتوى فعلي، لكنها مقتصرة على مراجع (ويتحمل قادة و/أو شركاء الإدارات المختلفة المسئولية عن الحفاظ على هذا المحتوى، وتحديثه ودقته والقدرة على نقله متى أمكن)
السجلات:	ما السجلات التي يجب تقديمها خلال الأزمة وبعدها. تفيد هذه السجلات من أجل جمع الأدلة والدروس المستفادة وتعقب الحوادث الفعلية.

الجانب الإلكتروني: السطو

خطة استمرارية الأعمال			
المرجع:	BCP-xxx.yy	الجانب الإلكتروني: السطو	عالمي
السيناريو:	توضح الأدلة أن البنية التحتية للسجل تم السطو عليها والعبث بها. قامت جهة غريبة بتثبيت برامج، وقامت بإنشاء حسابات وأدوات للوصول عن بعد، إلخ... من أجل التسلل إلى السجل. تم استخراج بيانات ربما تكون (حساسة). .		
التنشيط:	قيد التقصي فورًا		
RTO:	24 ساعة		
RPO:	فقد البيانات لمدة 24 ساعة.		
فريق الأزمات:	المدير القانوني. - ivan.horvat@registry.tld - +CC 123 55 88 . المدير الفني – juan.perez@registry.tld – +CC 123 44 55 مدير استمرارية الأعمال – jane.doe@registry.tld – +CC 123 33 66 . المدير العام - yamado.toro@registry.tld - +CC 123 56 44		
الأولويات:	حماية توافر وتكامل خوادم الاسم ومنطقة tld. عزل البنية التحتية لخادم الاسم إذا لزم الأمر. عزل النظم التي تم السطو عليها. جمع الأدلة.		
التقييم:	في حالة العثور على دليل بأن البيانات قد تسربت، القيام أيضًا بتنشيط خطة استمرارية العمل لانتهاك البيانات. إجراء تقييم وجرد للنظم التي تم اختراقها. ما الخدمات التي تأثرت؟ هل تأثر نظام DNS، أو منصة التسجيل أو النظم الداخلية أو موقع الويب؟ تحقق من البنية التحتية لخادم الاسم. هل للمهاجم الغلبة الدائمة؟ هل المهاجم حاضر في وقت التحري والتقصي؟ هل يلزم الحصول على مساعدة خارجية من الشركات المتخصصة في حوادث السطو الإلكتروني (هل ثمة دليل على وجود متورطين حكوميين)؟		

الاحتواء:	التأكد من أن البنية التحتية لخادم الاسم مصانة مع عزل خوادم الاسم عن المنطقة المتضررة. تعطيل أو إيقاف تشغيل النظم المتأثرة. لا تحاول إصلاح أو ضبط الأنظمة المتضررة أو محاربة المتطفل. يجب التركيز على عزل النظم المتضررة. حاول جمع الأدلة؛ ولا تعبث بالأدلة.
التعافي:	يجب إعادة بناء الأنظمة الأنظمة المتضررة وإعادة نشرها. في حالة تعرض معدات المستخدم النهائي للضرر، يتم نشر أنظمة جديدة.
الاحتواء:	بمجرد عزل الأنظمة المتضررة وإيقاف تشغيلها واستعادة الخدمات من خلال استخدام الأنظمة المعاد تشغيلها ونشرها؛ يقوم فريق الأزمات بتعيين فريق من أجل التعامل مع الأنشطة التالية: 1. الاتصال بجهات إنفاذ القانون وتقديم شكوى. 2. التأكد من تخزين الأنظمة المتضررة بشكل آمن وتجنب ملفات السجلات كأدلة. تحليل تكامل ونزاهة قاعدة البيانات الجوهرية (هل ثمة أدلة على وجود تغييرات؟).
التواصل:	الاتصال الداخلي فقط الاتصال الأولي بجميع أنظمتنا التي تعرضت للاختراق وأننا نقوم بعزل الأنظمة المخترقة. التأكيد على أن المزيد من الاتصالات بالعالم الخارجي سوف يتم التعامل معها من خلال مدير الاتصالات والمدير القانوني مباشرة. الاتصالات الخارجية: إبلاغ أصحاب المصلحة (مجلس الإدارة والجهات المعنية) إبلاغ أمناء السجلات في حالة تعطيل الأنظمة (أي موقع الويب أو خدمة whois أو بروتوكول التزويد المرن) وإبلاغهم بالخطوات الإضافية التي يتم اتخاذها. إبلاغ جهات إنفاذ القانون.
المواد الحيوية:	توثيق البنية التحتية والإعدادات. مخازن كلمات المرور للوصول إلى مختلف الأنظمة. نشر البنية التحتية والتخطيط لها من أجل نشر بنية تحتية جديدة. قوائم التوزيع من أجل الاتصالات (أمناء السجلات والموظفين)
السجلات:	إنشاء سجل بالأحداث، وما تم اكتشافه، وما الإجراءات التي تم القيام بها، وما الأدلة التي تم جمعها. قم بذلك خلال التعامل مع الأزمات وليس في مرحلة لاحقة.

