هيئة تنظيم الاتصالات والحكومة الرقمية
TELECOMMUNICATIONS AND DIGITAL GOVERNMENT REGULATORY AUTHORITY

الدليل الإرشادي للجهات الاتحادية لتطبيق برامج صيد الثغرات الرقمية

تاريخ الإصدار: 2023

المحتويات

1. نبذة عامة

سعياً إلى تحقيق مئوية الإمارات 2071، ومواءمتها مع الاستراتيجية الوطنية لجودة الحياة 2031 وسياسة جودة الحياة الرقمية واستراتيجة الحكومة الرقمية 2025، وبناءً على قرار مجلس الوزراء رقم (2 و3) لسنة 2021 المتعلق باستراتيجية الخدمات الحكومية لدولة الإمارات والسياسات المرتبطة بها، ليعلن عن عهد جديد يتم فيه تقديم خدمات رقمية بنسبة 100%. تم تطوير هذا الدليل الإرشادي لبرنامج صائد الثغرات الرقمي لرفع الكفاءة الحكومية وتمكين واستدامة حكومة المستقبل الرقمية القائمة على اقتصاد المعرفة الرقمي، كمنظومة رقمية تكاملية تشمل المجتمع بتطوير وتحسين الخدمات الرقمية<

الغرض من هذا الدليل الإرشادي وضع منهجية مقترحة بمثابة مرجع لجميع الجهات الاتحادية في دولة الإمارات العربية المتحدة الراغبة بتطبيق برامج صيد الثغرات، ويقدم الدليل توصيات رئيسية بشأن تخطيط وتنفيذ خطة عمل نموذجية.

يهدف الدليل إلى تمكين الجهات الاتحادية من تحقيق التميز برفع مستوى جودة خدماتها الرقمية وتعزيز حضورها الرقمي، عبر تطوير برامج صيد الثغرات الرقمية، سعياً للتحسين المستمر للبيئة الممكنة للمعاملات الرقمية بشتى أنواعها، وتسهيل تقديم خدمات رقمية استباقية سلسة من أي مكان 24/7 للجمهور من خلال تجربة رقمية 100%، وحكومة لا ورقية عبر التصدي لأي ثغرات أمنية وتقنية إجرائية في قنوات تقديم الخدمات الرقمية.

2. ملخص تنفيذي

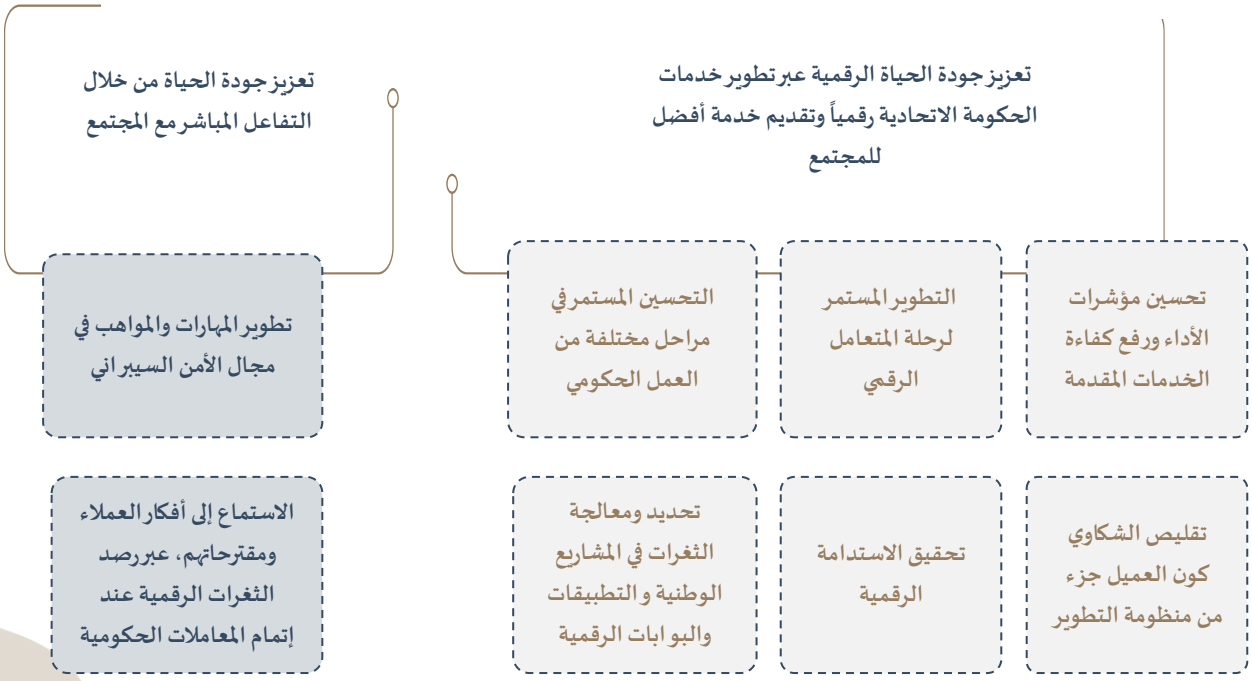
برامج صيد الثغرات هي مبادرات تعهيد جماعي تكافئ الأفراد على اكتشاف الثغرات في تطبيقات أو برامج معينة والإبلاغ عنها، وعادة ما يتم البدء بها من قبل الجهة المنظمة والراعية.

