الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

مسودة

المبادئ العامة
للتصميم الآمن

(SBD – 1: 2020)

إشارة المشاركة: أبيض
تصنيف الوثيقة: غير مصنف

بسم الله الرحمن الرحيم

بروتوكول الإشارة الضوئية (TLP)

تم إنشاء نظام بروتوكول الإشارة الضوئية لمشاركة أكبر قدر من المعلومات الحساسة ويستخدم على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

- **أحمر – شخصي وسري للمستلم فقط**
  المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد سواء من داخل أو خارج المنشأة خارج النطاق المحدد للاستلام.

- **برتقالي – مشاركة محدودة**
  المستلم بالإشارة البرتقالية يمكنه مشاركة المعلومات في نفس المنشاة مع الأشخاص المعنيين فقط، ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة .

- **أخضر – مشاركة في نفس المجتمع**
  حيث يمكنك مشاركتها مع آخرين من منشأتك أو منشأة أخرى على علاقة معكم أو بنفس القطاع، ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

- **أبيض – غير محدود**

قائمة المحتويات

الملخص التنفيذي

إن التوسع في استخدام التقنية يفتح آفاقاً متجددة للتهديدات السيبرانية، مما يتطلب المرونة ومواكبة المستجدات في الفضاء السيبراني والتعامل الفعال مع التطورات التقنية للحد من هذه التهديدات. ولذلك، تعمل المملكة على تبني نهجاً استباقياً واستراتيجياً يأخذ في الاعتبار المخاطر السيبرانية بحيث تشمل تنفيذ المبادرات الجديدة والمشاريع المعلوماتية والتقنية وإدارة التغيير فيها.

ومن هذا المنطلق، قامت الهيئة الوطنية للأمن السيبراني (ويشار لها في هذه الوثيقة بـ "الهيئة") بالعمل على مبادرة التصميم الآمن والتي تهدف لنشر أفضل الممارسات في هذا المجال. وكأحد الجهود المتضمنة في هذه المبادرة، تم تطوير هذه الوثيقة لتقدم مجموعة من مبادئ التصميم الآمن العامة بهدف إرشاد الأطراف المعنية بأبرز الممارسات الأساسية في الأمن السيبراني، حيث اشتملت منهجية إعداد الوثيقة على الخطوات الأساسية التالية:

- تحليل تجارب الدول في هذا المجال
- مدخلات وآراء المختصين في الأمن السيبراني
- دراسة أفضل الممارسات العالمية في التصميم الآمن

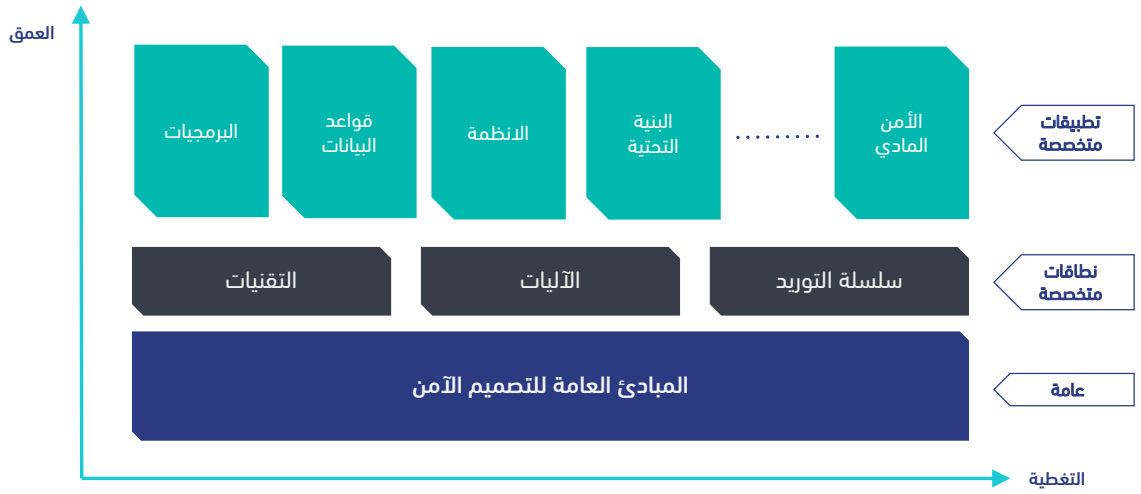
صممت المبادئ لتأخذ بالاعتبار الشمولية والدقة والتكاملية عند تنفيذها فهي مبنية على ثلاثة مراحل:

أولا: المبادئ العامة ذات الشمولية الفعالة

ثانيا: مجموعة مبادئ لنطاقات متنوعة لتغطي مجالات مختلفة لها تقنيات متشابهة

ثالثا: مبادئ لتقنيات محدده

جميع هذه المراحل مكملة بعضها البعض وتغطي جميع جوانب التصميم الآمن. الشكل ا يوضح منهجية تصميم المبادئ.



الشكل ا: منهجية تصميم مبادئ التصميم الامن

وفقاً لذلك، فقد تم وضع ثمانية مبادئ لأبرز الممارسات الأساسية للتصميم الآمن وهي:

١	منح الحد الأدنى من الصلاحيات	Least Privileges
٢	الحاجة إلى المعرفة	Need to Know
٣	فصل المهام	Segregation of Duties
٤	تجنب الغموض كوسيلة للأمان	Avoid Security by Obscurity
٥	الدفاع الأمني متعدد المراحل	Defense in Depth
٦	عدم الثقة	Zero Trust
٧	الضبط الآمن للإعدادات الافتراضية	Secure Defaults
٨	تقليص نطاق الهجوم	Attack Surface Reduction

المقدمة

إن وجود بنية تحتية رقمية وطنية متكاملة وآمنة يعد أحد أهم العوامل الممكنة للنمو والازدهار، حيث أنها تتطلب انسيابية في المعلومات وأمانها وتكامل أنظمتها وتستوجب المحافظة على الأمن السيبراني للمملكة العربية السعودية وتعزيزه حماية للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية.

وحيث أن التوسع في استخدام التقنية يفتح آفاقاً جديدة للثغرات الأمنية والتهديدات السيبرانية؛ مما يستوجب تعزيز الأمن السيبراني لحماية الشبكات، وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات وحماية ما تقدمه من خدمات وما تحويه من بيانات من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال وكذلك لتعزيز الربط التقني الآمن بين الخدمات الحكومية ودعم الاقتصاد الرقمي.

لكن معالجة جوانب الأمن السيبراني بعد تطوير الأنظمة يزيد التكلفة ويصعب التنفيذ ويتطلب جهوداً مضاعفه لتأمين، واختبار، وإطلاق الأنظمة. إضافة إلى المخاطر الناتجة عن عدم كفاءة الحلول لمراقبة واختبار الثغرات خلال فترة التشغيل وتحديث الأنظمة بسرعة وفعالية.

لذلك تعمل المملكة على تبني نهجٍ استباقيٍ لتعزيز جوانب الأمن السيبراني في الأنظمة والأجهزة والخدمات بدءاً من التصميم حتى الإنتاج ومن ثم التشغيل وانتهاءً بالإتلاف من أجل الوصول إلى تطبيق معايير تقنية تضمن وجود أنظمة وأجهزة وخدمات رقمية ذات جودة ومستوى أمني مرتفع. ومن هذا المنطلق، قامت الهيئة بالعمل على مبادرة التصميم الآمن والتي تهدف لأخذ جوانب الأمن السيبراني في عين الاعتبار في جميع مراحل التطوير، والنظر في أي نظام – ويشمل ذلك جميع مكوناته– باعتباره معرضاً للهجمات السيبرانية مما يتطلب بناء الدفاعات المناسبة له في جميع المراحل.

وتقدم هذه الوثيقة مجموعة من المبادئ العامة للتصميم الآمن والتي تهدف لتوضيح ونشر أبرز الممارسات في هذا الجانب والتي يمكن إتباعها على نطاق واسع، وعرض هدف كل مبدأ مع أمثلة حول كيفية تطبيقها. وتتطلع الهيئة من خلال هذه الوثيقة إلى إطلاق العمل في مبادرة التصميم الآمن مما يساهم في تحقيق فضاء سيبراني سعودي آمن وموثوق.