خارجي: الهجوم الإرهابي

خطة استمرارية الأعمال			
المرجع:	BCP-xxx.yy	خارجي: الهجوم الإرهابي	مقر العمل
السيناريو:	وقع هجوم إرهابي بالقرب من مقر(مقار) الشركة الخاص بالسجل. وتعني كلمة "بالقرب من" إما في نفس المدينة أو ضمن محيط 25 كيلومتر. وتنطبق هذه الخطة على مدار الساعة.		
التنشيط:	على الفور		
RTO:	غير محددة		
RPO:	غير محددة		
فريق الأزمات:	مسئول المقر - +CC 123 44 55 - jan.modaal@registry.tld مدير الموارد البشرية - +CC 123 66 23 - maija.meikalainen@registry.tld مدير استمرارية الأعمال – +CC 123 33 66 – jane.doe@registry.tld . المدير العام - +CC 123 56 44 - yamado.toro@registry.tld		
الأولويات:	سلامة الموظفين.		
التقييم:	اعتمادًا على مدى خطورة الهجوم، فإن العواقب قد تكون صعبة الحل (تعطيل المواصلات العامة، نشر فرق التدخل السريع، إلخ...). بادئ ذي بدء، يجب أن يكون الموظفين وذويهم في أمان. بما أن السجل يدعم العمل من المنزل، يجب على زملاء العمل عدم المكوث في مقر العمل أو المجيء إليه.		
الاحتواء:	يتم إغلاق المقر على الفور، إذا سمح الموقف بذلك ويتم إرسال الموظفين إلى منازلهم. إذا كان الهجوم قريب للغاية من المقر، يتم توجيه الموظفين إلى التزام أماكنهم واتباع إرشادات جهات إنفاذ القانون والمصادر الحكومية.		
التعافي:	يقوم مسئول المقر بالتأكد من أن جميع الموظفين على اطلاع وأنه تم احتسابهم. ويلتزم بإشعار جميع الموظفين بأن المقر قد أغلق ولا يسمح بالدخول إليه حتى إشعار آخر. يلتزم مسئول مقر العمل بإبلاغ مدير الموارد البشرية أو مدير استمرارية الأعمال بالموقف. ويلتزم مدير الموارد البشرية أو مدير استمرارية الأعمال بإبلاغ الإدارات والمديرين المعنيين بمزاولة الأنشطة متى ما كان ذلك منطبقًا.		

الاحتواء:	يتبع مسئول مقر العمل الإرشادات المقدمة من جهات إنفاذ القانون والمصادر الرسمية ويقوم بإشعار الموظفين عند إعادة فتح مقر العمل.
التواصل:	الاتصال الداخلي فقط التواصل الأولي شفهيًا أو من خلال الرسائل النصية (SMS) عن طريق مسئول مقر العمل للموظفين المتضررين. اتباع المراسلات عن طريق البريد الإلكتروني من خلال مسئول مقر العمل أو الموارد البشرية أو مدير استمرارية الأعمال.
المواد الحيوية:	قائمة بالموظفين مع أرقام الهواتف وعناوين البريد الإلكتروني.
السجلات:	سجل للموظفين بأن جميع زملاء العمل قد تم إشعارهم واحتسابهم.

الجانب الإلكتروني: فيروسات الفدية

خطة استمرارية الأعمال			
المرجع:	BCP-xxx.yy	الجانب الإلكتروني: فيروسات الفدية	مقر العمل ومعدات المستخدم النهائي
السيناريو:	أدت الإصابة بفيروسات الفدية إلى تعطيل عدد محدود من أجهزة الكمبيوتر المحمولة التي تعمل بنظام مايكروسوفت ويندوز وقفلها. وكانت الإصابة متركزة في مقر واحد للعمل أو أنها تنتشر في جميع قطاعات المؤسسة.		
التنشيط:	قيد التقصي فورًا		
RTO:	في غضون يوم عمل واحد.		
RPO:	فقد البيانات لمدة يوم عمل واحد.		
فريق الأزمات:	. المدير الفني – +CC 123 44 55 – juan.perez@registry.tld مدير استمرارية الأعمال – +CC 123 33 66– jane.doe@registry.tld . المدير العام - +CC 123 56 44 - yamado.toro@registry.tld		
الأولويات:	حماية توافر وتكامل البنية التحتية لخادم ويندوز. عزل النظم المتضررة. إعادة ترتيب النظم المتضررة.		
التقييم:	هل الإصابة آخذة في الانتشار؟ من هو/كان أول المصابين؟ هل يمكننا عزل الإصابة؟		
الاحتواء:	عزل الأجهزة المصابة (أي إغلاق روابط الشبكة المؤدية إلى مركز البيانات). إغلاق الأجهزة غير المتضررة سواء البعيدة أو مطالبة المستخدمين -إذا بدا الحل الأول مستحيلاً- بإغلاق الأجهزة الخاصة بهم.		
التعافي:	يجب اعتبار الأنظمة المتضررة وكأنها مفقودة ويجب إعادة تثبيتها. ربما يصبح بعض الموظفين غير متصلين بالشبكة لبضعة أيام.		

الاحتواء:	يقوم فريق الأزمات بتعيين فريق من أجل: 1. تحديد وتعريف فيروسات الفدية والتحقق من التوقيعات أو طرق الكشف الأخرى. 2. تحديد السلسلة الأولية... كيف تمت إصابة أول المتضررين؟ 3. إنشاء بيئات شبكات معزولة (سلكية ولاسلكية) في المكان الذي وقعت فيه الإصابة؛ يجب بدء تشغيل الأنظمة غير المتضررة والتحقق مما إن كانت غير مصابة ببرامج ضارة. 4. وضع خطة لإعادة تثبيت أجهزة الكمبيوتر المحمولة التي تمت إصابتها. بالنسبة للمقار البعيدة، قد يكون هذا الأمر مشكلة وربما يتعين إرسال مهندس ميداني. 5. تقديم شكوى رسمية لدى جهات إنفاذ القانون و/أو الجهات الأخرى استنادًا إلى الالتزامات/التوصيات القانونية.
التواصل:	<u>الاتصال الداخلي فقط</u> إبلاغ جميع الموظفين بتفشي فيروسات الفدية وتوجيههم إلى إغلاق أجهزة الكمبيوتر المحمول (بنظام ويندوز) الخاصة بهم على الفور (واستخدام البريد الإلكتروني والهاتف والرسائل).
المواد الحيوية:	توثيق البنية التحتية والإعدادات. مخازن كلمات المرور للوصول إلى مختلف الأنظمة. قوائم التوزيع من أجل الاتصالات (الموظفين).
السجلات:	إنشاء سجل بالأحداث، وما تم اكتشافه، وما الإجراءات التي تم القيام بها، وما الأدلة التي تم جمعها. قم بذلك خلال التعامل مع الأزمات **وليس** في مرحلة لاحقة.