تنفذ البرامج افتراضياً بهدف تعزيز مشاركة أفراد المجتمع في عمليات التطوير المستمرة للممكنات الحكومية وواجهات / تطبيقات الخدمات الحكومية، عبر رصد الثغرات الرقمية وإمكانية الإبلاغ عن أي ثغرات تقنية أو اجرائية قد تواجه العملاء عند إتمام المعاملات الحكومية. وذلك من خلال منصات مختارة من قبل الجهة لتمكن جميع أفراد المجتمع من المشاركة فيما يتعلق باكتشاف ثغرات المواقع والبرمجيات، أو غيرها. وتؤهلهم في بعض الأحيان للحصول على مكافآت نقدية ومعنوية لقاء اكتشاف الثغرات.

تسهم البرامج بالكشف عن مواطن الضعف والثغرات لدى الجهة، وتمكنها من تكوين مجموعة كبيرة ومتنوعة من الباحثين عن الثغرات، من أجل التخفيف من مخاطر الثغرات المحتملة، بالاضافة إلى التحقق من نضج الأنظمة والتطبيقات الرقمية.

يتيح الدليل الإرشادي قواعد عمل مشتركة للمبادئ التوجيهية والمنهجية التي يمكن اعتمادها لإعداد وتطبيق برامج صيد الثغرات الرقمية، وذلك بغرض تمكين الجهات من إدارة وتطبيق البرامج بكفاءة وفاعلية.

الرسم التوضيحي 1: أهداف مقترحة



3. الغرض من هذه الوثيقة

الغرض من هذا الدليل الإرشادي تقديم توصيات رئيسية بشأن وضع وتنفيذ خطة عمل نموذجية، ولا تهدف هذه الوثيقة إلى أن تحل محل أي دليل إرشادي حالي أو مستقبلي، وهي بمثابة استعراض للمتطلبات الوطنية أو التنظيمية المتعلقة بإجراء إطلاق وتنفيذ برامج صيد الثغرات فقط.

كما وجب التنويه أن هذه البرامج لا تعتبر بديلاً للجهة عن إجراء التقييم الأمني أو الاختبارات التقنية، مثل مراجعات التعليمات البرمجية الآمنة واختبار الاختراق. بدلاً من ذلك، ينبغي استخدامه لتكملة استراتيجية إدارة الثغرات في الجهة وضمن خطط التحسين المستمر من المنظور العام.

تختلف برامج صيد الثغرات عن الأساليب الأخرى من تقنيات التقييم والاختبار الأمني من حيث الأهداف والمنهجيات. حيث يوضح الجدول التالي على سبيل المثال الاختلافات بين برامج صيد الثغرات واختبارات الاختراق النموذجية:

المحور	برامج صيد الثغرات Bug Bounty Programs	اختبارات الاختراقات الأمنية Penetration Testing
النطاق	الوصول إلى عدد كبير من الباحثين عن الثغرات	يقتصر على مجموعة صغيرة من الاستشاريين الأمنيين
آلية الابلاغ عن النتائج	تقرير رئيسي عن النتائج التي تم اكتشافها والتوصيات، مع عدم وجود الكثير من المعلومات حول النهج والأهداف.	عادة ما تكون تقارير محددة النهج مسبقاً، بالاضافة إلى الأهداف والإطار الزمني وتأكيد على الاختبار
التنافسية	بيئة تنافسية للغاية وذلك بسبب المكافآت والحوافز المادية والمعنوية للشخص الذي يبلغ عن ثغرات	بيئة غير تنافسية حيث لا تحتوي على مكافآت
الحوافز والمكافآت	إمكانية تكريم المشاركين Wall of Fame أو تقديم سحوبات تأهل المشتركين لجوائز مالية أو عينية	لا ينطبق
الهدف	تحديد أكبر ثغرات ممكنة في فترة زمنية محددة ومشاركة أكبر عدد من الباحثين عن الثغرات	تحديد العديد من نقاط الضعف والثغرات، في إطار زمني محدود وعدد محدود من الفنيين العاملين على ذلك
معالجة الثغرات	يستند معالجة الثغرات عادة إلى إطار إدارة المخاطر وبحسب نوع الثغرات وأولوياتها	عادة ما يتم تطوير خطة معالجة فورية بعد تقارير الاختبار من قبل الجهة

4. المبادئ التوجيهية / الإطار العام للدليل

4.1 نقترح على الجهة الأخذ بعين الاعتبار قبل البدء في تحديد نطاق البرامج المزمع إطلاقها، اختيار نطاق يشمل تطبيقات رقمية غير حساسة بالنسبة للجهة ومتاحة للعامة، ثم التخطيط لتوسيع نطاق البرنامج في وقت لاحق، والاستفادة من الخبرة المكتسبة

4.2 إعداد سياسة الكشف عن الثغرات للبرنامج لضمان الشفافية والمصداقية.

