# خطة الاستجابة و التصعيد لمواجهة الهجمات السيبرانية

تم الإعداد بواسطة

## المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات

# المحتويات

# تأثير الحوادث السيبرانية

يجب إعطاء الأولوية للتعامل مع الهجمات السيبرانية بناء على العوامل التالية

- **الأثر الوظيفي للهجوم Functional Impact**
  - يؤثر الهجوم الذي يستهدف أنظمة تكنولوجيا المعلومات عادةً على الخدمات التي توفرها تلك الأنظمة، مما يؤدي إلى نوع من التأثير السلبي على مستخدمي تلك الأنظمة.
  - يجب تحديد أولوية التعامل مع الهجوم السيبراني بالنظر في كيفية تأثير الحادث على الخدمات الحالية والمستقبلية للأنظمة المتأثرة.

- **التأثير المعلوماتي للهجوم Informational Impact**
  - قد يؤثر الهجوم على سرية وسلامة وتوافر معلومات المؤسسة. يجب على معالجي الحوادث النظر في كيفية تأثير عملية سرقة المعلومات على المؤسسة.
  - قد يؤثر أي حادث يؤدي إلى سرقة معلومات حساسة أيضًا على المنظمات الأخرى.

الجمع بين التأثير الوظيفي للهجوم والتأثير المعلوماتي للهجوم يحدد تأثير وأولوية الهجوم.

# تقييم المخاطر السيبرانية

العنصرين الأساسيين لتقييم المخاطر:

- **الاحتمالية Likelihood**
  - الاحتمالية هي فرصة أو احتمال أن يستغل تهديد معين نقطة ضعف معينة.
  - العوامل التي تدخل في الاحتمالية تشمل أشياء مثل دوافع وقدرات المهاجم، ومدى سهولة استغلال الثغرة، ومدى حساسية الهدف المعرض للخطر.
  - في حالة وجود وسيلة استغلال لثغرة أمنية معينة، وكون المهاجم ماهرًا ومتحفزًا للغاية، والنظام المستهدف لديه القليل من عناصر الأمان، فاحتمالية حدوث الهجوم تكون مرتفعة. عندما يكون عكس أي من ذلك صحيحًا، تقل الاحتمالية.
- **التأثير Impact**
  - يصف التأثير الضرر الذي يمكن أن يلحق بالمؤسسة وأصولها إذا كان هناك تهديد محدد لاستغلال ثغرة أمنية معينة، ومن الواضح أن حساسية المعلومات والخدمات لبعض المؤسسات أكثر قيمة من غيرها حيث تعتبر بنية معلوماتية حرجة.

بافتراض وجود ثغرة أمنية وتهديد متطابقين، فمن الضروري النظر في كل من الاحتمالية والتأثير لتحديد مستوى الخطر.

توضح مصفوفة المخاطر البسيطة الموضحة في الشكل العلاقة بين الاثنين:

Impact

| Likelihood | LOW | MEDIUM | HIGH |
|---|---|---|---|
| HIGH | Medium risk (3) | High risk (4) | Highest risk (5) |
| MEDIUM | Low risk (2) | Medium risk (3) | High risk (4) |
| LOW | Lowest risk (1) | Low risk (2) | Medium risk (3) |