الملحق: ورشة العمل

الإطار الزمني لورشة العمل

	الوصف	التوقيت بالحد الأدنى	من
1	طرح الدليل العملي - توزيع وثيقة خطة DR/BCP	45	
2	الأسئلة والأجوبة في الدليل العملي	15	
3	تعبئة النماذج - BIA - BCP - استنادًا إلى نطاق ccTLD الخاص بك - توزيع نموذج DR/BCP	45	
4	مناقشة نتيجة النموذج	30	
5	إعداد فرق العمل (بحد أقصى 5 فرق) - توزيع البطاقات، السجل OK وخطة استمرارية العمل في حالة الهجوم الإلكتروني	5	
6	التعرف على البطاقات	10	
7	5 جولات من ممارسات المحاكاة الفعلية (TTX)	60	
8	استخلاص معلومات التدريب	30	

(240 دقيقة)

ممارسة طرح وتعبئة النماذج

إجراء طرح وتعريف لمدة 45 دقيقة + 15 دقيقة للأسئلة والأجوبة حول الوثيقة لتسليط الضوء على الموضوعات الرئيسية.

وخلال مدة 45 دقيقة نتيح للمشاركين ما يلي

1. إعداد قائمة بأصحاب المصلحة ونقوم بتدوين التوقعات
2. مراجعة سجل التهديدات - أيهما يمكن تطبيقه؟
3. ما المخاطر الهامة بالنسبة للمؤسسة وتحديد المستويات.
4. اختيار تهديد وإجراء تقييم لتأثير الأعمال (BIA) عليه.
5. واستنادًا إلى ذلك التهديد، يجب تحديد خطة استمرارية العمل (BCP)؛ وسرد عناصر المواد الحيوية

قائمة أصحاب المصلحة

أصحاب المصلحة في هذه القائمة مجرد أمثلة فقط. لا تتردد في إضافة أصحاب المصلحة الذين لم يتم ذكرهم وترى أنهم ذوي صلة.
الصلة باستمرارية الأعمال: عالية، متوسطة، منخفضة، بدون

المساهم أو صاحب المصلحة	التوقعات	الصلة باستمرارية الأعمال
الحكومة		
ICANN		
مجلس الإدارة		
عامة الناس		
جهات إنفاذ القانون		
أمناء السجلات		
المشتركون		

سجل التهديدات

تحقق من التهديدات المنطبقة وما هي الاحتمالية استنادًا إلى المعلومات الإحصائية.

فئة التهديد	التهديد	منطبق (نعم/لا)	الاحتمالية
الكوارث الطبيعية	الحريق الفيضان الإعصار/الزوبعة/العاصفة الطقس المناوئ الزلزال الانزلاق الأرضي/الانهيار الجليدي النشاط البركاني تسونامي ضربات البرق الهبوط الأرضي التلوث انتشار الحشرات القوارض _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____
الموارد البشرية والجانب الطبي	خسارة فريق العمل الرئيسي المرض الوبائي نقص المهارات/العاملين المسائل الأسرية السطو التلف الضار (التخريب) الابتزاز _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____
الجانب الإلكتروني	هجوم حجب الخدمة الموزعة DDOS القراصنة فقد البيانات فيروسات الفدية الأنشطة ذات الصلة بالحرب الإلكترونية _____	☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____
خارجي	الكساد العصيان المدني النشاط الإرهابي الحرب/الغزو التدخل السياسي/تغييرات السياسات السطو التغييرات/الصلة التكنولوجية _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____
الجوانب المالية	مشكلات التدفقات النقدية/السيولة نضوب رأس المال المخالفات المالية الديون المعدومة مخاطر الفائدة	☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____

	خطر سعر الصرف مخاطر الخزانة _____	☐ ☐ ☐	_____ _____ _____
التكنولوجيا والبنية التحتية	فشل الشبكة - عالمي الكهرباء - حالات فشل الشبكة حالات فشل التيار المتردد حالات فشل مركز البيانات حالات فشل المكونات[5] _____	☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____
فشل التوريد	فشل مستوى الخدمة عيوب الجودة خسارة الخدمات المقدمة حالات فشل التوريد من الخارج/نفاد مخزون التعاقد على التوريد خسارة الأصول الأساسية الأخرى التقيد بمورّدين معينين _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____

الاحتمالية:

1. احتمالية كبيرة: حدث يقع سنويًا أو بوتيرة أكبر
2. محتمل: حدث يقع كل ثلاث سنوات في المتوسط
3. نادر: حدث يقع كل عشر سنوات
4. غير محتمل: حدث يقع مرة كل 50 سنة أو أكثر
5. خارج النطاق: خارج النطاق - لا يتم الالتفات إلى هذه الأحداث في استمرارية الأعمال

[5]حالات فشل المكونات عبارة عن مظلة جامعة تشير إلى قصور الأداء الوظيفي لأنظمة الكمبيوتر ووحدات تزويد الطاقة وذاكرة الكمبيوتر والأقراص إلخ... يمكن للمرء أن يقرر وضع هذه الأشياء في نطاق استمرارية الأعمال أو افتراض التخفيف من ذلك في تصميم وهندسة البنية التحتية بشكل افتراضي (أي وحدات تزويد الطاقة المكررة أو أنظمة أقراص RAID أو ذاكرة ECC في الخوادم، إلخ...).