4.3 ذكر نطاق الاختبار بوضوح، على سبيل المثال عناوين URL وأسماء التطبيقات، وأنواع الاختبارات غير المسموح بها، واستثناءات استحقاق المكافآت ... إلخ

4.4 الاستعداد داخلياً وتحديد آليات وأطر الاستجابة للثغرات من خلال البرنامج، وذلك للمراقبة وأن تكون الجهة على استعداد للاستجابة في حالة أي طارئ قد يحدث نتيجة الاختبارات، ويؤدي إلى تعطيل أو التأثير على الخدمات الرقمية.

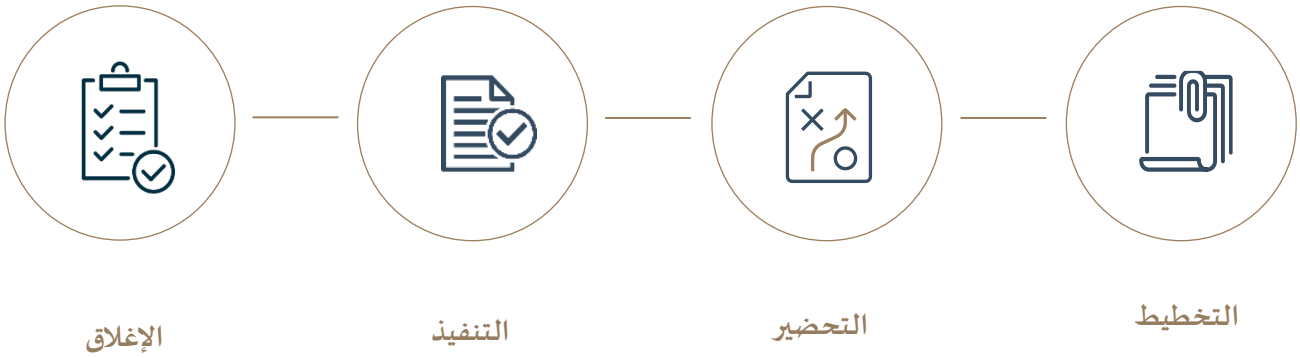
4.5 اعتماد إطار لمعالجة الثغرات، لضمان أن تكون المعالجة والإجراءات التصحيحية ضمن فترة زمنية مسبق تحديدها

4.6 تحديد الميزانية الإجمالية للموارد الداخلية والمكافآت قبل البدء بالبرنامج.

5. منهجية وآلية التطبيق

صمم هذا الدليل الإرشادي اعتماداً على أربع ركائز أساسية كمتطلبات لإطلاق البرامج وضمان توفر موارد كافية وحوكمة فعالة للتطبيق والتنفيذ.

وعليه نوصي الجهات باتباع هذه المراحل لتطبيق البرامج والتي سيتم التطرق لها بشكل تفصيلي في الدليل:



5.1 المرحلة الأولى : التخطيط

5.1.1 تطوير السياسات والعمليات

على جهة العمل تطوير سياسة المشاركة ببرامج صيد الثغرات، بالإضافة إلى تطوير العمليات الداخلية وتحسين القدرة على التعامل مع تقارير الثغرات، ووضع خطة اتصال داخلية وخارجية

5.1.2 اختيار البرامج التقنية للبرنامج

أن تقوم الجهة بإجراء تقييم مخاطر في مرحلة اختيار الموردين الخارجيين والنظام الأساسي لتشغيل البرنامج، والذي يشمل نطاق التقييم والمجالات مثل الأمن وخصوصية البيانات والمخاطر التشغيلية والمخاطر القانونية واستمرارية الأعمال.

فيما يلي بعض الاعتبارات الأخرى في عملية اختيار المنصة المناسبة للجهة:

- منصة قادرة على تشغيل البرامج وإتاحة المشاركة سواء ببرامج صيد ثغرات خاصة أو عامة
- توفير أو إعداد قناة داخلية لتتبع الثغرات الأمنية أو الإجرائية أو التقنية التي يتم الإبلاغ عنها داخلياً مثل برنامج جيرا

- أن يمكن النظام صائدي الثغرات من الموافقة على سياسة الكشف والمشاركة عن الثغرات.
- توفير المرونة في الخدمات المدارة، على سبيل المثال يقوم المزود أو المنصة المتاحة من إدارة البرنامج من البداية إلى النهاية.
- توفير خيار للعملاء والمشاركين لاختيار الخدمات التي سيتم تقييمها في حال وجود أكثر من تطبيق
- إمكانية أن يحصر النظام الأساسي الوصول بالمستخدمين الذين يحتاجون الوصول إليه فقط
- توافر إمكانية إصدار تقارير مكافآت الثغرات والمقاييس والتنبيهات والتحليلات وخاصية تتبع الحالة داخلياً، وتتبع التقارير وخاصية إعداد تقارير أداء حول مدى فعالية البرنامج.
  - نماذج تقديم آمنة تسمح للمشاركين تقديم التقارير أو توفير آلية للكشف عن الثغرات للجهات
  - سهولة تتبع المشكلات على النظام الأساسي والمرونة للتكامل مع قسم تقنية المعلومات أو الأقسام ذات العلاقة في الجهة
  - أن يأخذ بعين الاعتبار اعتبارات الاعتماد والامتثال مثل GDPR و ISO27K و ISO 29147 ، إن أمكن
  - التأكد من أن النظام المستخدم بإمكانه إنشاء مرجعية أو تذكرة للطلب المقدم كمرجع لجميع الثغرات
  - التأكد من أنه من السهل إضافة مهندسي البرامج ذوي الصلة للبرنامج
  - توفير إن أمكن خاصية توجيه رسائل البريد الإلكتروني تلقائياً إلى عنوان بريد إلكتروني آخر
  - إمكانية حفظ جميع التقارير مما سيسهم في سهولة إزالة الطلبات المكررة
  - لوحة تقرير أداء للإدارة العليا لمتابعة البرامج والمخصصات المالية وغيرها في أي وقت

