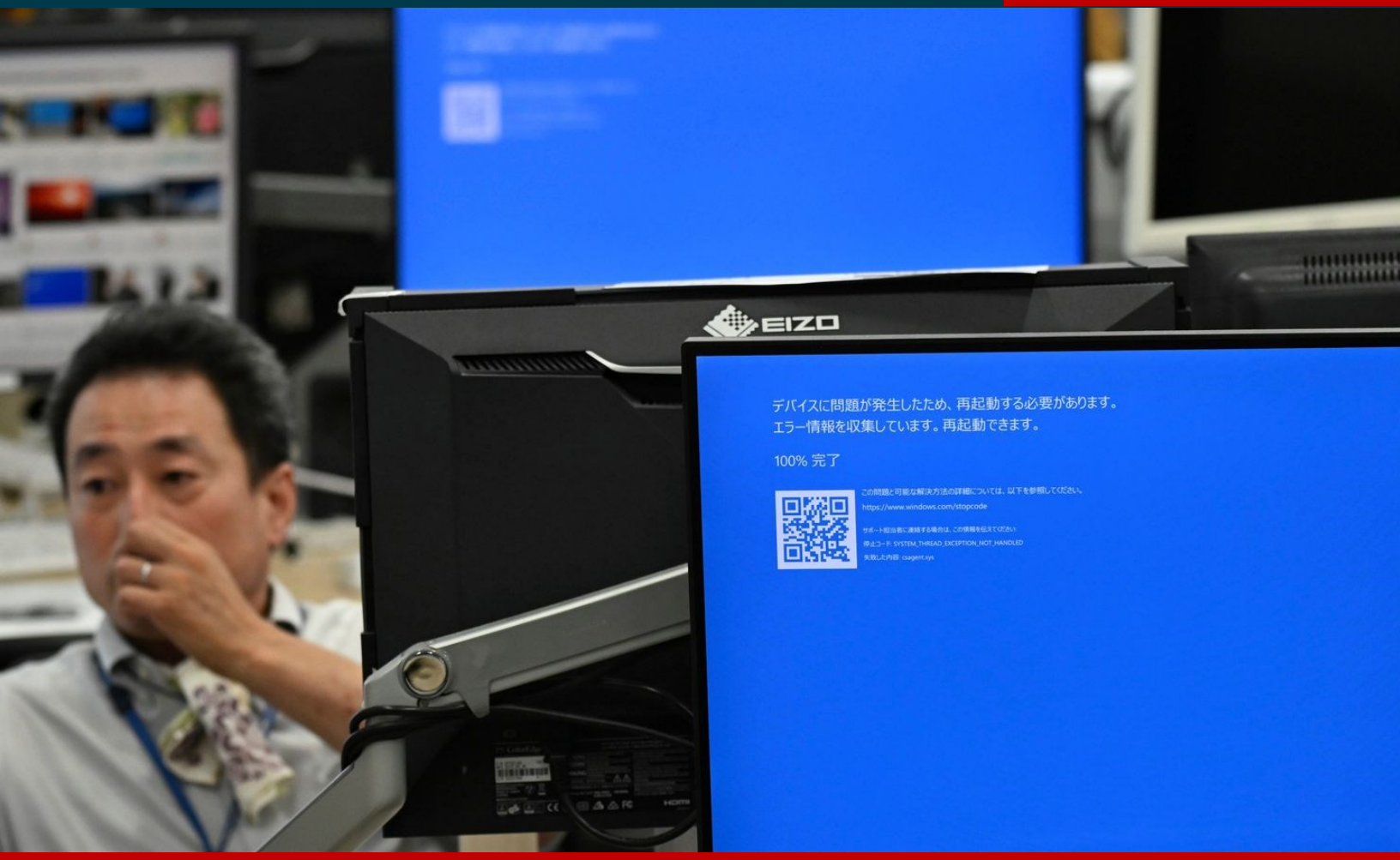
مجلة تحليل الأعمال
Business Analysis Magazine

عـــدد خـــاص
Special Issue

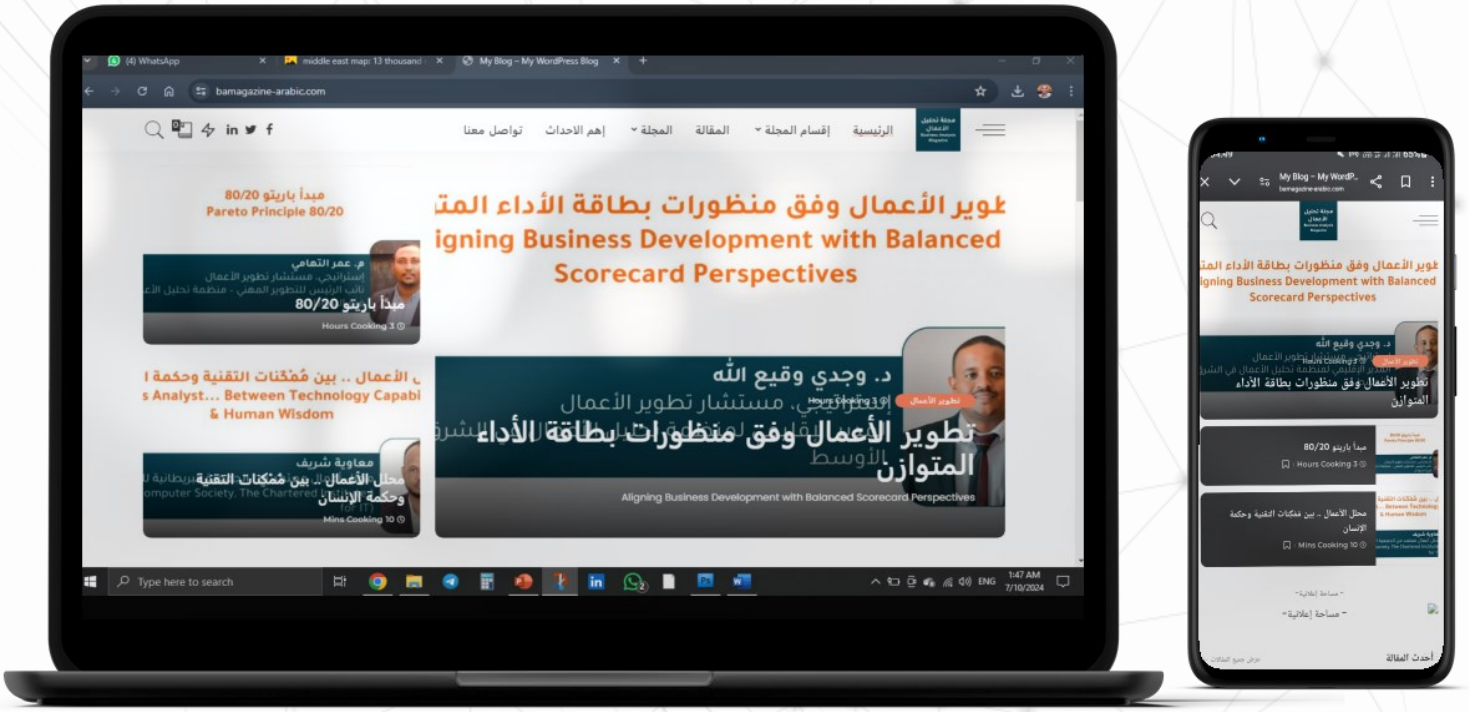
21 يوليو 2024
21 July 2024

IIBA® Sudan Chapter

مجلة شهرية متخصصة في تحليل الأعمال
تصدر باللغتين العربية والإنجليزية بالتعاون مع:



إنقطاع خدمات مايكروسوفت عالمياً:
التدابير الوقائية من منظور إستراتيجي



قـريـبـاً

الموقع الإلكتروني
لمجلة تحليل الأعمال

مجلة تحليل الأعمال

Business Analysis Magazine

A monthly Magazine Issued in Association with:

IIBA® Sudan Chapter

www.sudan.iiba.org

تنويه:

- المقالات المنشورة يعبر عنها كُتَّاب المحتـوى وليسـت بالضرورة تعبر عن آراء المجلة.
- قد تحتوي بعض المقالات على روابط إنترنت، فالمجلة ليست مسؤولة عن أي محتوى في تلك المواقع.

Notice:

- The published articles are expressed by the content authors and do not necessarily reflect the agenda of the magazine.
- Some articles may contain Internet links. The magazine is not responsible for any content on those sites.

Design by:

HAMEEDOV

Hameedove@gmail.com

+249 91 800 7781 +20 101 399 1857

www.hameedov.com

20 July 2024

محتوى العدد Contents

إفتتاحية

هيثم الكاشف
- خبير تحليل الأعمال
- مستشار إستدامة الأعمال

في العصر الحديث أصبحت التكنلوجيا جزء أساسي من حياتنا. دخلت في كل المجالات تقريباً منها الصناعية والزراعية والتعليمية والصحية، ودورها الفعال في عملية الإتصال، وكان سبب تسمية أن العالم أصبح قرية صغيرة كناية علي أن ما يحدث في مكان ما في العالم يعلم به أشخاص في مكان آخر من العالم، والموضوع تجاوز المعرفة إلى التأثير المباشر.