مصفوفة المخاطر

النوع	بدون أو لا يوجد	منخفضة	متوسطة	عالية	خطير
الجوانب المالية	الخطر غير موجود أو غير منطبق				
الجانب التشغيلي					
على مستوى السمعة					
الجانب القانوني					
الحوكمة[6]					
الجانب الإنساني					

[6] ربما تكون مخاطر الحوكمة الأكثر صعوبة وفي الوقت ذاته هي الأكثر تحديدًا من بين أنواع المخاطر. بالنسبة لبعض السجلات قد لا يكون الخطر موجود من الأساس. وهذا يستلزم من الإدارة إجراء وصف وتحديد واضحين لكيفية اعتماد السجل على التأثيرات الخارجية.

تقييم تأثير الأعمال التجارية

تناول أحد التهديدات المحددة في سجل التهديدات ذات التأثير الواضح على استمرارية الأعمال وقم بإجراء تقييم للتأثير على المخاطر المختلفة استنادًا إلى مصفوفة المخاطر. الاحتمالية مكررة من واقع سجل التهديدات.

الاحتمالية:

1. احتمالية كبيرة: حدث يقع سنويًا أو بوتيرة أكبر
2. محتمل: حدث يقع كل ثلاث سنوات في المتوسط
3. نادر: حدث يقع كل عشر سنوات
4. غير محتمل: حدث يقع مرة كل 50 سنة أو أكثر
5. خارج النطاق: خارج النطاق - لا يتم الالتفات إلى هذه الأحداث في استمرارية الأعمال

إن RTO (هدف وقت الاستعادة أو مدى سرعة عودة الأعمال لسابق عملها بعد الانقطاع) وأيضًا RPO (ما مقدار خسارة البيانات الذي يمكننا قبوله) يتم تعريفهما من خلال الأعمال (ويمكن أن يكون ذلك مطلبًا تعاقديًا أو قانونيًا أو على مستوى الحوكمة)، ويجب ألا يحتسب ما هو ممكن أو غير ممكن من الناحية الفنية.

فئة التهديد	التهديد	منطبق (نعم/لا)	الاحتمالية
		نعم	
المخاطر	**المستوى**	**التحفيز / الوصف / التوضيح**	
الجوانب المالية			
الجانب التشغيلي			
على مستوى السمعة			
الجانب القانوني			
الحوكمة			

الجانب الإنساني		
هدف وقت الاستعادة		
هدف نقطة الاستعادة		
تخفيف المخاطر	"لا يوجد" أو وصف الخطط المخصصة للحد من الخطر	
قبول الخطر		
تجنب الخطر		
الحد من الخطر		
احتواء الخطر		
نقل الخطر		

خطة الاستمرار في العمليات التجارية

خطة استمرارية الأعمال (القالب)			
المرجع:	[المرجع]	نوع التهديد	تأثر الأصول
السيناريو:	يصف الظروف التي أدت إلى إطلاق الخطة. ويمكن أن يكون ذلك حدثًا أو وقتًا أو ظرفًا خاصًا، إلخ...		
التنشيط:	متى يتم تنشيط الخطة؟ يمكن أن يكون ذلك أثناء التحريات أو بعد وقوع الحادثة بعدة ساعات.		
RTO:	هدف وقت الاستعادة		
RPO:	هدف نقطة الاستعادة		
فريق الأزمات:	من هو فريق الأزمات؟ من الذي يتعامل فعليًا مع الحادثة؟ استخدم أسماء الموظفين والشركات والمورّدين من أجل إزالة الغموض.		
الأولويات:	ما هي الأولويات؟ يجب ترجمة ذلك إلى قائمة متتابعة.		
التقييم:	المرحلة الأولى في التعامل مع أي حادثة مسببة للتعطل تكون بتقييم مدى ونطاق الحادثة. صِف العوامل التي يجب وضعها في الاعتبار.		
الاحتواء:	صِف المسار الإجرائي الذي يجب اتباعه من أجل منع ازدياد الموقف سوءًا.		
التعافي:	صِف المسار الإجرائي الذي يجب اتباعه من أجل استعادة الحد الأدنى من الجاهزية التشغيلية، مع الأخذ في الاعتبار الأولويات سالفة الذكر.		
الاحتواء:	وبمجرد استعادة العمليات مرة أخرى، يترك فريق الأزمات الأمر ويترك تعليمات من أجل مزيد من الإجراءات للعودة إلى حالة ما قبل الحادثة.		

التواصل:	حدد المراسلات الداخلية والخارجية، والتي تشمل الرسائل بالإضافة إلى قائمة التوزيع وأيضًا الوسائل اللازمة لذلك. ابدأ دائمًا بالمراسلات الداخلية.
المواد الحيوية:	قائمة المصادر اللازمة من أجل التعامل مع الحادثة. وهو جزء من مرحلة التحضير. لا تحتوي الخطة على محتوى فعلي، لكنها مقتصرة على مراجع (ويتحمل قادة و/أو شركاء الإدارات المختلفة المسئولية عن الحفاظ على هذا المحتوى، وتحديثه ودقته والقدرة على نقله متى أمكن)
السجلات:	ما السجلات التي يجب تقديمها خلال الأزمة وبعدها. تفيد هذه السجلات من أجل جمع الأدلة والدروس المستفادة وتعقب الحوادث الفعلية.