المنهجية

تم بناء مبادئ التصميم الآمن بمنهجية شاملة وخطوات أساسية؛ بدأت بدراسة أبرز المخاطر السيبرانية التقنية العالمية والمحلية، وتطوير إطار تكاملي وشامل يغطي جميع مراحل تقديم الحلول التقنية. كما تمت الاستفادة من أفضل الممارسات والخبرات العالمية بشكل يتناسب مع احتياج المملكة؛ بالإضافة إلى مدخلات وآراء المختصين في الأمن السيبراني على المستوى الوطني لصياغة منهجية واضحة وشاملة ووضع مجموعة من المبادئ العامة.

تساهم هذه المبادئ بشكل مباشر فيما يلي:

- تعزيز الصمود السيبراني.
- تقليص نطاق الهجوم السيبراني.
- تكامل ضوابط الأمن السيبراني مع الوظائف الأساسية للحلول التقنية.

تتكامل هذه المبادئ مع إصدارات الهيئة الأخرى علماً بأن هذه الوثيقة تشكل نقطة انطلاق لمبادرات التصميم الآمن ذات النطاق المحدد والطبيعة الخاصة.

نطاق الوثيقة

تقدم هذه الوثيقة مجموعة من مبادئ التصميم الآمن التوجيهية لأغراض توعوية. وتشجع الهيئة جميع الجهات والقطاعات في المملكة العربية السعودية بتنوع طبيعة أعمالها على اتباع هذه المبادئ لإعداد وتطوير وتشغيل مشاريع تقنية المعلومات والتقنيات التشغيلية، وذلك للحد من مخاطر الأمن السيبراني على أعمالهم وأنظمتهم وبياناتهم.

مبادئ التصميم الآمن العامة

I منح الحد الأدنى من الصلاحيات (Least Privileges)

تقييد صلاحيات المستخدمين[1] ضمن نطاق عملهم وتخصصهم لتنفيذ مهامهم المخولين بها فقط.

يعتمد هذا المبدأ على منح المستخدمين الحد الأدنى من الصلاحيات اللازمة لإتمام مهامهم الرسمية. ينطبق هذا المبدأ على جميع المستويات في النظام، بما في ذلك المستخدمين والبرامج والشبكات والتطبيقات وكل جوانب تقنية المعلومات المختلفة.

ولتحقيق هذا المبدأ، ينبغي تحليل إجراءات العمل ومتطلباتها بما في ذلك تحليل وتصنيف البيانات ذات العلاقة، ومن ثم تقييد صلاحيات المستخدمين بحسب أدوارهم ومسؤولياتهم إلى الحد الأدنى المطلوب لأداء مهامهم.

يمنع هذا المبدأ إمكانية الوصول إلى الأنظمة أو البيانات غير الضرورية للمستخدم مما يقلل المخاطر المتعلقة بتسريب البيانات أو الإجراءات غير المشروعة. بالإضافة إلى تقليص نطاق الهجوم المحتمل.

مثال

قد يحتاج أحد موظفي الموارد البشرية إلى حق الوصول للقراءة والكتابة لقاعدة بيانات مسيرات الرواتب، ولكن لا تتطلب مهامه الوظيفية الوصول إلى قاعدة بيانات العملاء؛ في الوقت نفسه، لا تتطلب مهام موظف قسم المبيعات سوى الوصول إلى قاعدة بيانات العميل (دون الحاجة للوصول إلى قاعدة بيانات الرواتب).

[1] يشار في هذه الوثيقة إلى "المستخدمين" كأشخاص فعليين أو حساب مستخدم (User Account) والأنظمة والبرامج.

٢ الحاجة إلى المعرفة (Need to Know)

حصر الوصول للمعلومات للمستخدمين المفوضين والذين تقتضي طبيعة أعمالهم الوصول إلى هذه المعلومات.[٢]

يعتمد هذا المبدأ على حصر الوصول إلى المعلومات للمستخدمين المفوضين ممن تقتضي طبيعة أعمالهم هذا الوصول. حيث لا يسمح للمستخدمين بالوصول الكلي إلى جميع المعلومات.

ويمكن تطبيق هذا المبدأ بطرق مختلفة كالعمل على تطبيق فصل فعلي للأنظمة، والتحكم بالوصول إلى سجلات معينة، وإعداد ضوابط تقنية، كتحديد الأوقات المسموح بها للوصول إلى المعلومات.