# الإجراءات التصعيدية لمواجهة الهجمات والاخطار السيبرانية

**في حالة حدوث هجوم سيبراني على اي من المؤسسات الخاصة بالدولة تكون الاجراءات كالتالي:**

- الابلاغ الفوري للمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات حال تحديد وقوع هجوم واتباع خطة التصعيد حسب تصنيف الخطورة للهجوم.
- تعيين مسؤول اتصال من داخل المؤسسة للإبلاغ والتواصل مع الاجهزة المعنية مع تحديد بديل له للحالات الطارئة.
- تحديد قنوات اتصال سريعة ومعتمدة مع توفير وسائل اتصال بديلة حال حدوث اي معوقات طارئة.
- تكوين فريق للتعامل المبدئي مع الهجوم والتعاون مع فريق الاستجابة للحوادث السيبرانية بالمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات ويحتوي هذا الفريق علي اخصائيين على دراية بالأنظمة والشبكة الخاصة بالمؤسسة.
- الاحتفاظ بالسجلات (log files) الخاصة بالخوادم وعناصر الشبكة لفترة زمنية لا تقل عن ستة أشهر والاحتفاظ بملفات السجلات (log files) المختلفة الخاصة بعناصر الشبكة على خادم مركزي خاص
- تزويد فريق المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات بملفات السجلات log files فورا حال وقوع الهجوم حتى يتمكن الفريق من تحليلها.
- اتباع اجراءات الاستجابة لأنواع الهجوم المختلفة المبينة لاحقا.

**ويتم تقسيم اجراءات الابلاغ التصعيدية حسب تصنيف الخطورة للهجوم على النحو التالي:**

- **تصنيف خطورة حرج (Critical)**

الابلاغ الفوري للمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات وللأجهزة السيادية للدولة على النحو التالي:

المؤسسة المتعرضة للهجوم

↓

فريق التعامل مع الحوادث السيبرانية بالمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات

↓

رئيس قطاع المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات

↓

نائب الامن السيبراني بالجهاز القومي لتنظيم الاتصالات

↓

رئيس الجهاز القومي لتنظيم الاتصالات

وزير الاتصالات وتكنلوجيا المعلومات

رئيس الوزراء – الأمين العام لوزارة الدفاع – الأمين العام للمخابرات العامة – المكتب الفني بوزارة الداخلية

- تكون جميع الفرق على أهبة الاستعداد On call.
- رفع حالة الاستنفار لمديري الشبكات وانظمة التأمين.
- عقد غرفة طوارئ على مدار الساعة تتكون من فريق المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات والفريق الخاص بالمؤسسة وممثلين الاجهزة السيادية بالدولة.
- التحرك الفوري لفريق المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات الى المؤسسة المستهدفة والعمل على احتواء الهجوم وتقديم تحديث دوري عن حالة الهجوم.

- **تصنيف خطورة عالي (high)**

ابلاغ المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات وللأجهزة السيادية للدولة في خلال يوم بحد أقصي على النحو التالي:

المؤسسة المتعرضة للهجوم

فريق التعامل مع الحوادث السيبرانية بالمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات

رئيس قطاع المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات

نائب الامن السيبراني بالجهاز القومي لتنظيم الاتصالات

رئيس الجهاز القومي لتنظيم الاتصالات

- تكون جميع الفرق على أهبة الاستعداد On call.
- رفع حالة الاستنفار لمديري الشبكات وانظمة التأمين.
- عقد غرفة طوارئ تقسم على ورديتين تتكون من فريق المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات والفريق الخاص بالمؤسسة.

- التحرك الفوري لفريق المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات الى المؤسسة المستهدفة والعمل على احتواء الهجوم وتقديم تحديث دوري عن حالة الهجوم.

- **تصنيف خطورة متوسط (medium) أو منخفض (Low)**
- ابلاغ المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات في خلال 1-3 ايام بحد أقصي على النحو التالي:

المؤسسة المتعرضة للهجوم

↓

فريق التعامل مع الحوادث السيبرانية بالمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات

↓

رئيس قطاع المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات

↓

نائب الامن السيبراني بالجهاز القومي لتنظيم الاتصالات

- يتابع فريق التعامل مع الحوادث السيبرانية بالمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات خطوات التعامل مع الهجوم من قبل المؤسسة.
- التحرك في خلال 1-3 ايام لفريق المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات الى المؤسسة المستهدفة والعمل على احتواء الهجوم حال الاحتياج.