خطة الاستمرار في العمليات التجارية

خطة استمرارية الأعمال (القالب)			
المرجع:	[المرجع]	نوع التهديد	تأثر الأصول
السيناريو:			
التنشيط:			
RTO:			
RPO:			
فريق الأزمات:			
الأولويات:			
التقييم:			
الاحتواء:			
التعافي:			
الاحتواء:			

التواصل:	
المواد الحيوية:	
السجلات:	

وصف تدريب المحاكاة (TTX)

التدريب مدون التفاصيل بالكامل وتتألف من 5 جولات مكونة من 10 دقائق لكل منها. وفي بداية كل جولة، يتم إعطاء الفريق تعقيبات وآراء ويجب عليهم التفاعل مع التعقيبات والآراء المقدمة من خلال استخدم خطة استمرارية الأعمال المناسبة.

ولتسهيل ذلك، يتم توزيع مجموعة من البطاقات فيما بين كل فريق. وتحتوي هذه البطاقات على إجراءات عملية يتم تنفيذها كرد فعل على التعقيبات والتوجيهات المقدمة في بداية الجولة.

يمكن للمشارك اختيار ما يصل إلى 3 إجراءات (بطاقات) لكل جولة والتي يتم تنحيتها من أجل النقاش فيما بعد. يتم تجميع البطاقات في 4 فئات: الفنية والقانونية والحوكمة والاتصال، والتي تمثل بشكل أساسي الإدارة الفنية والإدارة القانونية والإدارة العامة وإدارة الاتصالات.

وخلال أي جولة، يمكن ضخ معلومات إضافية في التدريب؛ ويجب معالجة هذه المعلومات الإضافية من خلال فريق العمل ويمكن أن يؤدي ذلك إلى تغيير في الإجراءات.

وبعد إجراء 5 جولات، يتم تجميع البطاقات ومناقشتها وفقًا لعدد من الموضوعات من أجل تجميع تعقيبات وآراء المشاركين.

وصف السجل

أنت موظف في **"السجل OK"**، وهو مشغل السجل لنطاق المستوى الأعلى لرمز الدولة ok. ونطاق OK المعروف أيضًا باسم Old Kontry عبارة عن دولة أوروبية صغيرة تعداد سكانها 50 ألفًا تقريبًا. وبسبب سياساتها التحررية، فإن نطاق المستوى الأعلى ok. معروف إلى حد ما ويضم 372.304 اسم نطاق مسجل اعتبارًا من الأول من نوفمبر/تشرين الثاني 2019. وتباع أسماء نطاقات ok. من خلال شبكة عالمية تضم ما يقرب من 250 أمين سجل.

وOld Kontry عبارة عن دولة ذات نظام ملكي دستوري برلماني وحدوي.

كما أن Old Kontry ليست عضوًا في الاتحاد الأوروبي.

ويقع السجل في العاصمة كما أنه جزء من **"جامعة OK"**، لكنه يدار بشكل مستقل (الإدارة والجانب المالي والفني)؛ على الرغم من أن الجامعة هي الهيئة المشرفة عليه.

ومن أجل الخدمات الأساسية في الخلفية، فإنها تستعين بشركة .MegaRyCorp. Inc. وهي عبارة عن شركة دنماركية توفر خدمات السجل ومتخصصة في الخدمات الخلفية للسجلات. وتتحمل إحدى الشركات الأمريكية التي توفر خدمات التوجيه متعدد الاتجاهات - anycast المسئولية عن خدمات نظام أسماء النطاقات، إلا أن السجل يضم 3 خوادم اسم بنظام التوجيه الأحادي unicast قديمة وتعمل من خلال شبكة الجامعة.

ولتحقيق تواجدها على الشبكة (موقع الشركة على الويب، ووسائل التواصل الاجتماعي، إلخ...) يعتمد السجل بشدة على وكالة محلية إبداعية في مجال البيانات والتكنولوجيا، وهي جزء من مجموعة شركات دولية.

وعلاوة على خادم الاسم الرئيسي الخفي وخوادم الاسم الرسمية، يدير السجل خادم EPP وخادم WHOIS بالإضافة إلى شبكة داخلية ممتدة لأطراف خارجية خاصة بأمين السجل ولها نفس ميزات بروتوكول التزويد المرن والمزيد.

ونظرًا للشيوع والأهمية بالنسبة للاقتصاد المحلي، اعتمدت **حكومة OK** تشريعات على مدار السنوات القليلة الماضية تتوازى مع قانون حماية البيانات العامة GDPR الأوروبي فيما يخص حماية البيانات الشخصية وتوجيه NIS فيما يخص حماية البنية التحتية الحيوية ومشغلي الخدمات الأساسية. كما قامت بتعيين وزارة الاتصالات لتكون الهيئة المشرفة على الامتثال والسياسات.

علمًا بأن **"سجل OK"** عبارة عن مؤسسة صغيرة تضم 7 أشخاص يعملون مباشرة لصالح السجل. ويمكنها الاعتماد على دعم تقنية المعلومات من أجل أجهزة الكمبيوتر المحمولة/كمبيوتر سطح المكتب/البريد الإلكتروني/إلخ... في الجامعة.

وهي توظف 3 مهندسين (1 مطور و1 مدير أنظمة و1 مهندس شبكات) يتولون الاهتمام ببوابة أمين السجل على الويب، والمراقبة وخوادم الاسم القديمة، وأنظمة جدران الحماية، والشبكة الداخلية(الواسعة)، ودعم أمين السجل والتقارير الفنية.

وهناك مدير عام ومدير للمبيعات والتسويق ومدير للماليات ومدير قانوني؛ بالإضافة إلى فريق فني يقدم يعمل تحت إمرة المدير العام مباشرة. وتندرج إدارة استمرارية الأعمال تحت مسئولية المدير القانوني.