ويهدف المبدأ للحد من الوصول غير المصرح به دون التأثير على أداء مهام الأعمال. أيضاً يهدف إلى إعاقة الوصول إلى المعلومات المقيدة عن طريق حصر الوصول لأقل عدد ممكن من المستخدمين.

مثال

منح مدراء الإدارات الصلاحيات للوصول لمعلومات الموظفين تحت إدارتهم فقط والمتطلبة لتنفيذ مهامهم الإدارية ويمنع مشاركة المعلومات الشخصية للموظف مع المدير المباشر مالم تقتضي حاجة العمل لذلك.

٢ يعني مبدأ "الحد الأدنى من الصلاحيات" بما يستطيع المستخدم تنفيذه من أنشطة، بينما يعنى هذا المبدأ بما يستطيع المستخدم من الوصول إليه من بيانات.

٣ فصل المهام (Segregation of Duties)

مشاركة أكثر من شخص في تنفيذ عملية محددة بمراحل مختلفة.

فصل المهام أو الفصل بين الواجبات هو مبدأ يهدف إلى فصل كل مهمة على مراحل تنفيذ عملية محددة عن طريق التأكد من ضرورة وجود أكثر من شخص لإكمال هذه المراحل وبصلاحيات مختلفة.

يتم تحقيق هذا المبدأ من خلال فصل المهام الحساسة[٣] إلى خطوات متعددة تعتبر كل منها ضرورية لإكمال المهمة وتعيين كل خطوة لشخص أو فريق عمل مختلف.

يحد تطبيق هذا المبدأ من الأخطاء الفردية في المهام الحساسة ويمنع أي شخص من انتهاك ضوابط الأمن السيبراني بمفرده.

مثال

طلبات التغيير يجب اعتمادها من أكثر من شخص، على سبيل المثال، يتم تنفيذ قواعد جدار الحماية (Firewall) من خلال شخص والموافقة عليها من شخص آخر، كما يتم رفع طلبات مسيرات الرواتب من شخص والموافقة عليها من شخص آخر.

[٣] مثل مهام منح التفويض (Authorization Functions) ومهام التدقيق والحصانة على الأصول.

٤ تجنب الغموض كوسيلة للأمان (Avoid Security by Obscurity)

تجنب الاعتماد على غموض مكونات وتصميم الأنظمة وإخفاء تفاصيلها كوسيلة رئيسية لتأمين الأنظمة.

يعطي الاعتماد على غموض المكونات والتصميم كوسيلة لحماية الأنظمة انطباعا خاطئاً، حيث بالإمكان معرفة مكونات وتصميم الأنظمة بطرق مختلفة. قد يستخدم مبدأ الأمن من خلال الغموض كوسيلة إضافية للدفاع ولكن يجب ألا يعتمد أمن النظام على سرية تصميمه أو مكوناته.

الأمن بالاعتماد على الغموض هو مبدأ يناقض مبدأ التصميم الآمن. يجب أن يتم تصميم الأنظمة بضوابط أمنية مع عدم اخذ غموض مكوناته أو إخفاء تفاصيله الداخلية كوسيلة رئيسية لتأمينها.

يهدف هذا المبدأ لحماية الأنظمة في حالة تسرب معلومات عن مكونات وتصميم الأنظمة وعدم الاعتماد على غموضها كوسيلة أساسية للأمان.

مثال

تجنب إخفاء كلمات المرور للحسابات في ملفات نصية مخزنة في مجلد مخفي، أو تغيير اسم مجلد التطبيقات الحساسة (مثلاً من "admin" إلى "admin2")، واستخدام آليات تشفير مطورة داخلياً.

0 الدفاع الأمني متعدد المراحل (Defence in Depth)

وضع مستويات متعددة من الضوابط الأمنية كآليات دفاعية.

هو مفهوم لتوكيد المعلومات (Assurance) حيث يتم وضع مستويات متعددة من الضوابط الأمنية كسلسلة دفاعية بحيث إذا فشلت إحدى الآليات تكون هناك آلية أخرى للدفاع.

استخدام آليات على مستويات متعددة مثل الجدار الناري وأنظمة كشف ومنع التسلل وتشفير البيانات وأنظمة المراجعة والتدقيق ووضع آليات الأمن المادي والإجرائي هي من أساسيات تحقيق هذا المبدأ.