هذا ما حدث عندما إستيقظ العالم على موجة أعطال إلكترونية غزت العالم تأثرت بها دول متقدمة على رأسها الولايات المتحدة الأمريكية وأوروبا والشرق الأقصى الصين وسنغافورة، تسبب على أثرها تعطل أنظمة المطارات والموانئ وأسواق المال والبنوك والقطاع المالي بشكل كامل.

بالإضافة للقنوات التليفزيونية وبعض الشركات العالمية، بسبب شركة (كراودسترايك) المتهم الأول بالعطل التقني العالمي وهي شركة أمن سيبراني، سبب أعطال تقنية علي أجهزة الكمبيوتر التي تعمل بنظام ميكروسوفت وهي المتضرر الأكبر من هذه الجائحة الآن.

العطل التقني تسبب في إنقطاع الإتصال بين سحابة التخزين والكمبيوتر والمستخدمين، لذلك نحن في (مجلة تحليل الأعمال) سوف نقوم بأول مهام تحليل الأعمال وهي تحديد وتعريف المشكلة بواسطة الكتاب المتخصصين الذين إستشعروا المسئولية والمساهمة في تحليل وتعريف هذه المشكلة والوصول بنا إلي الدروس المستفادة من هذه الأزمة.

ماذا يجب على الشركات والحكومات والأفراد أن تقوم به لتقليل أو تفادي المخاطر التقنية مستقبلاً.

ثغرة "الفشل المفتوح" في برنامج CrowdStrike Falcon Sensor:

التحديات والحلول

م. نزار سيف الدين
إستشاري أمن المعلومات والحوكمة

إن السبب الرئيسي لثغرة CrowdStrike Falcon Sensor يكمن في كيفية تطبيق حماية إزالة التثبيت عبر برنامج تثبيت مايكروسوفت (MSI) تحديدًا، هي الثغرة التي تنشأ بسبب الطريقة التي تُعالج بها الإجراءات المتخصصة (CAs) أثناء عملية إزالة التثبيت. لهذا عندما تفشل عملية التحقق من رمز إزالة التثبيت المخصص أو تتوقف بشكل غير متوقع، هنا يستمر برنامج MSI في إزالة التثبيت بدلاً من التوقف، وهذا ما يُعرف بـ"الفشل المفتوح" بدلاً من "الفشل المغلق".

و يسمح هذا الخلل للمهاجم الذي لديه صلاحيات إدارية بتجاوز حماية إزالة التثبيت عن طريق تعطيل أو إيقاف عملية الإجراء المخصص.

تخيل أن هناك نظام حماية يعتمد على برنامج MSI لإزالة التثبيت، وتم تصميمه بحيث لا يمكن لأي شخص إزالة البرنامج إلا بعد التحقق من رمز إزالة التثبيت.

كمثال توضيحي:

عندما يبدأ المستخدم عملية إزالة التثبيت، يقوم برنامج MSI بتنفيذ إجراءات مخصصة (Custom Action) للتحقق من رمز إزالة التثبيت. وهي أوامر أو برامج نصية (scripts) تُضاف إلى حزمة التثبيت لتنفذ مهام معينة أثناء عملية التثبيت أو إزالة التثبيت. في سياق برنامج تثبيت مايكروسوفت (MSI)، يمكن إستخدام الإجراءات المخصصة لتنفيذ عمليات إضافية لا يمكن تنفيذها بواسطة تعليمات MSI القياسية فقط.

لذا فإذا كان الرمز صحيحاً، تستمر عملية إزالة التثبيت.أما إذا كان الرمز غير صحيح، تتوقف عملية إزالة التثبيت، ويظهر للمستخدم رسالة خطأ.

السيناريو الذي يحدث فيه الثغرة:

يبدأ المستخدم (أو المهاجم الذي لديه صلاحيات إدارية) عملية إزالة التثبيت. وهنا برنامج MSI يبدأ في تنفيذ الإجراءات المخصصة للتحقق من الرمز. ويقوم المهاجم بتعطيل عملية الإجراء المخصص (مثلاً، عن طريق قتل العملية أو التسبب في تعطلها). حيث يقوم برنامج MSI يستمر في إزالة التثبيت رغم فشل التحقق من الرمز، بسبب "الفشل المفتوح".

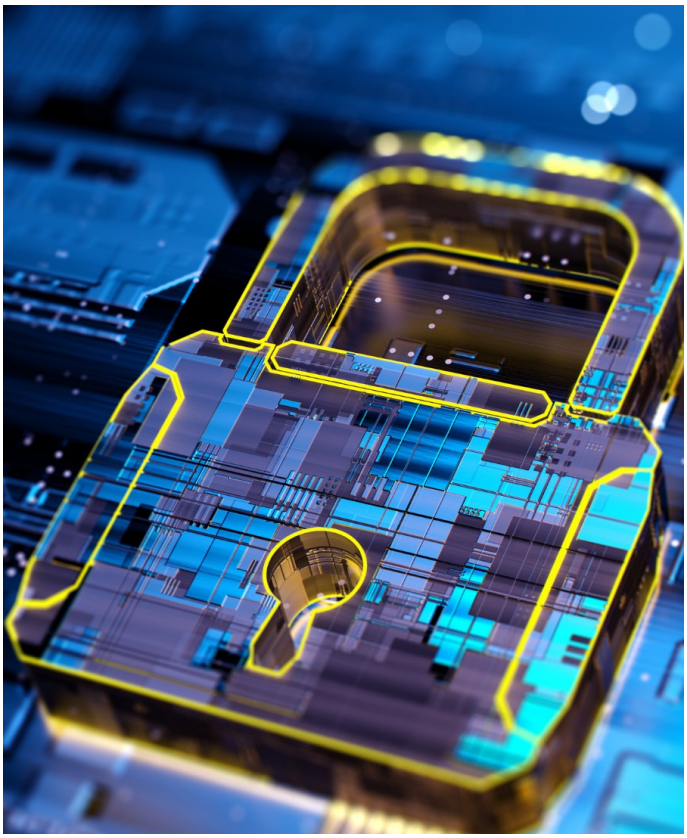
تبسيط السيناريو:

تخيل أنك تحاول دخول غرفة محمية برمز سري، ففي الحالة العادية، إذا أدخلت الرمز بشكل صحيح، يفتح الباب أما إذا أدخلت الرمز بشكل خاطئ، يبقى الباب مغلقًا.

لكن في هذا السيناريو ما يحدث هو حتى لو أدخلت الرمز بشكل خاطئ أو عطلت عملية التحقق، يفتح الباب تلقائيًا ويتيح لك الدخول.

هذا ما يسمي بالفشل المفتوح، حيث يتجاوز النظام إجراءات الحماية عندما تواجه مشكلة، بدلاً من إيقاف العملية وحماية النظام.

الإجراءات المخصصة (CAs) في MSI تمثل نقطة ضعف محتملة إذا لم يتم التعامل معها بشكل صحيح، حيث يمكن للمهاجم تعطيلها أو التلاعب بها لتجاوز إجراءات الحماية المفروضة أثناء عملية التثبيت أو الإزالة.



ولتفادي مثل هذه الأحداث من منظور إستراتيجي وتقني، يمكن إتباع الإجراءات التالية:

أولاً من منظور إستراتيجي:

١- يجب تقييم الأمان بشكل دوري وإجراء مراجعات أمان منتظمة لتحديد الثغرات المحتملة وتطبيق التحديثات الأمنية اللازمة.

٢- وضع سياسات قوية وتطوير هذه السياسات والإجراءات الصارمة لإدارة التثبيت والإزالة للتطبيقات الحساسة.

٣- تدريب الموظفين على أهمية الأمان الإلكتروني وكيفية التعامل مع التهديدات المحتملة.

٤- إختبار الأمان كإجراء إختبارات الإختراق دورية (Penetration Testing) للتأكد من متانة الأنظمة وإجراءات الحماية الصحيحة وإمكانيه معالجة الثغرات.

٥- تحديد وضبط الصلاحيات للأنظمة بدقة، بحيث لا يمتلك أي شخص صلاحيات إدارية إلا عند الضرورة.

ثانيا - من منظور تقني:

١- التأكد من أن العمليات الحيوية تفشل بطريقة مغلقة (Fail Closed) بحيث تتوقف العمليات عند حدوث خطأ.

٢- مراجعة وتدقيق الشيفرة بإجراء مراجعات دورية للشيفرة المصدرية للكشف عن الثغرات الأمنية.

٣- تطبيق إجراءات تحقق متعددة الطبقات (Multilayer factor authentications) لتأكيد الهويات قبل السماح بإزالة التثبيت.

٤- القيام بالتحديثات الأمنية بشكل مستمر للحفاظ على النظام ضد الثغرات المكتشفة حديثًا.