# اجراءات الاستجابة لأنواع الهجمات المختلفة

- نظرا للتهديدات الحالية التي تواجه المؤسسات الحيوية والحرجة بالدولة فإن أنواع التهديدات الأكثر انتشاراً هي
  - هجمات تغيير وتشويه المحتوى (Web Defacement)
  - هجمات تعطيل وحجب الخدمات (DDoS)
  - انتشار البرمجيات الخبيثة وفيروس الفدية (Malware Infection, Ransomware)
  - هجمات التصيد الاحتيالي (Phishing)

- يتم الاستعداد للهجمات عن طريق اتخاذ التدابير والتوصيات في مختلف مراحل الهجوم التي تتمثل في التالي:

  - مرحلة الاستعداد (Preparation)
  - مرحلة تحديد الهجوم (Identification)
  - مرحلة احتواء الهجوم (Containment)
  - مرحلة المعالجة (Remediation)
  - مرحلة استعادة العمل بشكل طبيعي (Recovery)

- **هجمات تغيير وتشويه المحتوى (Web Defacement)**

**مرحلة الاستعداد (Preparation)**

تهدف خطوات هذه المرحلة إلى تحديد الاجراءات وقواعد تجميع البيانات التي تمكن المؤسسة من التعامل مع الهجوم حال وقوعه وتشمل:

- تحديث والاحتفاظ بقائمة الاتصال بالجهات المعنية حال وقوع الهجوم (مثل بالمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات، ومقدم الخدمة والجهات المذكورة في خطة التصعيد).
- إنشاء وتحديث مخططات (schemes) خاصة بالتطبيقات المتعلقة بخادم الويب من حيث اصدارات هذه التطبيقات وطريقة عملها وكيفية الاحتفاظ ببياناتها.
- انشاء مواقع احتياطية (backup websites)، هي نفس المواقع من حيث المحتوى، ولكن ذات عناوين (IP address) مختلفة.
- تحديد الإجراءات المطلوبة لإعادة توجيه الزائر إلى الموقع الاحتياطي.
- المتابعة المستمرة (ويمكن عن طريق أدوات المراقبة monitoring tools) لاكتشاف أي سلوك غير طبيعي على مواقع الويب الهامة بسرعة.
- عمل خطة لعزل قواعد البيانات المهمة عن باقي الخوادم حال اكتشاف اختراق او عند حدوث الهجمة.
- الاحتفاظ بالسجلات (log files) الخاصة بالخوادم وعناصر الشبكة لفترة زمنية لا تقل عن ستة أشهر.
- الاحتفاظ بملفات السجلات (log files) المختلفة الخاصة بعناصر الشبكة على خادم مركزي خاص centralized server.
- مزامنة التوقيت على كل الخوادم وعناصر الشبكة، حتى يتم تحليل السجلات والربط بينهم بصورة صحيحة.
- التأكد من وجود خريطة للشبكة بالكامل محدثة.

**مرحلة تحديد الهجوم (Identification)**

تهدف خطوات هذه المرحلة إلى كشف الحادث وتحديد نطاقه وإشراك الأطراف المناسبة وتشمل:

- متابعة قنوات الكشف المعتادة كمراقبة صفحات الويب.
- التحقق من سجلات الخادم.
- البحث في سجلات الوصول إل صفحة الويب وسجل الأخطاء عن أي نشاط مشبوه أو غير مألوف.
- التحقق من سجلات جدار الحماية IDS أوIPS ، إذا كانت متوفرة.
- فحص الملفات ذات المحتوى الثابت.
- فحص قواعد البيانات بحثا عن محتوى ضار.
- التحقق من الروابط الموجودة في الصفحة.
- الابلاغ الفوري للمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات حال تحديد وقوع هجوم واتباع خطة التصعيد حسب تصنيف الخطورة للهجوم.