5.1.3 مواءمة الموارد الداخلية وفرق العمل

تتطلب إدارة وتطبيق برامج صيد الثغرات فريقاً من الموظفين ذوي الخبرة من مختلف الأقسام، لضمان نجاح البرامج، وعليه ننصح الجهات بتحديد الفرق المعنية والنظر في استخدام مصفوفة RACI لتحديد الأدوار والمسؤوليات. كما نود التنويه، أنه بحسب الدراسات من المتوقع تخصيص حوالي 20-30٪ من وقت الموظف في برامج صيد الثغرات

على الجهة الأخذ بعين الاعتبار تكوين فريق عمل من الأقسام التقنية، والمالية والقانونية والاتصال المؤسسي وخدمة العملاء وغيرهم، كما يجب التنويه على أهمية التأكد من أن جميع الموظفين في الجهة على دراية كاملة بالبرامج حتى يتمكنوا من المساعدة في إعادة توجيه الاستعلامات وفقاً لذلك.

من الممكن للجهة أن تجري تمرين محاكاة كوسيلة لتعريف الموظفين بالأدوار والمسؤوليات ومن هذه المسؤوليات على سبيل الذكر لا الحصر:

- المعرفة بالإجراءات وآلية الرد عن أي استفسارات وآليات التصعيد والعمليات والتعامل مع النتائج والتقارير خلال تنفيذ البرامج.
- القدرة على الاستجابة والتواصل مع صائد الثغرات للتحقق من صحة الثغرات التي تم الإبلاغ عنها ومعالجتها
- القدرة على فرز وتتبع المدفوعات والمكافآت المالية أو غير المادية بعد ذلك.

5.1.4 تحديد نطاق اختبار البرنامج

يجب تحديد النطاق بوضوح، مثل مواقع الويب أو التطبيقات الموجودة داخل النطاق وخارجه وعليه لن تنطبق المكافآت إلا على ثغرات مواقع الويب والتطبيقات الموجودة في النطاق.

يوضح النطاق للمتقدمين ما يمكنهم وما لا يمكنهم اختباره أو تقديم تقارير الثغرات عنه- وهو أمر بالغ الأهمية للحصول على النتائج المرجوة من البرنامج. وعلى سبيل المثال بعض الاعتبارات الرئيسية هي:

- الوضوح والشفافية وعدم ترك أي مجال للتأويل أو عدم الوضوح
- معرفة وفهم التطبيقات والخدمات والقنوات المشاركة للاختبار في البرامج
- المواءمة مع الأهداف والأولويات بوضوح
- من المهم تحديد ما يمكن اختباره بوضوح في كل خدمة أو تطبيق، وتحديد مجالات التركيز بناءً على ذلك.

ولتحديد ذلك، ممكن للجهة طرح بعض الأسئلة الإسترشادية لتحديد النطاق:

- ما هي الأصول التي ترغب في اختبارها؟
- هل حددت ما هي الثغرات خارج النطاق؟
- ومن الأمثلة الأخرى على نقاط الضعف غير المؤهلة ما يلي:
  - القضايا المتعلقة بأي طرف ثالث غير الجهة أو مواقع، ولا تخضع لإدارة الجهة المنظمة
  - محاولات الهندسة الاجتماعية بما في ذلك رسائل البريد الإلكتروني الاحتيالية
  - الاستغلال بما يتجاوز الحد الأدنى المطلوب لإثبات وجود الثغرة على شبكة الإنترنت.
  - ثغرات تم الكشف عنها مؤخراً

5.1.5 البرامج الخاصة مقابل البرامج العامة

يمكن تشغيل برامج صيد الثغرات عامة أو خاصة. حيث ممكن أن تقوم الجهة بإطلاق برنامج مفتوح للعامة للتقديم والتقصي عن الثغرات، أو من الممكن دعوة مجموعة فرعية صغيرة حصرياً لأسباب اختبار خاصية أو تطبيق معين

وعليه على الجهة تحديد هل سيتم فتح باب التقديم للعامة أو تقديم برنامج صيد الثغرات لفئة معينة (برنامج صيد الثغرات الخاص)، وهو جانب يجب مراعاته ما إذا كان سيتم تشغيل برنامج مكافآت عام أو برنامج خاص. وهل يسمح البرنامج العام لأي شخص بالمشاركة والإبلاغ عن الثغرات. أو أن يتطلب البرنامج دعوة فئة معينة للمشاركة من أجل الإبلاغ عن الثغرات.