٥- إستخدام أدوات مراقبة وتنبيه للكشف عن أي سلوك غير عادي أو محاولات غير مصرح بها لتعطيل الإجراءات.

ثالثاً ومن منظور تحليل المخاطر:

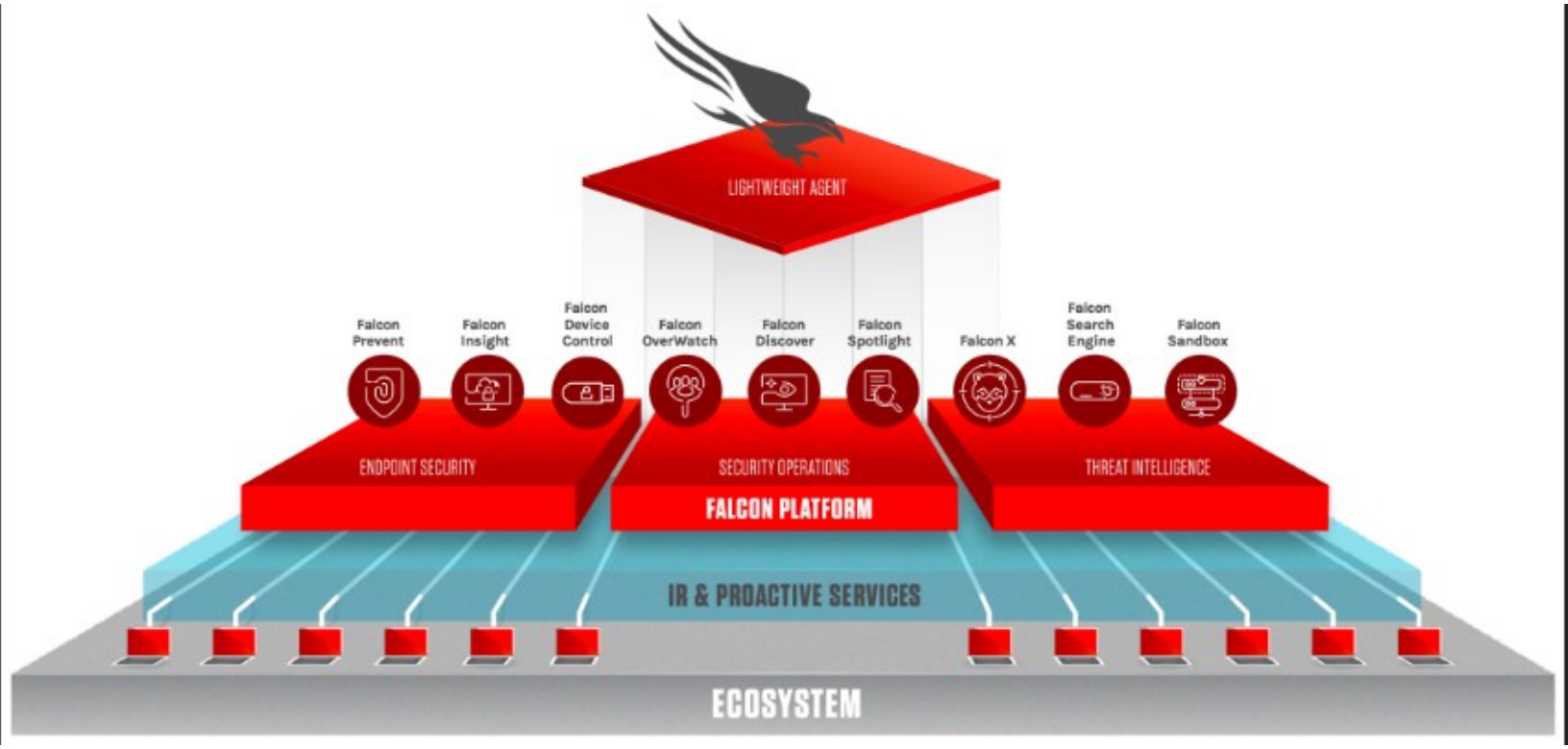
١- جمع المعلومات حول نقاط الضعف المحتملة وتحديد المخاطر والسيناريوهات التي يمكن أن تؤدي إلى استغلال الثغرة.

٢- تقييم تأثير الثغرات على النظام والشركة بناءً على مدى الضرر الذي يمكن أن يحدث.

٣- تحليل مدى إحتمالية وقوع الهجوم أو إستغلال الثغرة.

٤- وضع خطط للحد من المخاطر من خلال تطبيق إجراءات حماية إضافية.

٥- مراقبة الأنظمة بإستمرار وإعادة تقييم المخاطر بناءً على التغييرات والتحديثات في البيئة الأمنية.



فشل النظُم الحيوية

م. محمد أبكم
إستشاري نظم المعلومات والتحول المؤسسي

"Anything that can go wrong will go wrong, and at the worst possible time."

قانون ميرفي Murphy's Law

ملاحظات وعبارات المهندس ميرفي جاءت في سياق تحليل فشل بعض عمليات إطلاق الصواريخ في منتصف القرن الماضي. وكثيراً ما أفكر في هذه العبارة لإستخلاص طرق منع حدوث المشاكل أو على الأقل تقليل أثرها.

عايشت عدداً من حوادث الفشل الكبيرة خلال مسيرتي المهنية وبعضها كنت طرفاً فيها منها ما حدث خلال الحرب الدائرة حالياً في السودان، فمن منا كان يصدق أن الحرب ستندلع وتعطل معها كل مراكز البيانات بما فيها المراكز البديلة بل والخدمات التي تشغل هذه المراكز ومنها أيضاً فشل النظام المحاسبي الذي كنت أشرف عليه في أوائل هذا القرن وشفع لي حينها أنني كنت دوماً أرفع تقارير للإدارة بأن هذا الحادث متوقع وأن هناك خيارات متعددة لمنع حدوثه وتقل كثيراً كلما تقدم الزمن لأنه في حال حدث ذلك ستقل الخيارات بدرجة كبيرة ويصبح طريق التعافي صعباً.

فشل النظم الذي حدث أمس متوقع من هذا الباب وأيضاً عايشت حادثاً مماثلاً كان لي الشرف أن كنت أول المبلغين عنه للشركة المطورة لنظام الحماية وكان أن إتخذنا قراراً فحواه أن ما حدث يمكن أن يحدث مرة أخرى، ولأننا لا يمكن أن نستغني عن نظم الحماية والتحديث المستمر للمخدمات والأجهزة وتجهيزاتنا كانت كما يلي: -

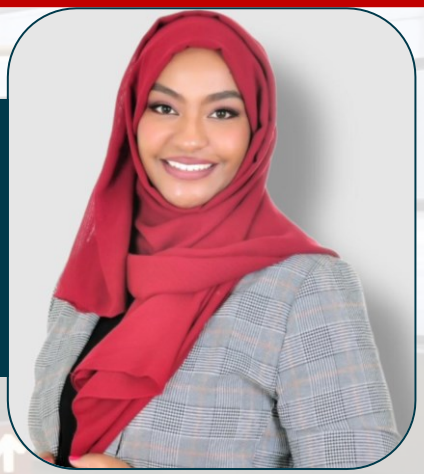
- التحديث التدريجي ومنع التحديث التلقائي الشامل.
- توفير عدد من الأجهزة التي يمكن بها تمرير العمليات الحيوية في حالة حدوث مشكلة عامة.
- تدريب الموظفين على التعامل مع مثل هذه الأحداث مثل حذف التحديث الأخير وإستعادة الأجهزة الطرفية لوضع ما قبل التحديث.

أخيراً مثل هذه الأحداث ينطبق عليها أيضاً العبارة التحذيرية لميرفي والتي يقول فيها:

"If there are two or more ways to do something and one of those results in a catastrophe, then someone will do it that way."

هذا لا يعني تقليل صلاحيات الموظفين في إتخاذ القرارات بقدر ما يعني توعيتهم على تفهم المخاطر التي تحيط بهذه القرارات.

إنقطاع خدمات مايكروسوفت عالمياً:
التدابير الوقائية من منظور استراتيجي



إسراء الماحي
إستراتيجي،
نائب الرئيس للفعاليات - منظمة تحليل الأعمال فرع السودان

ما حدث:

واجهت العديد من خدمات مايكروسوفت، بما في ذلك Teams و Outlook و 365 و Azure، إنقطاعًا عالميًا في 19 يوليو 2024.

تسبب الإنقطاع في تعطيل البريد الإلكتروني وتطبيقات مشاركة الملفات والعديد من الخدمات الأساسية الأخرى للشركات والمنظمات حول العالم.

تأثرت بورصات الأوراق المالية وخطوط الطيران والعديد من القطاعات الأخرى بشكل كبير.

هذه الحادثة كشفت عن نقاط ضعف في عملية نشر التحديثات وضرورة تبني إستراتيجيات وقائية فعّالة.