خطة استمرارية العمل للجانب الإلكتروني: السطو

خطة استمرارية الأعمال			
المرجع:	BCP-101.01	الجانب الإلكتروني: السطو	عالمي
السيناريو:	توضح الأدلة أن البنية التحتية للسجل تم السطو عليها والعبث بها. قامت جهة غريبة بتثبيت برامج، وقامت بإنشاء حسابات وأدوات للوصول عن بعد، إلخ... من أجل التسلل إلى السجل. تم استخراج بيانات ربما تكون (حساسة).		
التنشيط:	قيد التقصي فورًا		
RTO:	24 ساعة		
RPO:	فقد البيانات لمدة 24 ساعة.		
فريق الأزمات:	المدير القانوني. - ivan.horvat@registry.tld - +CC 123 55 88 . المدير الفني – juan.perez@registry.tld – +CC 123 44 55 مدير استمرارية الأعمال – jane.doe@registry.tld – +CC 123 33 66 . المدير العام - yamado.toro@registry.tld - +CC 123 56 44		
الأولويات:	حماية توافر وتكامل خوادم الاسم ومنطقة ok. عزل البنية التحتية لخادم الاسم إذا لزم الأمر. عزل النظم التي تم السطو عليها. جمع الأدلة.		
التقييم:	إجراء تقييم وجرد للنظم التي تم اختراقها. ما الخدمات التي تأثرت؟ هل تأثر نظام DNS، أو منصة التسجيل أو النظم الداخلية أو موقع الويب؟ تحقق من البنية التحتية لخادم الاسم والخدمة. هل للمهاجم الغلبة الدائمة؟ هل المهاجم حاضر في وقت التحري والتقصي؟ هل يلزم الحصول على مساعدة خارجية من الشركات المتخصصة في حوادث السطو الإلكتروني (هل ثمة دليل على وجود متورطين حكوميين)؟ هل تسربت البيانات وإن كان الأمر كذلك فما نوع البيانات التي تسربت؟ ما تأثير البيانات المسربة؟		
الاحتواء:	التأكد من أن البنية التحتية لخادم الاسم مصانة مع عزل خوادم الاسم عن المنطقة المتضررة. تعطيل أو إيقاف تشغيل النظم المتأثرة. لا تحاول إصلاح أو ضبط الأنظمة المتضررة أو محاربة المتطفل. يجب التركيز على عزل النظم المتضررة. حاول جمع الأدلة؛ ولا تعبث بالأدلة.		

التعافي:	يجب إعادة بناء الأنظمة المتضررة وإعادة نشرها. في حالة تعرض معدات المستخدم النهائي للضرر، يتم نشر أنظمة جديدة.
الاحتواء:	بمجرد عزل الأنظمة المتضررة وإيقاف تشغيلها واستعادة الخدمات من خلال استخدام الأنظمة المعاد تشغيلها ونشرها؛ يقوم فريق الأزمات بتعيين فريق من أجل التعامل مع الأنشطة التالية: 1. الاتصال بجهات إنفاذ القانون وتقديم شكوى. 2. التأكد من تخزين الأنظمة المتضررة بشكل آمن وتجنب ملفات السجلات كأدلة. تحليل تكامل ونزاهة قاعدة البيانات الجوهرية (هل ثمة أدلة على وجود تغييرات؟).
التواصل:	**الاتصال الداخلي:** الاتصال الأولي بجميع أنظمتنا التي تعرضت للاختراق وأننا نقوم بعزل الأنظمة المخترقة. التأكيد على أن المزيد من الاتصالات بالعالم الخارجي سوف يتم التعامل معها من خلال مدير المبيعات والتسويق أو من خلال المدير القانوني مباشرة. **الاتصالات الخارجية:** إبلاغ أصحاب المصلحة (مجلس إدارة الجامعة والجهات المعنية) إبلاغ أمناء السجلات في حالة تعطيل الأنظمة (أي موقع الويب أو خدمة whois أو بروتوكول التزويد المرن) وإبلاغهم بالخطوات الإضافية التي يتم اتخاذها. إبلاغ جهات إنفاذ القانون. نشر ما تحقق من عمل بصفة منتظمة على حسابات مواقع التواصل الاجتماعي وعلى مواقع الويب العامة.
المواد الحيوية:	توثيق البنية التحتية والإعدادات. مخازن كلمات المرور للوصول إلى مختلف الأنظمة. نشر البنية التحتية والتخطيط لها من أجل نشر بنية تحتية جديدة. قوائم التوزيع من أجل الاتصالات (أمناء السجلات والموظفين وأصحاب المصلحة)
السجلات:	إنشاء سجل بالأحداث، وما تم اكتشافه، وما الإجراءات التي تم القيام بها، وما الأدلة التي تم جمعها. قم بذلك خلال التعامل مع الأزمات وليس في مرحلة لاحقة.

سيناريو التدريب

الجولة 1: التعقيبات الجمعة، 05:00 مساءً

- يقوم باحث في مجال الأمر بالاتصال بالمدير العام لمشغل السجل بأنه قد عثر على دليل حول سلة اللصق لمستخلص من قاعدة بيانات تشير على ما يبدو إلى شبكة خارجية للسجل يستخدمها أمناء السجلات التابعون له.
- قام الباحث بفحص كلمات المرور المجزأة في سلة اللصق ونجح في "فك" بعض كلمات المرور بسهولة إلى حد ما. وكما هو متوقع فإن كلمة المرور "password123" كانت شائعة إلى حد ما. ويؤكد أنه نجح في تسجيل الدخول إلى شبكة أمين السجل الخارجية في بعض الأوقات المحددة (ويقوم بتحديد تلك الأوقات للمدير).

- ولا تزال سلة اللصق متصلة بالإنترنت ويعثر الباحث أيضًا على بعض الأدلة على أن شخصًا يقوم ببيع بيانات إثبات الهوية على الويب المظلم.
- ويعتقد في وجود أدلة كافية لافتراض أن شخصًا قام بالسطو على السجل وأن هذا المجرم قد بدأ في التربح من هذا العمل.