- **برامج صيد الثغرات العام**

يتم الإعلان عن هذه البرامج للعامة علناً، ويتم نشره بشكل عام للجمهور على الإنترنت ومتاح لأي شخص للمشاركة.

- **برامج صيد الثغرات الخاص**

لا يتم الإعلان عن هذه البرامج للعامة علناً، ويتم اختيار فئات محددة من المشاركين، بالإضافة إلى أنه محدد زمنياً. وتكون المشاركة فيه عن طريق الدعوة فقط. ويتم دعوة مجموعة من صيادي الثغرات والباحثين مع عدم الخروج عن النطاق واتباع قواعد البرنامج، وهو عادة الأفضل للميزانية المحدودة أو الاحتياجات قصيرة الأجل

5.1.6 الخدمة المدارة مقابل الخدمة غير المدارة

- من الممكن أن تستعين الجهة بإحدى المنصات المدارة لخدمة برامج صيد الثغرات أو أن تقوم داخلياً بتطوير قناة أ و تطبيق أو آلية داخلية للتفاعل مع الباحثين عن الثغرات
- في حال تم اختيار الجهة لطرف ثالث لإدارة البرامج، سيتم تقديم الخدمات الاستشارية الأساسية. سيكون هناك عادة تفاعل محدود مع الباحثين عن الثغرات
- التأكد من قدرة مقدم خدمة إدارة برامج الثغرات المدارة على تغطية ما يلي:
  - مراجعة النطاق معاً لتحديد القواعد وشبكة المكافآت.
  - اختيار الباحثين عن الثغرات وخصوصاً في حالة برامج صيد الثغرات الخاصة وفقاً لنطاق الجهة واحتياجاتها.
  - المساعدة في تحديد الحوافز والمكافآت بما يتماشى مع نضج الجهة وميزانيتها للحفاظ على جاذبية البرنامج وتأكيد تحقيق أهدافه

5.2 المرحلة الثانية : التحضير

أحد الركائز الأساسية المهمة للبرامج هو وجود إدارة قوية للثغرات وخطة استجابة منسقة وفعالة لفرز ومعالجة الثغرات المبلغ عنها، أو إذا أسفر الاختبار عن وقوع حادث.

5.2.1 تحديد الميزانية للبرنامج والتي سيكون لها أثر مباشر على جداول وآلية توزيع المكافآت

تحديد العائد من الاستثمار بشكل مباشر أو غير مباشر وذلك لتبرير الميزانية، حيث ينصح بالأخذ بعين الاعتبار كل من المدخلات والمخرجات، مثال ما هي تكلفة كل ثغرة أمنية، إجرائية أو تقنية تم أو سيتم الكشف عنها

5.2.2 أهلية المشاركة بالبرامج، ومثال على ذلك:

- تحديد الفئة العمرية للمشاركة
- إقرار الموافقة والالتزام بقواعد البرامج والشروط القانونية كما هو مذكور في سياسة المشاركة.
- أن يكون المتقدم متاحاً لتقديم معلومات إضافية، حسب حاجة فريق العمل
- موظفي الجهة غير مؤهلين للمشاركة في هذه البرامج

5.2.3 الأهلية للحصول على المكافآت

تحديد متطلبات التأهل للحصول على مكافأة مالية، على سبيل المثال لا الحصر:

- أن يكون المشترك أول شخص يرسل الثغرة الأمنية أو الإجرائية والتقنية للجهة.
- أن يتم تأكيد صلاحية الثغرة من قبل فريق العمل
- الامتثال لجميع شروط البرامج المعلن عنها.
- تحدد المبالغ والمكافآت وفقاً لتقدير فريق عمل البرامج، والذي سيقوم بتقييم كل تقرير من حيث الخطورة والتأثير والجودة.

5.2.4 دورية البرامج

بالرغم من وجود عدد من الفوائد لصيد الثغرات بشكل مستمر، إلا أن ذلك يتطلب جهد من فرق العمل وميزانيات إضافية، وعليه يجب على الجهة تحديد آلية دورية لعرض البرامج ومدتها والجوانب المتعلقة بذلك.

5.2.5 بناء نموذج تشغيلي

- الابتكار بآلية التقديم:
  - إذا كان الهدف الكشف عن ثغرات بتطبيق معين، يمكن إتاحة خاصية التقديم للعملاء فقط عن طريق الإبلاغ الفوري عن الثغرات الرقمية من التطبيق نفسه،
  - تطبيق آلية الرد التلقائي للطلبات المقدمة. حيث على سبيل المثال ممكن أن يتضمن الرد التلقائي شروط المشاركة وسياسة المشاركة والاستثناءات، مما يقلل من الحجم الإجمالي للتقارير التي تتطلب الاهتمام بنحو 50٪.
  - "خاصية الاهتزاز" والتي تتيح للمستخدم الإبلاغ الفوري عن وجود ثغرات رقمية قد يواجهها عند استخدامه التطبيق، حيث سيقوم الهاتف المحمول من خلال هذه الميزة بالتقاط صورة الشاشة تلقائياً مع إمكانية إرسالها على الفور، مثال على ذلك آلية الإبلاغ عن الثغرات في منظومة "تم".