الحادثة

- تسبب التحديث في ظهور الشاشة الزرقاء (BSOD) على آلاف الأنظمة، مما أدى إلى تعطيل العمليات عالميًا.
- رغم تحديد CrowdStrike للمشكلة بسرعة وتقديم حل، إلا أن الأضرار كانت قد وقعت بالفعل.

السبب:

- حددت مايكروسوفت سبب المشكلة في تغيير خاطئ في التكوين تم إجراؤه على شبكتها العالمية.
- لم يكن الحادث نتيجة لهجوم سيبراني.

الإستجابة:

- عملت مايكروسوفت بسرعة على تحديد المشكلة وإصلاحها. تم إستعادة جميع الخدمات المتأثرة بالكامل في غضون ساعات قليلة.
- أصدرت مايكروسوفت بيانًا إعتذرت فيه عن الإنقطاع وأوضحت سبب المشكلة.

التأثير:

- تسبب إنقطاع الخدمات في خسائر مالية كبيرة للشركات والمنظمات المتأثرة.
- أثار الحادث أيضًا مخاوف بشأن إعتماد الشركات المتزايد على خدمات الحوسبة السحابية.

التـــدابير الإســـتراتيجية لمنـــع الحـــوادث المستقبلية

1. إختبار التحديثات بدقة

- إختبارات ما قبل النشر الشاملة:

تنفيـذ إختبـارات مكثفـة فـي بيئـات محاكـاة لتعكس الظروف الواقعية لتحديد المشكلات المحتملة قبل النشر.

- الإطلاق المرحلي:

تطبيق التحديثات على عدد محدود من الأنظمة فـي البدايـة للكشـف المبكـر عـن المشـكلات وحلها دون تأثير واسع.

2. الأنظمة الإحتياطية وخطط الإسترداد

- أنظمة إحتياطية موزعة جغرافيًا:

إنشـاء أنظمـة إحتياطيـة عبـر منـاطق متعـددة لضمان عدم تأثير المشكلات في منطقة واحدة على العمليات العالمية.

- آليات الإسترداد القوية:

تطوير وإختبار آليات إسترداد لضمان الإنتقـال السلس والحد الأدنى مـن التعطيـل فـي حالـة فشل النظام.

3. إجراءات التراجع التلقائية

- قدرات التراجع الفوري:

تطوير إجراءات تراجع تلقائيـة يمكـن تفعيلهـا بسرعة للعودة إلى حالـة مسـتقرة سـابقة فـي حال تسبب التحديث في مشكلات.

- المراقبة المستمرة والتنبيهات:

تنفيذ أنظمة مراقبة في الوقت الحقيقـي تـوفر تنبيهات فورية، مما يسمح بالتدخل السريع.

4. تعزيز المراقبة والغستجابة للحوادث

- تدريبات الإستجابة للحوادث بانتظام:

إجراء تدريبات بإنتظام لضمان إسـتعداد فـرق الإســـتجابة للحـــوادث للتعامـــل مـــع السيناريوهات الواقعية بكفاءة.

5. التنسيق والمساءلة مع مقدمي الأنظمة

- تعزيز الشراكات مع البائعين:

تحسين التنسيق مع البائعين الخارجيين لضمان أن تكون تحديثاتهم موثوقة ومختبرة بشكل كافٍ.

- مساءلة البائعين:

وضع إجراءات مساءلة واضحة مع البائعين لضمان حل المشكلات بسرعة والتواصل الفعّال أثناء الحوادث.

تجربة شخصية

في الماضي، عملت في شركة توفر برامج مكافحة الفيروسات بالإضافة إلى اجهزة أمن الشبكات الأخرى.ومعظم عملائنا كانوا بنوك وكبرى الشركات السودانية. كنت أقوم بإختبار برنامج مكافحة الفايروسات للتأكد من عدم تأثيرها السلبي على الأنظمة الحساسة. كانت هذه الإجراءات تتضمن تنزيل البرنامج على أكثر الأجهزة حساسية ويحتوي على أكبر عدد من البرامج وإختبارها بدقة، ثم تخصيص الإعدادت لتتناسب مع هذه البرامج و عمل إستثناءات لضمان عدم مسح أي من مكونات البرنامج. ومن ثم سحب هذه الإعدادات و تعميمها على كل أجهزة الشبكة التي تكون بآلاف عند بعض العملاء.

كنت أبقى على إتصال دائم مع العميل لمعالجة أي مشاكل فور حدوثها، لضمان إستقرار النظام وإستمرارية العمل.

الخلاصة

يعد الإنقطاع الأخير لخدمات مايكروسوفت تذكيرًا صارخًا بتعقيدات ومخاطر العمليات التقنية العالمية. من خلال تنفيذ هذه التدابير الإستراتيجية، يمكن للمنظمات تعزيز مرونتها بشكل كبير، وتقليل تأثير الحوادث المستقبلية، وضمان استمرارية خدماتها.

أثر إنقطاع الإنترنت على القطاع المالي والمصرفي:
كيف يمكن الإستعداد للمستقبل

محمد الخير
خبير الخدمات المالية والرقمية

تابعنا أول أمس الخبر الصادم والخاص بالعطل الذي تعرضت له شركة CrowdStrike الأمريكية، وهي شركة متخصصة في الأمن السيبراني تعمل على حماية قطاعات واسعة في جميع أنحاء العالم من المتسللين والإنتهاكات الخارجية. وفقًا للمعلومات المتاحة، حدث العطل أثناء تنفيذ الشركة لتحديث إلزامي روتيني، مما أدى إلى تعطل الأجهزة التي تعمل بنظام التشغيل Microsoft Windows.

ربما يكون من السابق لأوانه التكهن بحجم الخسائر المادية التي تكبدتها الدول والمؤسسات المالية المختلفة ولكن من المؤكد أن الأضرار الإقتصادية كبيرة وتصل إلى مليارات الدولارات، خاصة وأنها تشمل مختلف قطاعات الإقتصاد العالمي.

يُعتبر القطاع المصرفي من أكثر القطاعات التي تضررت من هذا العطل نظرًا لأهمية القطاع وإعتماده الكبير على حياة الناس اليومية والمعاملات المالية التي تتم بشكل يومي وبالإعتماد الكامل على خدمة الإنترنت.

تأثير إنقطاع خدمة الإنترنت على القطاع المصرفي

يعتبر الإنترنت عنصرًا حيويًا في العمليات المصرفية الحديثة، وإنقطاع خدمة الإنترنت يمكن أن يؤثر بشكل كبير على القطاع المصرفي بعدة طرق ، من أهم التأثيرات المحتملة:

1. توقف الخدمات الإلكترونية

- المدفوعات الإلكترونية: يتوقف العملاء عن القدرة على إجراء المدفوعات عبر الإنترنت، مما يؤثر على المعاملات اليومية.
- التحويلات المصرفية: تتوقف عمليات التحويل بين الحسابات والتي تعتمد بشكل كبير على الإنترنت.

2. تعطيل العمليات الداخلية

- إدارة الحسابات: تعتمد البنوك على الأنظمة المترابطة عبر الإنترنت لإدارة الحسابات وتتبع المعاملات، وإنقطاع الخدمة يعطل هذه العمليات.
- الإتصال بين الفروع وأجهزة الصراف الألي : يعتمد التواصل بين الفروع المختلفة على الإنترنت، مما يؤثر على التنسيق والعمل اليومي.

- عمليات المقاصة اليومية : من المؤكد أن توقف خدمة الإنترنت قد يتسبب في تعطيل عملية مقاصة الشيكات بين البنوك المختلفة الأمر الذي من شأنه أن يخلق ربكة كبيرة في أسواق المال نسبة لعدم مقدرة الشركات والتجار بتحصيل قيمة الشيكات المستحقة نتيجة لإنقطاع الخدمة.

3. تأثير على العملاء

- عدم القدرة على الوصول إلى الحسابات: يعجز العملاء عن الوصول إلى حساباتهم عبر الخدمات البنكية الإلكترونية، مما يسبب الإزعاج ويزيد من الحاجة للذهاب إلى الفروع.
- العملاء الدوليون: يعاني العملاء الذين يعتمدون على التحويلات الدولية من تأخير في المعاملات.

4. خسائر مالية

- فقدان الإيرادات: توقف الخدمات الإلكترونية يؤدي إلى فقدان البنوك للإيرادات التي تُجنى من الرسوم على الخدمات المصرفية الإلكترونية.
- تكاليف إضافية: قد تتحمل البنوك تكاليف إضافية لإصلاح الأنظمة أو اللجوء إلى بدائل مؤقتة.

5. تأثير على الثقة

- ثقة العملاء: يتأثر مستوى الثقة لدى العملاء في المؤسسة المالية بسبب عدم الاستقرار في الخدمات.
- سمعة البنك: تتضرر سمعة البنك إذا تكرر إنقطاع الخدمة، مما يؤدي إلى فقدان العملاء الحاليين وصعوبة جذب عملاء جدد.

6. الأمن السيبراني

زيادة المخاطر: يمكن أن يؤدي إنقطاع الإنترنت إلى زيادة المخاطر السيبرانية إذا كانت البنوك تستخدم حلولاً مؤقتة غير آمنة لإستعادة الخدمة.