وهذه هي المعلومات الأولية التي تلقاها السجل. كيف تكون ردة فعل المدير، ماذا عساه فاعل؟ من هنا، يجب تزويد المدير ببعض المعلومات الإضافية اعتمادًا على المسار الإجرائي الذي يتخذه. لا تنس مراعاة عنصر الوقت. أمام المشاركين 15 دقيقة فقط لكل جولة.

اختر 3 بطاقات

الجولة 2: التعقيبات — الجمعة، 08:00 مساءً

- مرت 3 ساعات منذ الاكتشاف الأولي
- يقوم شخص بنشر الرابط عبر التغريد لسلة لصق أخرى بالوسم #freeDomains4All #longLive.OK؛ وهو نسخة من سلة اللصق الأصلية.
- وتتم ملاحظة التغريدة وإعادة نشرها؛ ويتم تعديل الوسم إلى #itWorks.

اختر 3 بطاقات

الجولة 3: التعقيبات — الجمعة، 10:00 مساءً

- مرت ساعتان
- تتواصل الصحافة مع مشغل السجل، ويريدون معرفة ما يحدث ويطلبون الحصول على بيان رسمي.
- ويصل إلى مدير مشغل السجل اتصال هاتفي من التلفزيون الوطني.
- ولا يزال المهندسون يبحثون في الأمر، لكنهم لم يجدوا إلى الآن مكان تسرب المعلومات.

اختر 3 بطاقات

جولة إضافية: الإدخال (3 دقائق قبل نهاية الجولة)

لجعل التدريب أكثر تشويقًا، يمكن ضخ معلومات إضافية. أما في الحياة الواقعية، فإن الأحداث لا تتبع نمطًا يمكن التنبؤ به، وليس بالتأكيد أثناء الأزمات. ولا تقدم الجولات الإضافية سوى معلومات إضافية يجب صياغتها والعمل عليها قبل نهاية الجولة.

- ولدى المهندسين بعض الأخبار الجيدة وبعض الأخبار السيئة للغاية.
- فقد اكتشفوا المكان الذي تسلل منه القراصنة للنظام وتعقبوا ما تغير.
- كما لاحظوا أن أكثر من 50 ألف اسم نطاق إضافية تم تسجيلها وتم تغيير عدد غير محدد من أسماء النطاقات الحالية؛ والبعض منها من النطاقات ذات الأهمية الكبرى.
- ويقترحون تخفيف عمل نظام أسماء النطاقات والتواصل مع أهم موفري خدمة الإنترنت من أجل إعادة تحميل وحدات تحويل العناوين.

تحديث 3 بطاقات

الجولة 4: التعقيبات — السبت: 06:00 صباحًا

- مرت 8 ساعات
- يقوم مركز CERT الوطني بالاتصال بمشغل السجل؛ فقد تلقوا بعض المعلومات حول مصدر الهجوم
- فقد تم إمطار وسائط التواصل الاجتماعي الخاصة بمشغل السجل بأسئلة من أصحاب أسماء النطاقات المعنيين ومن أمناء السجلات
- وقد اكتظت صناديق وارد البريد العامة بأكثر من 5.000 بريد إلكتروني
- وتقوم الوسائط بالاتصال بمشغل السجل مرة أخرى من أجل الحصول على تحديثات ويسألون عن السبب وراء استغراق حل المشكلة لكل هذا الوقت الطويل

- تقوم الوزارة المشرفة المعنية بالأمر (مثل الاتصالات السلكية واللاسلكية) بالاتصال بالمدير العام لمشغل السجل، ويريدون الحصول على إحاطة بالحالة وتلخيص تأثيرات الحادثة

اختر 3 بطاقات

الجولة 5: الإغلاق الأحد: 09:00 صباحًا

- مرت 21 ساعة
- قام الفريق الهندسي بوقف قاعدة البيانات يوم الخميس في تمام الساعة 11:47 مساءً، وكان هذا هو النسخ الاحتياطي الأقرب دون دلل على تعديل أسماء النطاقات
- وتمت إعادة تحميل خوادم الاسم
- وقد تم إصلاح نقاط الاختراق، التي استغلها القراصنة
- وتم إعادة تعيين جميع بيانات إثبات الهوية الخاص بأمين السجل
- تلقت إدارة الدعم قائمة بأسماء النطاقات وأمناء السجلات والمسجلين الذين تضرروا
- ثمة احتياطي رئيسي بدعم من أكثر من 10.000 بريد إلكتروني لدعم طلبات الدعم وعدد لا يحصى من التغريدات الغاضبة
- وقد لاحظ العديد من المدونين ومدوني الفيديوهات هذه المشكلة وقاموا بنشر آرائهم

اختر 3 بطاقات

نهاية التدريب - وقف مؤقت

سوف يكون المشارك بحاجة لاستراحة ☹

التلخيص

يقوم كل فريق بتقديم بطاقاتهم.

لتحقيق تدريب فعال وكافٍ، من الضروري إجراء تلخيص صحيح ومناقشة إجراءات الفريق. ولذلك فإن مخرجات ونتائج فريق الأزمات يجب التعرف عليها وتدوينها إما خطيًا أو من خلال التسجيل. ويجب أن يركز التلخيص على عدد من الموضوعات:

1. ما هي الاستجابة العامة للتدريب؟
2. ما مدى جودة اتباع خطة استمرارية الأعمال؟
3. أين بدأ الفريق في الارتجال؟
4. هل شعروا أنه مناسبين وعلى قدر المهمة؟
5. ما الذي تعلموه؟
6. ما التحسين اللازم؟

البطاقات

قم بطباعة هذه البطاقات في نسق حسب حجم بطاقات الشركة، وفي النهاية استخدم ألوان مختلفة لكل فئة.