5.2.6 تحديد أنواع الثغرات

تحديد نوع الثغرات والأنظمة أو التطبيقات المشاركة والمؤهل التقديم عليها في البرامج:

الرسم التوضيحي 2: أنواع ثغرات مقترحة

5.2.7 آلية الإبلاغ عن الثغرات

- معلومات الثغرات هي معلومات حساسة للغاية. وعليه لا ينصح استخدام البريد الإلكتروني للإعلان عنها
- من المهم تضمين المعلومات التالية على الأقل في طلب التقديم:
  - اسم المؤسسة وجهة الاتصال
  - أرقام التواصل
  - المنتجات أو الحلول والإصدارات المتأثرة
  - وصف الثغرة الأمنية أو التقنية أو الإجرائية المحتملة، بما في ذلك التأثير على المستخدمين أو غيرهم

- تقديم تفاصيل عن الثغرة، بما في ذلك المعلومات اللازمة للتخلص من الثغرة.

5.2.8 تقارير الإبلاغ عن الثغرات

- الحد الأدنى من التقرير الجيد يتطلب ما يلي:
  - وصف شامل للثغرة
  - تعليمات مفصلة خطوة بخطوة حول كيفية اكتشاف الثغرة المبلغ عنها
  - تحليل واضح للأثر يبرر خطورة الحالة.
  - إن أمكن توفير دليل يمكن التحقق منه على وجود الثغرة الأمنية (مثل صورة شاشة أو فيديو أو برنامج نصي)
  - توفير معلومات كافية حول الثغرة المكتشفة، ومن الأمثلة على ذلك:
    - عنوان *URL* و / أو عنوان *IP* للنظام المتأثر
    - تاريخ ووقت الوصول (الطابع الزمني)
    - المنتج والإصدار وتكوين البرنامج الذي يحتوي على الثغرة
    - إجراءات المعالجة أو الإصلاحات المقترحة إن وجدت

5.2.9 تحديد أولويات معالجة الثغرات

- تحديد آلية أو عملية فعالة لإدارة معالجة الثغرات، لتكون الجهة على استعداد لمعالجة جميع الثغرات وفق المعلومات المقدمة، علاوة على ذلك، من الممكن تكامل البرنامج أو الآلية مع أدوات مثل JIRA، لسد الفجوة بين البرنامج وفرق معالجة الثغرات بحسب نوعها
- معالجة الثغرات
  - الخطوة الأخيرة في هذه العملية هي إصلاح نقاط الضعف والثغرات. حيث توفر البرامج تغذية راجعة للثغرات كما تتطلب صيانة ثابتة. باستخدام حلول مدارة بالكامل من قبل فرق العمل المعنية

5.2.10 التأكد من أن الجهة لديها الفرق المناسبة وجميع المعلومات التي تحتاجها لتحديد أولويات المعالجة بدقة .

5.2.11 خطة الاتصال المؤسسي

نظرا لأن برامج صيد الثغرات تعتمد على الثقة، فإن التواصل نقطة أساسية ليس فقط داخلياً، ولكن خارجياً أيضاً. وعليه من المفضل القيام بإعداد خطة وقنوات اتصال واضحة داخلياً من أجل تعزيز عمل الفرق الداخلية، وإعداد عناوين رقمية وقنوات تواصل، لصائدي الثغرات للتواصل مع الجهة في حال وجود أي أسئلة أو استفسارات

التأكد من أن الموظفين في الجهة على دراية كاملة بالبرنامج حتى يتمكنوا من المساعدة في الرد على الاستفسارات.

5.2.12 الحو افز والمكافآت

تحديد نطاق المكافآت الأولي - سواء كانت مبالغ نقدية أو هدايا عينية أو تقدير المشاركين.

وعليه يجب تحديد نطاق المكافآت المناسب مع مراعاة متطلبات العمل والأهداف. هذه الخطوة مهمة في جذب اهتمام المشاركين للبرامج. كما يجب على الجهة تحديد الاستثناءات مثال على ذلك، من قبيل السرد لا للحصر:

- هجمات رفض الخدمة على مستوى الشبكة
- رفض التطبيق للخدمة عن طريق قفل حسابات المستخدمين
- رسائل الخطأ الوصفية
- الكشف عن الملفات أو الدلائل العامة المعروفة، (مثل الروبوتات، txt)
- إصدارات البرامج
- ملفات تعريف الارتباط التي تفتقر إلى إعدادات HTTP فقط أو إعدادات آمنة للبيانات غير الحساسة
- الهجمات التي تتطلب الوصول الفعلي إلى جهاز المستخدم
- الهجمات التي تعتمد على الهندسة الاجتماعية

5.2.13 آلية صرف ودفع المكافآت

- في هذه المرحلة، ستتلقى الجهة ثغرات صالحة وجاهزة للمعالجة بحسب توصيات المكافآت وتحديد الأولويات. من هناك، بمجرد التحقق، يتم إرسال أسماء الفائزين ي، وتتم عملية الدفع بحسب آلية محددة لضمان الدفع بسرعة وسلاسة.
- تحدد الجهة المعلومات المطلوبة من المشترك للحصول على المكافآت
- تحديد إجراء مدفوعات المكافآت الممنوحة تلقائياً وطرق الدفع