7. التأثير على الأسواق المالية :

- تأخير المعاملات:يؤثر على المعاملات في أسواق المال والبورصة حيث تعتمد العديد من العمليات على الإتصال الإلكتروني الفوري.
- التداول الإلكتروني: يتوقف التداول الإلكتروني الذي يعتمد عليه العديد من المستثمرين والبنوك.

الحلول المقترحة لتقليل تأثير إنقطاع الإنترنت مستقبلاً :

لقد أصبحت خدمة الإنترنت بمثابة العمود

الفقـري لضـمان إسـتمرارية العديـد مـن الخدمات في القطاعات المختلفة ويعتبر قطاع الخدمات المالية المصرفية من أهمها ،بطبيعة الحـال لا توجـد وصـفة يمكـن أن تمنـع الأثـار السـالبة لأنقطـاع خدمـة الإنترنـت بشـكل تـام ولكـن تظـل هنالـك عـدد مـن الخطـوات والترتيبـات التـي يمكـن أن تقلـل مـن تـأثير إنقطـاع الإنترنـت علـى القطاعـات الحيويـة كالقطاع المصرفي.

وضمان إستمرارية الخدمات الهامة ومن أهـم هذه الخطوات :

1. تطوير بنية تحتية متينة:

- الإسـتثمار فـي بنيـة تحتيـة شـبكية متقدمـة وموثوقة لضمان إسـتمرارية الخدمـة وتقليـل فرص الإنقطاع.
- إسـتخدام تقنيـات الشـبكات الإحتياطيـة لضمان وجود بدائل جاهزة في حال حدوث أي إنقطاع.

2. أنظمة إحتياطية متقدمة :

- تطـوير وتطبيـق أنظمـة إحتياطيـة يمكنهـا العمـل بشـكل مسـتقل فـي حـال إنقطـاع الإنترنت لضمان إستمرار العمليات الحيوية.
- إجـراء إختبـارات دوريـة علـى هـذه الأنظمـة للتأكد من جاهزيتها وقدرتها على العمـل فـي حالات الطوارئ.

3. تعزيز أنظمة الأمن السيبراني :

- تعزيز الإجراءات الأمنية لحماية الأنظمـة مـن الهجمـات السـيبرانية، خاصـة فـي أوقـات الاعتماد على حلول مؤقتة.
- تنفيذ برامج تدريبية دورية لموظفي الأمن السـيبراني للتعامـل مـع السـيناريوهات الطارئة.

4. تطبيق إستراتيجيات التعافي السريع :

- وضـع خطـط إسـتعادة الخدمـة السـريعة والتأكد من توفر الموارد اللازمة لتنفيذها عند الحاجة.
- تحديد فرق عمل مختصة للتعامل مع حـالات الإنقطاع وضمان إستعادة الخدمة بأسرع وقت ممكن.

5. الإعتماد على مزودي خدمة متنوعين :

- الإعتماد على أكثـر مـن مـزود خدمـة إنترنـت لضمان توفير بـدائل فوريـة فـي حـال تعطـل أحدهم.
- تنويـع مـزودي الخـدمات لضـمان تغطيـة جغرافية واسعة وخدمات متعددة.

6. التعاون مع الجهات الحكومية والخاصة :

- تعزيز التعاون مع الجهات الحكومية والخاصة لتحسين البنية التحتية العامة للإنترنت وتطوير سياسات وإجراءات التعامل مع حالات الإنقطاع.
- المشاركة في المبادرات الوطنية والإقليمية لتعزيز إستقرار وإستمرارية خدمات الإنترنت.

7. تحسين البروتوكولات والتقنيات المستخدمة :

- إعتماد تقنيات حديثة مثل شبكات الجيل الخامس (G5) وتقنيات الألياف البصرية لزيادة السرعة والإستقرار.
- تطوير وتحسين البروتوكولات المستخدمة في إدارة الشبكات لضمان الكفاءة والأمان.

8. إستثمار في تكنولوجيا الحوسبة السحابية:

- إستخدام خدمات الحوسبة السحابية لضمان توافر البيانات والخدمات المصرفية حتى في حالة إنقطاع الإنترنت في المقرات المحلية.
- ضمان توافر نسخ إحتياطية من البيانات على السحابة لتسهيل إستعادة الخدمة.

9. تعزيز التدريب والتوعية:

- تدريب الموظفين على التعامل مع حالات الطوارئ والإنقطاع وكيفية إستمرارية الأعمال في مثل هذه الظروف.
- توعية العملاء حول الإجراءات الواجب إتباعها في حالة إنقطاع الإنترنت لضمان إستمرار حصولهم على الخدمات المصرفية الضرورية.

أثر الأعطال التقنية على خدمة العملاء

آن محمد
محلل أعمال
مدير خدمة العملاء

عانت العديد من الشركات من مشاكل تقنية في أنظمة Microsoft Office، والتي أثرت بشكل كبير على كفاءة خدمات العملاء عبر الهاتف ووسائل خدمات التواصل الإجتماعي. أدت هذه المشاكل إلى إنقطاعات في الخدمة، تأخير في معالجة الطلبات وزيادة في معدلات الشكاوى، مما أثر سلبًا على رضا العملاء وثقتهم.

كيف أثرت هذه المشاكل على خدمات العملاء؟

1. تأخير في الإستجابة: عندما تتعطل أنظمة Microsoft Office، يجد الموظفون صعوبة في الوصول إلى الوثائق والبيانات الحيوية اللازمة لمعالجة إستفسارات العملاء بشكل سريع. هذا يؤدي إلى زيادة وقت الإنتظار للعملاء ويقلل من كفاءة الخدمة المقدمة.
2. تعطيل العمليات اليومية: تعتمد العديد من الشركات على Office لتسيير عملياتها اليومية، بما في ذلك إدارة البريد الإلكتروني، إعداد التقارير وجدولة الإجتماعات. أي عطل في هذه الأنظمة يمكن أن يؤدي إلى تداخل كبير في سير العمل.
3. زيادة معدلات الشكاوى: مع زيادة وقت الإنتظار وصعوبة الوصول إلى المعلومات، يشعر العملاء بالإحباط ويزيد عدد الشكاوى. هذا يؤثر سلبًا على سمعة الشركة وقدرتها على الحفاظ على رضا العملاء.
4. فقدان البيانات: في بعض الحالات، قد تؤدي مشاكل البرمجيات إلى فقدان البيانات المهمة أو عدم القدرة على الوصول إليها، مما يعقد الأمور أكثر.

كيفية تفادي تأثير هذه المشاكل في المستقبل؟

1. تحديث الأنظمة بإنتظام: من الضروري تطبيق جميع تحديثات الأمان والبرمجيات بإنتظام لضمان حماية الأنظمة من الثغرات التقنية والهجمات السيبرانية. تأكد من أن لديك فريق تقني مخصص لمتابعة هذه التحديثات وتطبيقها بشكل فوري.
2. إعداد خطط للطوارئ: تجهيز خطط بديلة للتعامل مع الإنقطاعات التقنية المفاجئة. يمكن أن تشمل هذه الخطط إستخدام أدوات بديلة أو الإنتقال إلى أنظمة إحتياطية لضمان إستمرار تقديم الخدمات بدون إنقطاع.

3. تدريب الموظفين: تدريب الموظفين على إستخدام الأدوات البديلة وتوفير دورات تدريبية حول كيفية التعامل مع حالات الطوارئ التقنية بكفاءة. هذا يساعد في تقليل وقت التعطل وزيادة الإستجابة السريعة للمشاكل.

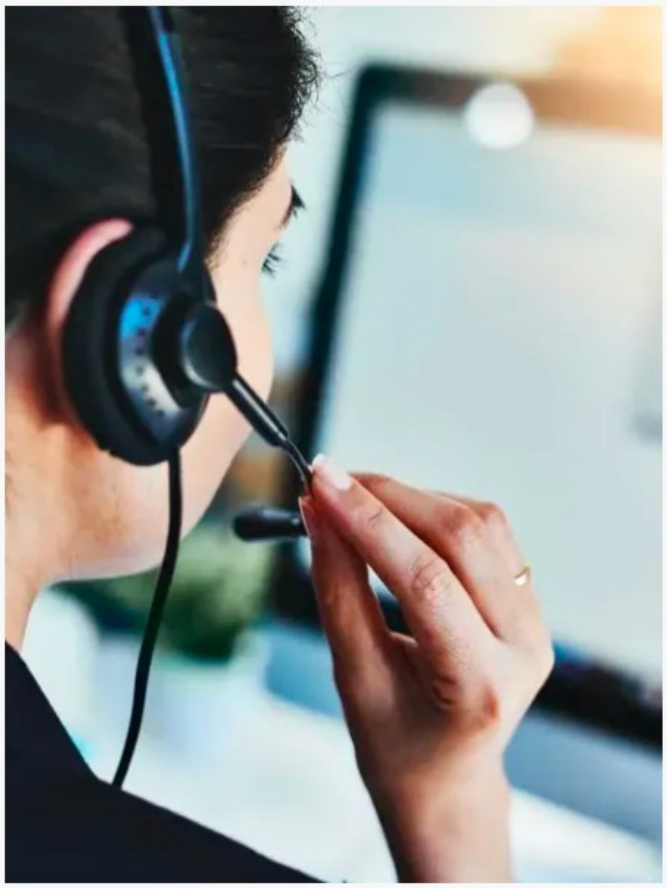
4. النسخ الإحتياطي: إعتماد أنظمة نسخ إحتياطي منتظمة للبيانات لضمان عدم فقدان المعلومات المهمة. يجب أن تكون هذه الأنظمة قابلة للوصول بسهولة في حالات الطوارئ.