**مرحلة احتواء الهجوم (Containment)**

تهدف خطوات هذه المرحلة إلى تخفيف آثار الهجوم وتتم مع اتباع ارشادات الم للمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات وتشمل:

- عزل الخوادم المخترقة.
- عمل نسخة تحليلية حيث تمكن فريق التحليل الجنائي الرقمي (Digital Forensics) من الوصول الى اسباب الاختراق.
- تحقق من موقع الثغرة الامنية التي تم من خلالها الهجوم.
- تحقق من عدم وجود الثغرة الأمنية التي استغلها المهاجم في مكان آخر بالشبكة.
- تحقق من النظام الذي يعمل عليه خادم الويب.
- تحقق من الاتصالات بالأنظمة الأخرى التي قد تكون تعرضت للهجوم أيضا.
- إذا كان مصدر الهجوم هو نظام آخر على الشبكة، فقم بعزله إن أمكن وتحقق منه.
- اكتشف الثغرة التي مكنت المهاجم من الدخول للنظام في المقام الأول وقم بإصلاحها.
- يتم اشراك الخوادم الاحتياطية التي تم تجهيزها مسبقا بنسخ مماثلة للمواقع المستهدفة وذلك إذا كانت غير معرضة للثغرة التي ادت للهجوم وبذلك يتم عودة الموقع إلى الخدمة في أسرع وقت وبالتالي تقليل الاثار السلبية المترتبة عن اختراق الموقع.
- يتم القيام بتعديلات في ال Policies الخاصة بأجهزة الحماية "حوائط نارية وموانع الاختراق" وذلك لسد الثغرة التي تم منها الاختراق.

**مرحلة المعالجة (Remediation)**

تهدف خطوات هذه المرحلة إلى ازالة اثار الهجوم وتجنب الهجمات المماثلة وتتم مع اتباع ارشادات الم للمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات وتشمل:

- إزالة كل المحتوى الذي تم تغييره واستبداله بالمحتوى الشرعي، الذي تمت استعادته من النسخة الاحتياطية السابقة بعد اكتشاف الثغرات ومعالجاتها.
- تأكد من أن هذا المحتوى خالٍ من الثغرات الأمنية.

**مرحلة استعادة العمل بشكل طبيعي (Recovery)**

تهدف خطوات هذه المرحلة إلى إعادة النظام العمل بشكل طبيعي وتتم مع اتباع ارشادات المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات وتشمل:

- العودة الى استخدام خادم الويب الاساسي بعد المعالجة، وتحديث المواقع الاحتياطية.
- الاستمرار في مراقبة الانشطة الخاصة بالموقع والبلاغ حال حدوث اي نشاط مشبوه يدل على حدوث اي قصور بعملية تحديد الهجوم والمعالجة.
- بعد انتهاء الهجمات يقوم المركز بإصدار تقارير عن نوعية وحجم الهجمات ونوعية البرمجيات المستخدمة بها وكيفية اتخاذ التدابير لاتقاء هذه النوعية من الهجمات مستقبليا على ان يتم عرض هذه التقارير على المؤسسة التي تعرضت للهجوم.

- **هجمات تعطيل وحجب الخدمات (DDoS)**

**مرحلة الاستعداد (Preparation)**

تهدف خطوات هذه المرحلة إلى تحديد الاجراءات وقواعد تجميع البيانات التي تمكن المؤسسة من التعامل مع الهجوم حال وقوعه وتشمل:

- قيام فريق العمل بالمركز الوطني للاستعداد الطوارئ الحاسبات والشبكات بمتابعة انشطة المجموعات الخاصة بالهجمات الالكترونية عن طريق متابعة نشرات الهجمات (Dark Web) والهاشتاج الخاصة بهذة المجموعات ومواقع التواصل الاجتماعي الخاصة بمجموعة المهاجمين على مدار الساعة لتحديد الأهداف المتوقعة للهجمات ونوعيتها