يهدف المبدأ إلى زيادة أمن الأنظمة وذلك بالحد من الثغرات وغلق الثغرات الأمنية وزيادة صعوبة الهجمات وتحسين القدرة على اكتشافها والاستجابة لها.

مثال

اخذ الموافقات اللازمة للوصول المادي للخوادم والدخول باستخدام تقنيات التحقق الثنائي وتفعيل سجلات الأحداث وكاميرات المراقبة. بالإضافة إلى تشفير البيانات (أثناء النقل والتخزين) واستخدام تقنيات منع تسريب البيانات.

٦ عدم الثقة (Zero Trust)

التحقق من جميع المستخدمين وأهليتهم للاستخدام قبل السماح بالوصول.

يمكن لجميع الأطراف الموثوقة، بما في ذلك المستخدمين والأطراف الخارجية وغيرهم أن يشكلوا خطراً على الأنظمة، لذلك يجب التحقق من كل مستخدم حتى الموثوق بهم عند استخدام أي خدمة أو أي نظام.

وفي مفهوم عدم الثقة، يجب التحقق من المستخدمين وأهليتهم، بما في ذلك المستخدمين الداخليين والأطراف الخارجية (3rd Party)، وتفعيل آليات المتابعة والمراقبة عند استخدام الخدمات والأنظمة.

من أهم الفوائد من تطبيق هذا المبدأ هو معرفة مستخدمي الأنظمة وتحليل البيانات التي من شأنها الكشف عن بعض الثغرات التشغيلية والحد من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية.

مثال

يعتبر تسريب البيانات أمراً ممكناً لأي شخص لديه حق الوصول إلى الشبكة. وللحد من ذلك، يجب أن يتم التحقق من كل هوية وكل عملية، وتسجيلها مع تطبيق الآليات الأخرى المناسبة مثل التشفير.

٧ الضبط الآمن للإعدادات الافتراضية (Secure Defaults)

تصميم المنتجات والخدمات بإعدادات تكوين تحقق أفضل الممارسات الأمنية بشكل افتراضي.

ينص هذا المبدأ على أن يتم تصميم الأنظمة لتكون إعدادات تكوينها آمنة بشكل افتراضي ودون الحاجة لاتخاذ أي إجراء من جانب المستخدم لإعداد النظام بشكل آمن.

وهذا المبدأ بمفهومة يوجب تفعيل المزايا الأمنية في إعدادات النظام بشكل افتراضي، وتعطيل الإعدادات غير الآمنة مع موازنة الحاجة لتقديم تجربة استخدام سهلة.

ويهدف هذا المبدأ إلى رفع مستوى الأمان عند استخدام المنتجات والخدمات وتقليل المخاطر المتعلقة بعدم معرفة المستخدم حول أفضل الممارسات الأمنية أو إهمال اتباعها.

مثال

تفعيل ميزة خدمة التحقق الثنائي عند تسجيل الدخول للنظام، وعدم إعداد الأنظمة بمعلومات مصادقة افتراضية (مثل اسم مستخدم وكلمة المرور).

٨ تقليص نطاق الهجوم (Attack Surface Reduction)

التقليل من انكشاف ما يجب حمايته من أنظمة وأجهزة وتطبيقات، وتقليص تعرضها للهجوم المباشر.

يتضمن نطاق الهجوم أي نقاط وصول للأنظمة تتيح للخصوم فرصة لاستغلالها (بما في ذلك مكونات الأجهزة والتطبيقات وغيرها). يتوسع هذا النطاق بزيادة تعقيد الأنظمة وتعدد مزاياها، مما يجعلها أكثر عرضة للهجمات الأمنية والذي بدوره يؤكد أهمية البساطة في تصميم الأنظمة.

يمكن تقليص مساحة الهجوم بالحد من التعقيدات غير الضرورية في الأنظمة مثل تقليل حجم الشفرة المصدرية للنظام، والأنظمة الخارجية التي يتّصل بها، وتعطيل المزايا والخدمات الغير ضرورية.

ويهدف هذا المبدأ إلى الحد من نقاط الهجوم (Attack Vectors) التي يمكن للمخترق اكتشافها ومحاولة استغلالها.

مثال

تعطيل المنافذ غير الضرورية في الأنظمة والحد من صلاحيات المستخدمين وإزالة التطبيقات والخدمات الغير مستخدمة.