5. التواصل الفعّال مع مزودي الخدمة: الحفاظ على تواصل دائم مع مزودي الخدمات التقنية للحصول على دعم فوري عند الحاجة. يمكن أن يساعد وجود عقود دعم فني على تسريع عملية حل المشاكل التقنية.

6. مراجعة وتقييم الأنظمة بإنتظام: إجراء مراجعات دورية وتقييمات شاملة للأنظمة التقنية لتحديد نقاط الضعف والتحسين المستمر. يمكن أن يشمل ذلك إجراء إختبارات منتظمة للتأكد من جاهزية الأنظمة للتعامل مع أي طارئ.

إستنتاج

بتطبيق هذه الإجراءات الوقائية، يمكن للشركات تعزيز إستقرار خدمات العملاء وتحسين تجربتهم بشكل كبير. تضمن هذه الخطوات الحفاظ على رضا العملاء وثقتهم، حتى في ظل وجود تحديات تقنية غير متوقعة. الشركات التي تستثمر في تحسين بنيتها التحتية التقنية وتدريب موظفيها تكون أكثر قدرة على مواجهة المشاكل التقنية بفعالية وتقليل تأثيرها على العملاء.



لخدمة العملاء عبر الهاتف:

- توفير أدوات إحتياطية: إستخدام برامج بديلة لإدارة المكالمات والبيانات لضمان إستمرار الخدمة أثناء تعطل Office.
- تدريب متخصص: توفير تدريب مستمر للموظفين حول كيفية التعامل مع الإنقطاعات التقنية وضمان قدرتهم على الوصول إلى المعلومات بطرق بديلة.
- التواصل السريع: إنشاء قنوات إتصال مباشرة مع فريق الدعم التقني لحل المشاكل بشكل سريع وتقليل التأثير على العملاء.

لخدمة العملاء عبر وسائل التواصل الإجتماعي:

- إستخدام منصات متعددة: التأكد من أن فريق خدمة العملاء يمكنه الوصول إلى حسابات الشركة عبر منصات متعددة خارج Office، مثل الهواتف الذكية والتطبيقات الخاصة بوسائل التواصل.
- إدارة الأزمات : تطوير استراتيجيات إدارة الأزمات الرقمية لضمان التواصل الفعّال والسريع مع العملاء خلال فترات التعطل.
- تحديثات منتظمة : نشر تحديثات منتظمة عبر وسائل التواصل الاجتماعي لإبقاء العملاء على اطلاع بأي مشاكل تقنية وتأثيراتها المحتملة.

بتطبيق هذه الإجراءات الوقائية، يمكن للشركات تعزيز إستقرار خدمات العملاء عبر الهاتف ووسائل التواصل الاجتماعي، مما يحسن من تجربتهم ويضمن رضاهم وثقتهم بالشركة حتى في ظل وجود تحديات تقنية غير متوقعة.

إستراتيجيات لحماية سلاسل الإمداد العالمية:
دروس من أزمة مايكروسوفت

إيناس أحمد
خبير سلاسل الإمداد

مقدمة:

في الأيام القليلة الماضية، تعرضت مايكروسوفت لهجوم سيبراني واسع النطاق أدى إلى تعطيل العديد من خدماتها السحابية والبرمجية. أثر هذا الهجوم بشكل كبير على العديد من الشركات والمؤسسات حول العالم، مما أدى إلى توقف العمليات وتأخير الإنتاجية. في هذا المقال، سنستعرض تفاصيل الأزمة، الجهات المتضررة، والتدابير الناجحة لتفادي مثل هذه الأزمات في المستقبل.

تفاصيل الأزمة:

في 18 يوليو 2024، تعرضت مايكروسوفت لهجوم سيبراني إستهدف خدماتها السحابية Microsoft Azure ومنصة الإنتاجية Office 365. تسبب هذا الهجوم في تعطل العديد من الخدمات الحيوية التي تعتمد عليها الشركات والمؤسسات في إدارة عملياتها اليومية.

1. تأثير الأزمة على سلاسل الإمداد:

- **إنقطاع الخدمات السحابية**: تسبب الهجوم في إنقطاع خدمات Azure في مناطق رئيسية مثل أمريكا الشمالية وأوروبا وآسيا. أشارت التقارير إلى أن حوالي 25,000 شركة واجهت تعطلاً في خدماتها السحابية، مما أدى إلى توقف العمليات وتأخير تلبية طلبات العملاء.
- **تعطل البرمجيات**: توقف خدمات Office 365 أثر على تواصل الفرق والعمل التعاوني في العديد من الشركات. تقارير من شركات في الولايات المتحدة وكندا وألمانيا وفرنسا أظهرت أن أكثر من 10,000 مؤسسة تأثرت بتوقف الخدمات، مما أدى إلى تأخير المشاريع وتراجع الإنتاجية.

2. الجهات المتضررة:

· الولايات المتحدة: شهدت العديد من الشركات الكبرى في قطاع التكنولوجيا والتصنيع تعطلاً كبيرًا، بما في ذلك شركات مثل Tesla و General Electric. توقف الخدمات السحابية أثر على عمليات التصنيع والإدارة الرقمية، مما أدى إلى خسائر مالية تقدر بملايين الدولارات.

· أوروبا: في ألمانيا، تعطلت عمليات شركات السيارات الكبرى مثل BMW و Volkswagen، حيث تعتمد هذه الشركات بشكل كبير على خدمات Azure في إدارة سلسلة التوريد والتصنيع.

· آسيا: في اليابان، تأثرت شركات الإلكترونيات مثل Sony و Panasonic، حيث تسبب توقف الخدمات السحابية في تعطيل إدارة البيانات وخطوط الإنتاج.

3. دروس مستفادة لتعزيز سلاسل الإمداد:

· تنويع البنية التحتية السحابية: يجب على الشركات تنويع مزودي الخدمات السحابية. تبني إستراتيجية هجينة تشمل إستخدام حلول سحابية مختلفة يمكن أن يقلل من الإعتماد على مزود واحد، مما يعزز المرونة في مواجهة الأزمات.

· تعزيز الأمن السيبراني: من الضروري تعزيز أنظمة الأمن السيبراني وتطبيق بروتوكولات صارمة لحماية البيانات والأنظمة من الهجمات. يجب تنفيذ تدابير مثل التشفير، والتحقق الثنائي، والتحديثات الأمنية المنتظمة.

· تطوير خطط استمرارية الأعمال: يجب أن يكون لدى الشركات خطط طوارئ واستمرارية الأعمال لمواجهة أي أزمات مفاجئة. تشمل هذه الخطط تحديد العمليات الحيوية، وتأمين النسخ الإحتياطية للبيانات، وتدريب الفرق على الإستجابة السريعة.

4. الحلول الناجحة لتفادي الأزمات المستقبلية:

· الإستثمار في التكنولوجيا المتقدمة: تبني تقنيات مثل الذكاء الاصطناعي والتحليلات المتقدمة يمكن أن يساعد في التنبؤ بالأزمات والإستجابة لها بشكل أسرع وأكثر فعالية.

· الشراكات الإستراتيجية: تعزيز التعاون مع الشركاء والموردين يمكن أن يساهم في تبادل الموارد والخبرات، مما يساعد في تجاوز الأزمات بشكل أكثر سلاسة.

· المرونة التنظيمية: يجب على الشركات تطوير هيكل تنظيمي مرن يمكنه التكيف مع التغيرات السريعة والإستجابة الفعالة للأزمات.

خاتمة:

أزمة مايكروسوفت الأخيرة تسلط الضوء على أهمية الإستعداد والتخطيط المسبق لمواجهة الأزمات في سلاسل الإمداد. من خلال تعلم الدروس المستفادة وتطبيق الحلول الناجحة، يمكن للشركات تعزيز مرونتها وضمان إستدامة عملياتها في مواجهة التحديات المستقبلية. دعونا نستفيد من هذه التجربة لتعزيز سلاسل الإمداد وتحقيق نجاحات مستدامة.

خطة إستمرارية الأعمال
Business Continuity Plan
ومايمكن أن تقدمه خلال أوقات الأزمات

م. أحمد تاج السر
خبير تحليل الاعمال والبنية المؤسسية

خطة إستمرارية الأعمال هي مجموعة من الإستراتيجيات والإجراءات التي تُعدّها المؤسسات لضمان إستمرار العمليات الأساسية والخدمات في حالات الطوارئ أو الكوارث.