والبرمجيات المستخدمة بها والاحجام المتوقعة من حيث السعة والمصدر لهذه الهجمات.
- قيام فريق العمل بالمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات بالتنسيق مع الجهات المتوقع الهجوم عليها وذلك لوضع خطط للدفاع وامداد فرق تأمين الشبكات في هذه الجهات بتعليمات متابعة تصدي الهجمات وتشمل وجود دوريات على مدار الساعة لمتابعة هذه الهجمات وتحديث الحوائط النارية ومانعات التدخل بأحدث اصدارات مضادات الهجوم او بإصدارات خاصة لهذه النوعية من الهجمات مصممة عن طريق فريق المركز الوطني للاستعداد الطوارئ الحاسبات والشبكات الصد وتقليل فاعلية هجمات تعطيل الخدمات.
- التأكد من أن قدرة البنية التحتية بأكملها غير مقيدة بعدد واحد أو محدود من الموارد (نقطة فشل واحدة).
- إنشاء خدمات وبوابات إنترنت Internet gatewaysبديلة.
- إنشاء قوائم التحكم في الوصول Access Control Lists لتحديد أولويات حركة المرور داخل الشبكة.
- إعداد قنوات اتصال بديل على الخدمات الهامة باستخدام VPN.
- تطبيق تصفية حركة المرور الواردة والصادرة inbound and outbound traffic filtering واستخدام إعادة توجيه المسار العكسي (Reverse Path Forwarding)

**مرحلة تحديد الهجوم (Identification)**

تهدف خطوات هذه المرحلة إلى كشف الحادث وتحديد نطاقه وإشراك الأطراف المناسبة وتشمل:

- قيام فريق العمل بالمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات بالتنسيق مع الجهات المعرضة للهجمات لتحليل سجلات الشبكة أو الأهداف لمعرفة نوع ومصادر الهجمات واتخاذ الاجراءات الفنية للحد من تأثير هجمات تعطيل الخدمات.
- يقوم المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات بالتنسيق مع مقدمي خدمات الانترنت في جمهورية مصر العربية للحد من مصادر هجمات تعطيل الخدمات داخلياً وخارجياً.
- في حالة وجود هجمات بشكل مكثف يقوم فريق العمل بالمركز بمخاطبة الدول مصدر الهجمات عن طريق مراكز الاستعداد الطوارئ الحاسبات والشبكات المحلية لهذه الدول لوقف الهجمات او مع Data Centers مصدر الهجمات لمنع وايقاف هجمات تعطيل الخدمات.
- البحث عن أنماط حركة المرور داخل الشبكة لكشف الهجمات المعروفة ومقارنتها بحركة المرور الطبيعية داخل الشبكة.
- الابلاغ الفوري للمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات حال تحديد وقوع هجوم واتباع خطة التصعيد حسب تصنيف الخطورة للهجوم.
- الحصول على قائمة بعناوين IP المهاجمة عن طريق تتبعها في ملفات السجلات.

**مرحلة احتواء الهجوم (Containment)**

تهدف خطوات هذه المرحلة إلى تخفيف آثار الهجوم وتتم مع اتباع ارشادات الم للمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات وتشمل:

- تعديلات الشبكة :
  - التبديل إلى مواقع أو شبكات بديلة باستخدام DNS أو أي آلية أخرى.
  - توزيع حركة المرور الهجومية عبر شبكة من مراكز البيانات Data Centres.

- توجيه حركة المرور على خدمات ومنتجات معالجة هجمات حجب الخدمة (Traffic Scrubbers).
- في حالة استمرار الهجمات لفترة زمنية طويلة وتأثيرها على أي من الخدمات الحيوية يقوم المركز الوطني للاستعداد الطوارئ الحاسبات والشبكات بعد موافقة السلطة المختصة (السيد وزير الاتصالات وتكنولوجيا المعلومات والسيد رئيس الجهاز القومي لتنظيم الاتصالات) بإعطاء تعليمات مباشرة لمقدمي خدمات الانترنت في مصر بعزل عناوين الانترنت المعرضة للهجمات عن الاتصال بالخارج وذلك للحفاظ على هذه الخدمات الحيوية داخل جمهورية مصر العربية.