	القطاع الفني	الإدارة القانونية / استمرارية الأعمال	الاتصالات	الحوكمة / الإدارة
1	أغلق خوادم الاسم الرسمية	اتصل بجهات إنفاذ القانون	قم بنشر بيان بالحالة على مواقع التواصل الاجتماعي	أعلن عن وجود حالة كوارث
2	اتصل بمشغل خدمة السجل وأبلغه بالمشكلة	أبلغ الإدارة باستراتيجية الاتصالات	أرسل رسالة على وسائط التواصل الاجتماعي	استدع فريق الأزمات
3	اتصل بمشغل التوجيه متعدد الاتجاهات - anycast وأبلغه بالمشكلة	اتصل بشركة خارجية في مجال الاستجابة للحوادث من أجل المساعدة في التعامل مع المشكلة	لبِّ نداء الصحافة	افتح خطة استمرارية الأعمال
4	أغلق منصة التسجيل	وجّه بخفض مستوى الاتصالات	قم بإعداد التواصل فيما يخص وقف العمل	اتصل بالهيئة / المجلس المشرف
5	ابدأ في البحث عن ملفات السجل المتاحة	وجّه بالشفافية الكاملة للإدارة	اكتب بيان(بيانات) صحفية	أبلغ هيئات الإشراف الحكومية
6	قم باستعادة قاعدة البيانات الجوهرية	تواصل مع موفري الاتصالات المحليين لإعادة بدء وحدات حل العناوين الخاصة بهم	اكتب قوالب ونماذج من أجل مراسلات الأزمات	اتصل بمركز CERT في البلد وأبلغهم بالحادثة
7	أعد تثبيت الأنظمة المخترقة	أرسل النتائج إلى جهات إنفاذ القانون	أرسل البيانات الصحفية حول التأثير	اعقد مؤتمرًا صحفيًا
8	أجر تقييمًا فنيًا واجمع أدلة الأنظمة المخترقة	اتصل بأمناء السجلات لتغيير كلمات المرور	لا تجر أية اتصالات على القنوات العامة حتى تأكيد ذلك من جانب المدير القانوني والعام	قدم إحاطة بالحالة إلى هيئات الإشراف الحكومية
9	ابدأ في الرد على طلبات حل المشكلات والطلبات الأخرى المقدمة عبر عنوان البريد الإلكتروني الخاص بالدعم	أبلغ مجلس حماية البيانات الأوروبية بالمشكلة	أرسل إحاطة داخلية بالحالة	أعلن عن نهاية الأزمة والتنحي - العودة إلى العمل كالمعتاد
10	ضع قائمة بأسماء النطاقات المعدلة لتحديد الضحايا	تقدم بمذكرة بالحادثة إلى جهات إنفاذ القانون	قم بتعيين متحدث رسمي للتواصل بخصوص الأزمة	اطلب المساعدة من مركز CERT الوطني
11	ضع قائمة بأسماء النطاقات المضافة	أبلغ شركة التأمين	قم بإنكار الاختراق	أبلغ ICANN

12	احجب الوصول إلى نظام التسجيل	أبلغ المسجلين المتضررين	أرسل رسالة بالبريد الإلكتروني إلى عمليات نطاقات المستوى الأعلى من أجل الحصول على المساعدة	اتصل بخط الطوارئ في IANA المتاح على مدار الساعة
13	قم تغيير جميع كلمات المرور	أبلغ السجلات الأخرى من خلال القائمة البريدية لعمليات نطاقات المستوى الأعلى		ألق باللوم على عمليات نطاقات المستوى الأعلى :-)
14	قم بتنزيل قائمة كلمات المرور من سلة اللصق	اطلب المساعدة من السجلات الأخرى من خلال القائمة البريدية لعمليات نطاقات المستوى الأعلى		
15	قم بتثبيت SIEM			

تتوفر منصة البطاقات للتنزيل على موقع عمليات نطاقات المستوى الأعلى على الويب بتنسيق أدوبي إنديزاين، وجاهزة للإرسال إلى المطبعة.

تلميحات وحيل لورشة العمل:

يحتوي هذا القسم على تلميحات وحيل لتمرين DR/BCP، برجاء مراسلة عمليات نطاقات المستوى الأعلى بالبريد الإلكتروني إذا كانت لديك أي رؤية جديدة فيما يخص كيفية تحسين TTX.

- فتحديد أصحاب المصلحة، والتهديدات والمخاطر ليست مهمة شخص واحد. واصل التعبير عن ذلك.
- بعض التهديدات "مرعبة"، وهذا هو السبب المنطقي الداعي لتوثيقها ووضع خطة للتعامل معها.
- اجعل تدريب الأفراد يحدد أيضًا ما هي الوظائف/المجموعات/الأفراد داخل كل نطاق مستوى أعلى يتصرف فعليًا بصفة مدير خطة استمرارية العمل؛ وقم بتحديد أصحاب المصلحة الفعليين لديه.
- البعض قد يعاني من التأثيرات المالية - وطلب المعونة من الناس في ذلك؛ فإن استمرارية الأعمال تدريب جامع لكل ذلك
- أوضح داخل مؤسستك من الذي يقوم بإنجاز دور مدير خطة استمرارية العمل، هل هي الإدارة القانونية أو مكتب مدير المشروعات أو الإدارة المالية أو مدير المعلومات أو مسئول خدمة العملاء أو المدير التنفيذي أو مسئول التشغيل؟
- ربما يجب عليك بدء العمل من خلال توزيع البطاقات الثلاثة التالية لكل فريق