إليكم اولاً خطوات وإستراتجيات خطة إستمرارية الأعمال:

1. تحديد الأهداف

- توضيح الأهداف: تحديد الأهداف الرئيسية لخطة إستمرارية الأعمال، مثل الحفاظ على العمليات الحيوية وتقليل وقت إنقطاع الخدمات...الخ.
- مواءمة الأهداف: التأكد من أن الأهداف تتماشى مع الإستراتيجيات العامة للمنظمة ومصالحها.

2. تقييم المخاطر

- تحديد المخاطر: إجراء تحليل شامل لتحديد المخاطر المحتملة التي قد تؤثر على الأعمال، مثل الكوارث الطبيعية (الزلازل، الفيضانات)، التهديدات السيبرانية (الهجمات الإلكترونية)، والأزمات الداخلية (فشل النظام).
- تحليل التأثير: تقييم التأثير المحتمل لكل نوع من المخاطر على الأعمال. يشمل ذلك تقدير مدى تأثيرها على العمليات المالية والتشغيلية.

3. تحديد الوظائف الحيوية

- تحديد العمليات الأساسية: تحديد الوظائف والعمليات الأساسية التي تعتبر حيوية لإستمرار النشاط التجاري.
- تحديد أولويات الإستمرارية: تصنيف هذه العمليات حسب الأولوية لتحديد كيفية إستعادتها في حالة حدوث إنقطاع.

4. إستراتيجيات الإستجابة

- تطوير إستراتيجيات الإستجابة: وضع إستراتيجيات محددة للتعامل مع أنواع مختلفة من الإضطرابات، بما في ذلك إستراتيجيات التعافي والتعويض.
- إجراءات الإستجابة: تطوير إجراءات مفصلة للتعامل مع حالات الطوارئ، مثل إخلاء المكاتب، تحويل العمليات إلى مواقع بديلة، أو إستعادة الأنظمة التكنولوجية.

5. تخصيص الموارد

- تحديد الموارد: تحديد الموارد اللازمة لتنفيذ إستراتيجيات الإستجابة، بما في ذلك الموارد البشرية (مثل فرق الطوارئ)، والتكنولوجية (مثل أنظمة النسخ الإحتياطي)، والمادية (مثل معدات الطوارئ).
- تخصيص الموارد: التأكد من تخصيص الموارد بشكل كافٍ لضمان إستمرارية العمل خلال الأزمات.

6. التدريب والإختبار

- تدريب الموظفين: إجراء تدريبات دورية للموظفين لضمان معرفتهم بدورهم في تنفيذ خطة الإستمرارية.
- إختبار الخطة: إجراء إختبارات منتظمة للخطة للتأكد من فعاليتها وتحديد أي ثغرات تحتاج إلى تحسين.

7. مراجعة وتحديث الخطة

- مراجعة دورية: مراجعة الخطة بإنتظام لتحديثها بما يتماشى مع التغيرات في بيئة العمل، التغيرات التكنولوجية، والأحداث الجديدة.
- تحسين مستمر: إجراء تحسينات مستمرة بناءً على نتائج الإختبارات والتدريبات والتغييرات في المخاطر.

لا ننسى طبعاً حساب تكلفة الحلول مقارنة مع تكلفة الخسائر المترتبة بعد حدوث المخاطر. كما يجب أيضاً التأكد من تقدير الحلول بناءً على المعلومات المتوفرة لتحقيق التوازن الأمثل بين التكلفة والفعالية. في بعض الحالات، قد تكون الكوارث نادرة الحدوث وتكلفة الحلول باهظة للغاية، مما يجعل من غير الممكن أو غير العملي تطوير خطة تفصيلية مسبقة لكل نوع من المخاطر. في مثل هذه الحالات، كما يمكن إتباع منهجية "الصدمة"، حيث يتم التعامل مع الكارثة بعد وقوعها بناءً على التجربة والتعلم من الوضع الفعلي، كما حدث مثلاً خلال أزمة كورونا. يتيح هذا النهج للمنظمات الإستجابة بسرعة ومرونة للمواقف غير المتوقعة، مما قد يكون أكثر عملية من تطوير خطط مفصلة لكل إحتمال نادر.

الخلاصة

كيف كان لخطة إستمرارية الاعمال أن تنقذ مطارات العالم من العطل الذي حصل في أنظمة التشغيل؟

الجواب: بعد الإستماع والتحليل للتفاصيل المتعلقة بالحادثة تبين أن العطل حدث بسبب تحديث أمني لأنظمة التشغيل الخاصة بشركة مايكروسوفت وأن كل المطارات التي قامت بتثبيت التحديث لم تقم بعملية إختبار للتحديث قبل إطلاقه في بيئة التشغيل.

فكان يجب أن تتضمن خطة إستمرارية الأعمال إختبار التحديثات في بيئة موازية (إختبارية) والتأكد من سلامة النظام ضد أي عيوب أو أعطال قد تعيق إستمرارية الأعمال وهذا الإجراء مطابق تماماً للاجراءات القياسية التي تقوم بها شركات البرمجيات أثناء تطوير وإختبار البرمجيات قبل إستخدامها.

ضمانات لإستمرارية عمل منصتك الرقمية

م. إبراهيم آدم
مطور الويب وتطبيقات الموبايل

لضمان إستمرارية عمل موقعك أو تطبيقك أو متجرك الإلكتروني دون إنقطاع، من الضروري إتباع عدة إستراتيجيات فعّالة.

أولاً، الإعتماد على إستضافة سحابية موثوقة توفر لك مرونة وتوافرية عالية.

ثانياً، إستخدام نظام تحميل متوازن يوزع الحمل على عدة سيرفرات، مما يمنع التحميل الزائد ويزيد من التوافرية.

ثالثاً، شبكات توصيل المحتوى (CDNs) تساهم في تسريع تحميل المحتوى وتقليل الضغط على السيرفرات الرئيسية.

بالإضافة إلى ذلك، النسخ الإحتياطية الدورية تضمن حماية البيانات وإسترجاعها في حالة الفقدان.

وأخيراً، تطبيق التحديثات الأمنية والبرمجية بإنتظام، مع إعداد خطة للطوارئ، يعزز من إستقرار النظام ويحافظ على إستمرارية الأعمال.

1. **الإستضافة السحابية (Cloud Hosting)**

الإستضافة السحابية هي إستخدام خدمات إستضافة تعتمد على الإنترنت حيث يتم تخزين الملفات والتطبيقات على خوادم متعددة متصلة بشبكة الإنترنت.

- كيف تعمل: تعتمد على شبكة من الخوادم المترابطة التي تعمل معًا لتوفير موارد الحوسبة مثل التخزين والمعالجة. عندما تقوم بإنشاء أو إستضافة موقع ويب أو تطبيق على السحابة، يتم توزيع الموارد المطلوبة على هذه الخوادم.

- **الفوائد:**

- التوسع المرن: يمكنك زيادة أو تقليل الموارد حسب الحاجة.

- التوافر العالي: تقلل من فترات التوقف حيث يتم توزيع الحمل على خوادم متعددة.

- الأمان: توفر مستويات عالية من الأمان والحماية ضد الهجمات السيبرانية.

2. نظام التحميل المتوازن (Load Balancer)