**مرحلة المعالجة (Remediation)**

تهدف خطوات هذه المرحلة إلى ازالة اثار الهجوم وتجنب الهجمات المماثلة وتتم مع اتباع ارشادات الم للمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات وتشمل:

- تحديد أولوية النطاق الترددي (Bandwidth) والحظر.
- رفض الاتصال بحسب المعلومات الجغرافية.
- رفض الاتصال القائم على IP والبصمة المشبوهة ( malicious IP's and traffic signatures).
- تنقية المرور داخل الشبكة Traffic Scrubbing عن طريق استخدام أجهزة ووحدات مخصصة مع أجهزة عالية الأداء.
- استخدام تقنية Sinkholing وهي تقنية تستخدم لإعادة توجيه حركة المرور الضارة من وجهتها الأصلية إلى خادم تحت سيطرة المدافع.

**مرحلة استعادة العمل بشكل طبيعي (Recovery)**

تهدف خطوات هذه المرحلة إلى إعادة النظام العمل بشكل طبيعي وتتم مع اتباع ارشادات الم للمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات وتشمل:

- التحقق من أن حركة المرور طبيعية بدون زيادات حادة. مع المتابعة لفترة زمنية بعد الهجوم لرصد اي نشاط غير طبيعي.
- التأكد من أن أداء البنية التحتية قد عاد إلى المقياس الطبيعي.
- بعد انتهاء الهجمات يقوم المركز بإصدار تقارير عن نوعية وحجم الهجمات ونوعية البرمجيات المستخدمة بها وكيفية اتخاذ التدابير لاتقاء هذه النوعية من الهجمات مستقبليا على ان يتم عرض هذه التقارير على المؤسسة التي تعرضت للهجوم.

- **انتشار البرمجيات الخبيثة وفيروس الفدية ( Ransomware or malware infection)**

**مرحلة الاستعداد (Preparation)**

تهدف خطوات هذه المرحلة إلى تحديد الاجراءات وقواعد تجميع البانات التي تمكن المؤسسة من التعامل مع الهجوم حال وقوعه وتشمل:

- تحديث التطبيقات وانظمة التشغيل بآخر تحديثات متوفرة.

- التوعية بعدم الدخول على اي روابط او مرفقات في رسائل البريد الالكتروني المرسلة من مصادر مجهولة.
- عمل نسخ احتياطية للبيانات في فترات دورية والاحتفاظ بها في جهاز منفصل وغير متصل بالإنترنت.
- استخدام القائمة البيضاء للتطبيق للسماح فقط للبرامج المعتمدة بالعمل على الشبكة.
- ضبط اعدادات الحوائط النارية لمنع وصول عناوين (IP Addresses) الخبيثة المعروفة.
- استخدام اجهزة خاصة لتصفية الرسائل غير المرغوب فيها لحماية الشبكة من التصيد الالكتروني بالتأكد من صحة مرسل الرسائل الالكترونية.

**تحديد الهجوم (Identification)**

تهدف خطوات هذه المرحلة إلى كشف الحادث وتحديد نطاقه وإشراك الأطراف المناسبة وتشمل:

- تحديد الاجهزة التي تم عليها الهجوم.
- حدد نوع (أنواع) البيانات الموجودة على الأجهزة أو مشاركات الملفات أو الأنظمة الأخرى التي يوجد بها اتصال مباشر.
- بناءً على هذه المعلومات، يحدد عدد الأجهزة المتأثرة خطورة الحادث.
- الابلاغ الفوري للمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات حال تحديد وقوع هجوم واتباع خطة التصعيد حسب تصنيف الخطورة للهجوم

**مرحلة احتواء الهجوم (Containment)**

تهدف خطوات هذه المرحلة إلى تخفيف آثار الهجوم وتتم مع اتباع ارشادات الم للمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات وتشمل:

- فصل جميع الأجهزة المصابة أو المشتبه فيها من الشبكة.
- عدم غلق الاجهزة وذلك حتى يتم الحفاظ وجمع الادلة والبيانات الموجودة في الذاكرة لتحليلها memory analysis.
- جمع ومراجعة الأدلة من مصادر أخرى .يمكن أن يشمل ذلك سجلات النظام وسجلات أجهزة الشبكة (جدران الحماية، وIDS، وما إل ذلك) .
- عمل نسخة تحليلية حيث تمكن فريق التحليل الجنائي الرقمي (Digital Forensics) من الوصول الى اسباب الاختراق.
- تحقق من موقع الثغرة الامنية التي تم من خلالها الهجوم.
- تحقق من عدم وجود الثغرة الأمنية التي استغلها المهاجم في مكان آخر بالشبكة.
- اكتشف الثغرة التي مكنت المهاجم من الدخول للنظام في المقام الأول وقم بإصلاحها.
- يتم القيام بتعديلات في ال Policies الخاصة بأجهزة الحماية "حوائط نارية وموانع الاختراق" وذلك لسد الثغرة التي تم منها الاختراق.

**مرحلة المعالجة (Remediation) ومرحلة استعادة العمل بشكل طبيعي (Recovery)**

تهدف خطوات هذه المرحلة إلى ازالة اثار الهجوم وتجنب الهجمات المماثلة وإعادة النظام العمل بشكل طبيعي تتم مع اتباع ارشادات المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات وتشمل:

- استعادة الانظمة من النسخ الاحتياطية السليمة والتأكد من عدم تعرضها للإصابة بالبرامج الضارة عن طريق فحصها وتحليلها.
- التأكد من معالجة الثغرات الأمنية التي ادت للإصابة بالبرامج الخبيثة.
- الاستمرار في متابعة الاجهزة المصابة بعد معالجتها لرصد أي نشاط غير طبيعي.
- بعد انتهاء الهجمات يقوم المركز بإصدار تقارير عن نوعية وحجم الهجمات ونوعية البرمجيات المستخدمة بها وكيفية اتخاذ التدابير لاتقاء هذه النوعية من الهجمات مستقبليا على ان يتم عرض هذه التقارير على المؤسسة التي تعرضت للهجوم.

## • هجمات التصيد الاحتيالي (Phishing attack)

### مرحلة الاستعداد (Preparation)

تهدف خطوات هذه المرحلة إلى تحديد الاجراءات وقواعد تجميع البيانات التي تمكن المؤسسة من التعامل مع الهجوم حال وقوعه وتشمل:

- أنشاء قائمة جهات اتصال المسؤولين عن إزالة صفحات التصيد الاحتيالي في:
  - شركات الاستضافة.
  - شركات التسجيل.
  - موفري خدمة البريد الإلكتروني.

- تعزيز برامج التدريب للمستخدمين داخل المؤسسة فيما يتعلق بهجمات التصيد المشتبه بها. قد تشمل المؤشرات الرئيسية المشبوهة لرسائل التصيد الاحتيالي ما يلي:

  - الأخطاء الإملائية في الرسالة أو الموضوع.
  - أسماء المرسلين المزيفة، بما في ذلك عدم التطابق بين اسم العرض وعنوان البريد الإلكتروني.
  - استخدام عناوين البريد الإلكتروني الشخصية للأعمال الرسمية (على سبيل المثال، رسائل البريد الإلكتروني Gmail أوyahoo.
  - الروابط الخبيثة أو المشبوهة.
  - تلقي بريد إلكتروني أو مرفق غير متوقع، ولكن من شخص معروف.
  - التأكد من أن موظفي تكنولوجيا المعلومات والأمن على اطلاع بآخر تقنيات التصيد الاحتيالي.
  -

### مرحلة تحديد الهجوم (Identification)

تهدف خطوات هذه المرحلة إلى كشف الحادث وتحديد نطاقه وإشراك الأطراف المناسبة وتشمل:

- تحديد العدد الإجمال ي للمستخدمينن المتأثرين.
- فهم اي اجراء تم بواسطة المستخدم ردا على رسالة البريد الإلكتروني المخادعة (على سبيل المثال، هل تم تنزيل المرفق، أو زيارة الموقع الاحتيالي، أو تقديم أي معلومات شخصية بيانات الدخول).
- **التحقق من:**
  - وسائل التواصل الاجتماع.
  - رسائل بريد إلكتروني يحتمل أن تكون مشبوهة.
  - رسائل البريد الإلكتروني التي تحتوي على روابط لعناوين URL خارجية وغير معروفة.
  - أي نوع من الإخطار بنشاط مشبوه.