5.3 المرحلة الثالثة: التنفيذ

مع جميع الاعتبارات التشغيلية والإدارية المذكورة في الدليل فأن على الجهة تحديد مدير لإدارة برامج صيد الثغرات، خلال فترة الإجراء الفعلي للبرنامج، علماً بأنه لن تبلغ وتيرة التقارير الواردة ذروتها دائما بنسبة 100٪. في البداية، وعليه يجب أن تكون الجهة مستعدة للرد على المزيد من التقارير عن نقاط الثغرات، خاصة خلال فترة عطلة نهاية الأسبوع حيث تميل الأنشطة إلى أن تكون أعلى. مع مرور الوقت وقربها للفترة الزمنية المحددة.

5.3.1 عملية فرز الثغرات

- يتم تصفية وفرز جميع الثغرات المقدمة لتحديد الثغرات المؤهلة فقط وفقاً وضمن نطاق اختبار البرامج. تستخدم هذه العملية لتقديم نتائج قابلة للتنفيذ
- يقوم فريق العمل بفرز الثغرات في كل تقرير، وتقييم التطبيق باستخدام مشكلة محتملة، وتحديد ما إذا كانت الثغرة المبلغ عنها حقيقية.
- عادة ما يتم التقدير ودفع المبالغ المالية والمكافآت إما بعد أن يتم فرز الثغرات وتأكيدها، أو بعد إصلاحها. ومعالجتها أو بعد انتهاء البرامج

5.3.2 التحقق من صحة التقارير

عند التحقق مما إذا كانت المشكلة التي تم الإبلاغ عنها تمثل ثغرة مقبولة بحسب سياسة المشاركة تحتاج الجهة والفريق المعني إلى التعمق أكثر من مجرد ما هو موجود في التقرير. لا يمكن للشخص الذي يقدم التقرير الوصول إلى الفريق التقني والوثائق، لذا لا يمكنه إلقاء نظرة على الشفرة والتخفيف لفهم السبب الجذري، ومعرفة المكان الآخر الذي قد توجد فيه نفس المشكلة في قاعدة التعليمات البرمجية. وعليه فأنه من الأهمية أن يتقصى الفريق التقني عن تحديد نطاق التأثير

5.4 المرحلة الرابعة : إغلاق البرنامج

5.4.1 إنهاء الوصول

- يجب أن تتوقف جميع عمليات الوصول المقدمة في تاريخ ووقت الانتهاء المحددين.
- إعداد التقرير الرسمي وتلخيص النتائج واختتام البرنامج.

5.2.1 المراجعة الدورية لخطة عمل البرامج وإعداد الخطط االتحسينية

- من الأهمية بمكان مراجعة نطاق البرنامج ونتائجه، ونسبة تحقيقه للأهداف المحددة، ينصح بإجراء التعديلات في كل خطوة من تنفيذ خارطة الطريق، للاستمرار في تلقي نتائج عالية القيمة.
- من المفيد النظر في كيفية التحسين بشكل أكبر من خلال النظر في البنود التالية:
  - الميزانية
  - عدد التقارير
  - جودة التقارير
  - مصفوفة المكافآت
  - التحقق من صحة النتائج وحسابات الخطورة
  - المعالجات وإعادة الاختبار

6 سياسة المشاركة

على جميع الجهات توفير سياسة المشاركة ونشرها لجميع المشتركين بشفافية، ومثال على البنود في مثل هذه السياسات، على سبيل الذكر لا الحصر ما يلي:

1. لا تمنح هذه السياسة تفويضاً أو إذناً أو تسمح بخلاف ذلك بالوصول الصريح أو الضمني إلى أنظمة معلومات الجهة أو الجهات المشاركة متاحة لأي فرد أو مجموعة من الأفراد أو شركة أو أي جهة تجارية أو قانونية آخرى. ومع ذلك، وعليه يعمل (صائد الثغرات) وفقاً لشروط وأحكام البرنامج
2. يجب الامتثال لجميع القوانين الاتحادية والمحلية المعمول بها فيما يتعلق بأنشطة البحث عن الثغرات وبالأخص الثغرات الأمنية. ولا يجوز المشاركة في أي بحث أمني أو نشاط للكشف عن الثغرات لا يتوافق مع شروط وأحكام البرنامج أو القانون.
3. في حال المشاركة في أي أنشطة لا تتوافق مع شروط وأحكام برامج صيد الثغرات أو القوانين ذات الصلة بالدولة، قد يخضع صائد الثغرات لعقوبات جنائية
4. يحق للجهة التي تدير البرنامج تعديل الشروط والأحكام أو إنهاء البرنامج في أي وقت