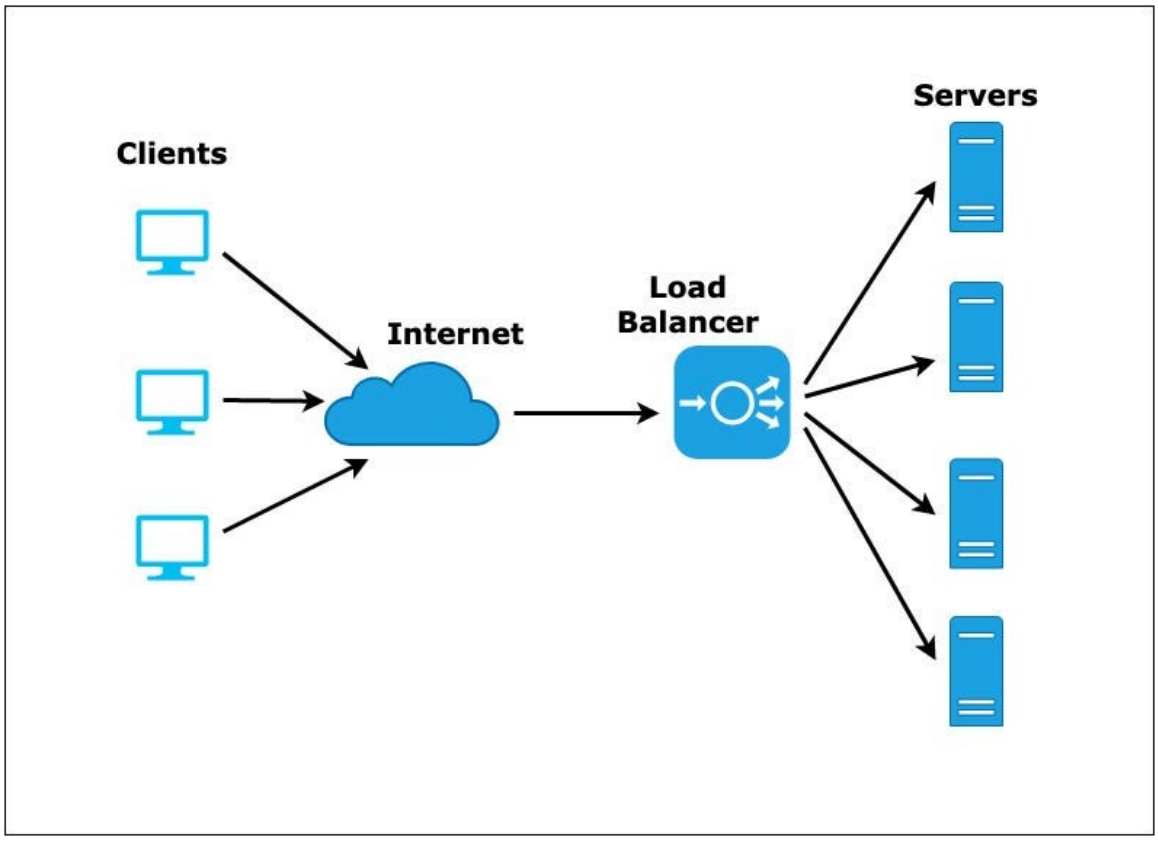
نظام التحميل المتوازن هو تقنية تستخدم لتوزيع حركة المرور عبر خوادم متعددة لضمان عدم تحميل سيرفر واحد بشكل زائد.

- كيف يعمل: عندما يصل طلب إلى الموقع، يقوم الموازن بإرساله إلى أحد الخوادم المتاحة بناءًا على قواعد محددة، مثل أقل سيرفر حملاً أو السيرفر الأقرب جغرافياً.

- **الفوائد:**

- توزيع الحمل: يمنع التحميل الزائد على سيرفر واحد.

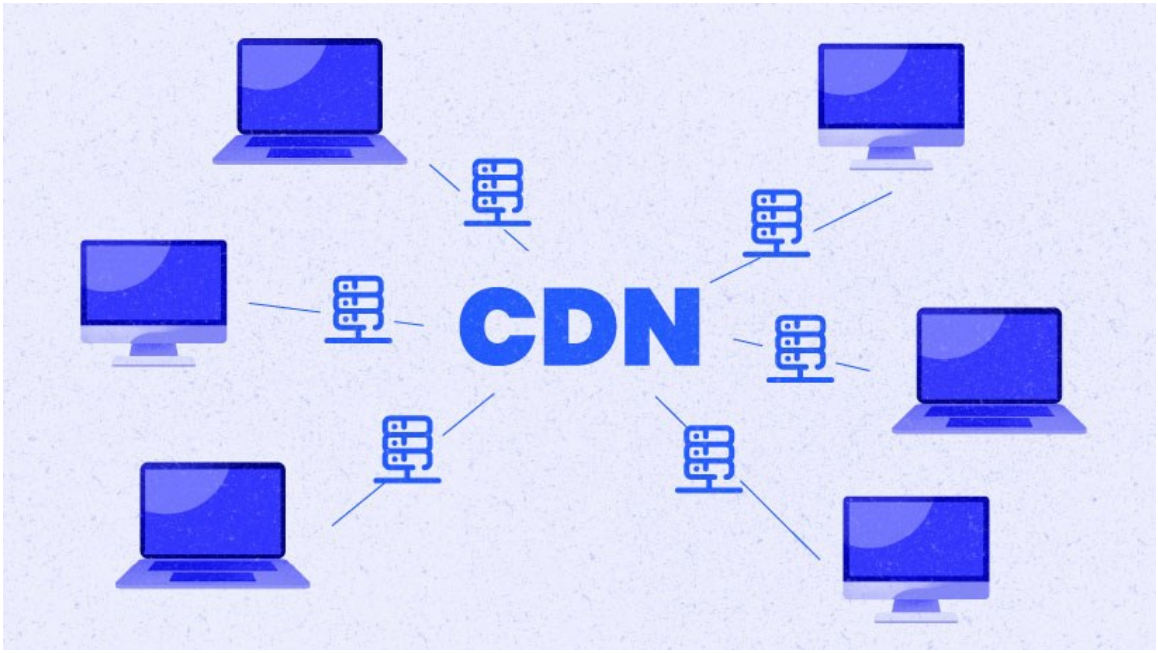
- التوافرية: يزيد من توافرية الموقع عن طريق توجيه الطلبات إلى السيرفرات العاملة في حالة فشل أحدها.



3. شبكات توصيل المحتوى (CDNs)

شبكات توصيل المحتوى هي نظام من الخوادم الموزعة جغرافياً تعمل على تسليم المحتوى للمستخدمين بناءً على موقعهم الجغرافي.

- كيف تعمل: تقوم بتخزين نسخ من المحتوى (مثل الصور والفيديوهات والملفات الثابتة) على خوادم موزعة حول العالم، مما يتيح تقديم المحتوى من أقرب خادم للمستخدم.
- **الفوائد:**
- تحسين سرعة التحميل: تقليل زمن التحميل من خلال تقديم المحتوى من أقرب موقع جغرافي للمستخدم.
- تقليل الحمل على السيرفرات: توزيع الطلبات على خوادم متعددة بدلاً من الإعتماد على السيرفر الرئيسي.



4 النسخ الإحتياطية الدورية (Regular Backups)

النسخ الإحتياطية الدورية هي عملية إنشاء نسخ إحتياطية من البيانات بإنتظام لحمايتها من الفقدان أو التلف.

- كيف تعمل: يتم إنشاء نسخ إحتياطية من البيانات والتطبيقات وتخزينها في موقع آمن. يمكن أن تكون النسخ الاحتياطية يومية، إسبوعية، أو شهرية حسب الحاجة.
- **الفوائد:**
- إسترجاع البيانات: يضمن إمكانية إستعادة البيانات في حالة فقدانها.
- المرونة: يمكنك إسترجاع النسخ الإحتياطية في أي وقت لضمان إستمرار العمل دون إنقطاع.

5. مراقبة الأداء والتنبيهات (Monitoring and Alerts)

مراقبة الأداء والتنبيهات هي عملية تتبع ومراقبة أداء الخوادم والتطبيقات وإرسال تنبيهات في حالة حدوث مشاكل.

- كيف تعمل: تعتمد على أدوات وبرامج مراقبة تجمع بيانات عن أداء النظام مثل سرعة الإستجابة، إستهلاك الموارد وسجلات الأخطاء. عند إكتشاف مشكلة، ترسل تنبيهات إلى الفريق التقني.

- **الفوائد:**

- كشف المشاكل: يوفر رؤية واضحة عن أداء السيرفرات والتطبيقات.
- الإستجابة السريعة: تنبيهات فورية عند حدوث مشاكل تتيح لك التدخل السريع قبل تفاقم الأمور.

6. التحديثات الأمنية والبرمجية (Security and Software Updates)

التحديثات الأمنية والبرمجية هي عملية تحديث البرامج والنظم لتضمين التحسينات الأمنية والوظائف الجديدة.

- كيف تعمل: تتضمن تثبيت أحدث الإصدارات من البرامج والنظم التي تستخدمها للحماية من الثغرات الأمنية وتحسين الأداء.

- **الفوائد:**

- حماية النظام: التحديثات الأمنية تحمي من الثغرات والتهديدات الجديدة.
- تحسين الأداء: التحديثات البرمجية توفر تحسينات في الأداء والموثوقية.

7. التخطيط للطوارئ (Disaster Recovery Plans)

التخطيط للطوارئ هو إعداد خطط لإسترجاع البيانات وإستمرار العمل في حالة حدوث كوارث تقنية.

- كيف تعمل: تشمل الخطط تحديد الإجراءات التي يجب إتباعها في حالة فشل النظام أو فقدان البيانات، مثل إستخدام النسخ الإحتياطية، تبديل الخوادم وإعادة تشغيل الأنظمة.

- **الفوائد:**

- ضمان الإستمرارية: خطط إسترجاع البيانات تساعد في إعادة تشغيل النظام بسرعة في حالة الكوارث.
- تقليل الفاقد: تضمن إستعادة البيانات وتقليل خسائر الأعمال.

HAMEEDOV™

carving ideas to art

Graphic Design

mohammed-hameedov

hameedov@gmail.com

+249 91 800 7781
+20 101 399 1857

www.hameedov.com

Key for Information Technolgy

عزز وجودك على الإنترنت مع خدمات تصميم وتطوير المواقع الاحترافية ..

www.k4-it.com

مجلة تحليل الأعمال

Business Analysis Magazine

أول مجلة عربية متخصصة في تحليل الأعمال