- تحليل الرسالة المشبوهة باستخدام جهاز آمن (على سبيل المثال، عدم فتح الرسائل على جهاز له إمكانية الوصول إلى بيانات حساسة لأن الرسالة قد تحتوي على برامج ضارة).

- **تحديد التالي:**
  - متلقي الرسالة والمستهدف من الهجوم.
  - عنوان البريد الإلكتروني للمرسل.
  - عنوان الموضوع.
  - نص الرسالة.
  - المرفقات (لا تفتح المرفقات إلا وفق الإجراءات المتبعة).
  - الروابط والمجالات وأسماء المضيف.
  - البيانات الوصفية للبريد الإلكتروني بما في ذلك رؤوس الرسائل (email header).
  - جميع عناوين IPالخاصة بالعميل وخادم البريد.

- **تحليل الروابط والمرفقات:**
  - استخدام خدمات الاستطلاع المتاحة nslookup وwhois للعثور على عناوين IPومعلومات التسجيل.
  - ارسال الروابط والمرفقات الى المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات.

**مرحلة احتواء الهجوم (Containment)**

تهدف خطوات هذه المرحلة إلى تخفيف آثار الهجوم وتتم مع اتباع ارشادات الم للمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات وتشمل:

- تغيير بيانات اعتماد تسجيل الدخول لحسابات المتأثرة.
- تقليل الوصول إلى الخدمات أو الأنظمة أو البيانات الهامة حتى اكتمال التحقيق.
- إعادة فرض المصادقة متعددة العوامل (Multi factor authentication).
- اجراء حظر على مؤشرات الاختراق المكتشفة، على سبيل المثال:
  - حظر المجالات الضارة باستخدام DNSأو جدران الحماية.
  - حظر اي رسائل تتشابه مع كلا من النصوص الرسائل، والموضوعات، والروابط، والمرفقات المكتشفة.
  - إزالة الرسائل ذات الصلة من البريد الوارد للمستخدمين الآخرين، أو جعل الوصول إليها غير ممكن.

**مرحلة المعالجة (Remediation) ومرحلة استعادة العمل بشكل طبيعي (Recovery)**

تهدف خطوات هذه المرحلة إلى ازالة اثار الهجوم وتجنب الهجمات المماثلة وإعادة النظام العمل بشكل طبيعي تتم مع اتباع ارشادات المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات وتشمل:

- في حالة استضافة صفحات التصيد الاحتيالي على موقع ويب مخترق، حاول الاتصال بمالك الموقع بالتنسيق مع المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات حتى يتخذ

الإجراءات المناسبة: إزالة المحتوى الاحتيالي، والأهم من ذلك كله ترقية الأمان الموجود عليه، حتى لا يتمكن المحتال من العودة باستخدام نفس الثغرة الأمنية.

- في حالة وجود إعادة توجيه (غالبًا ما ينتقل الرابط الموجود في البريد الإلكتروني إلى عنوان URL لإعادة التوجيه)، قم أيضًا بإزالة إعادة التوجيه عن طريق الاتصال بالشركة المسؤولة عن الخدمة ويتم بالتنسيق مع المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات.
- في حالة الاستجابة تأكد من أن الصفحات أو عناوين البريد الإلكتروني الاحتيالية معطلة.
- استمر في مراقبة عنوان URL الاحتيالي. في بعض الأحيان، قد يظهر موقع ويب للتصيد الاحتيالي مرة أخرى بعد بضع ساعات. في حالة استخدام إعادة التوجيه وعدم إزالتها، استمر في مراقبتها.