سياسة / شروط وأحكام الإفصاح عن المعلومات

1. مشاركة المعلومات مع الجهة فقط حول الثغرة الأمنية أو الإجرائية أو التقنية

2. عدم إلحاق أي ضرر أو استغلال أي ثغرة تتجاوز الحد الأدنى من الاختبارات المطلوبة لإثبات وجودها أو لتحديد مؤشر مرتبط بها.
3. على المتقدم أن يقدم الطلب بسرعة وفعالية، وأخذ ما يلي بعين الاعتبار:
    a. خصوصية العملاء
    b. خصوصية مزودي الخدمة
4. سرية و سلامة و توافر الأنظمة / التطبيقات / المواقع الرقمية والخدمات
5. التصرف بمسؤولية وبما يحقق المصلحة العامة وعلى وجه الخصوص:
6. عدم مخالفة القانون: .
    a. عدم استخدم تقنيات الهندسة الاجتماعية أو التصيد الاحتيالي أو الهجمات ضد العملاء أو البنية التحتية أو الموظفين
    b. عدم القيام بأي هجوم يمكن أن يضر بموثوقية أو سلامة الأنظمة أو الخدمات أو البيانات
    c. عدم تعريض أي بيانات للخطر؛
    d. عدم الافصاح أو الإعلان عن الخطأ علنياً قبل إصلاحه والتصدي له
7. أن يتأكد مقدم الطلب من أن الثغرة المحتملة التي يتم الابلاغ عنها ضمن النطاق المحدد والمعلن عنه.
8. عدم إجراء أي تغييرات في البيانات
9. إذا قام المتقدم عن غير قصد بالوصول إلى البيانات الخاصة المقيدة أثناء التحقيق في ثغرة ما، عليه التوقف فوراً عن أي نشاط قد يؤدي إلى مزيد من الوصول إلى البيانات وإبلاغ الجهة بذلك
10. تجنب الوصول عمداً إلى محتوى أي اتصالات أو بيانات أو معلومات عابرة أو مخزنة على نظام أو أنظمة - باستثناء الحد الذي تكون فيه المعلومات مرتبطة مباشرة بثغرة ويكون الوصول ضرورياً لإثبات وجودها
11. عدم الإفصاح عن أي بيانات تحت أي ظرف من الظروف.
12. عدم تعمد المساس بخصوصية أو سلامة موظفي الجهة أو أي طراف آخر. وعدم الكشف عن أي ثغرة تم اكتشافها أو الابلاغ عنها والتعامل مع التقرير على أنه سري حتى تتاح الفرصة للفرق المعنية للتصدي لها ومعالجتها
13. يتم استبعاد الثغرات التي تعتبر ضمن رمز طرف ثالث خارج نطاق هذا البرنامج حيث يمكن الإبلاغ عن الثغرات ولكن لا تتأهل للمكافآت.
14. ستعالج التقارير المكررة والتقارير الوثيقة الصلة على أساس كل حالة على حدة.

15. عدم الالتزام بهذه الشروط والاحكام (السياسة) يسقط حق المشارك ويعتبر التقرير غير مؤهل للحصول على مكافآت
16. عدم عرض أي معلومات عن الملكية الفكرية أو المصالح التجارية أو المالية الأخرى لأي من الجهات المشاركة أو موظفيها، أو أي أطراف ثالثة
17. عدم الكشف علنا عن أي تفاصيل عن الثغرة أو مؤشر الضعف أو محتوى المعلومات المتاحة بواسطة ثغرة، إلا عند تلقي إذن كتابي صريح من الجهة
18. إذا تعرض المتقدم أثناء البحث عن غير قصد لمعلومات غير مصرح للجمهور بالوصول إليها، على المتقدم محو بشكل فعال ودائم جميع المعلومات المحددة التي بحوزته وفقاً لتوجيهات الجهة
19. عدم إجراء اختبار رفض الخدمة أو أي اختبارات (مثل الوصول إلى المكاتب أو الأبواب المفتوحة أو التتبع) أو الهندسة الاجتماعية، بما في ذلك التصيد الاحتيالي، فيما يتعلق بموظفي الجهة أو الجهات المشاركة أو أي طرف ثالث.
20. عدم إرسال عدد كبير من التقارير منخفضة الجودة
21. في حال عدم التأكد في أي وقت من أي ثغرة أو كيفية التعامل مع الطلب، فيرجى التواصل مع فريق العمل

8 مسؤوليات الجهة

1. أخذ جميع التقارير المقدمة جدياً والتحقق من كل إفصاح والسعي جاهدة لضمان اتخاذ الخطوات المناسبة للتخفيف من المخاطر ومعالجة جميع نقاط الضعف المبلغ عنها
2. الالتزام بالتنسيق مع صائد الثغرات بشفافية وسرعة. ويشمل ذلك اتخاذ الإجراءات التالية:

8.2.1 إرسال تأكيد استلام الطلب المرسل وأن الفريق سيعمل على التحقيق في التقرير وقد يتصل بك للحصول على مزيد من المعلومات في غضون يوم عمل واحد،

3. عندما يكون ذلك ممكناً ومعتمداً، ستؤكد الجهة وجود الضعف للمتقدم وتبقي الباحث على اطلاع، حسب الاقتضاء، أثناء معالجة الثغرة
4. أن يتم إضافة المتقدم للائحة التكريم *(wall of fame)* تقديراً لمساهماته، إذا كانت هذه هي رغبة المتقدم، عندما يكون ذلك ممكناً عملياً، ولن يتم الكشف العلني عن نقاط الضعف إلا بموافقة كتابية صريحة من الجهة.