الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

المركز الوطني الإرشادي
للأمن السيبراني
SAUDI CERT

دليل الممارسات السيبرانية الآمنة للموظفين في بيئة العمل

إشارة المشاركة: أبيض
تصنيف الوثيقة: متاح

CERT-GEW-1:2021

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 المنشأة 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

المقدمة ٦
الفصل الأول: الممارسات الآمنة لعموم الموظفين ٨
الفصل الثاني: الممارسات الآمنة للمدراء والقادة ١٥
الفصل الثالث: الممارسات الآمنة لموظفي تقنية المعلومات ومختصي الأمن السيبراني ١٨
المصادر والمراجع الإضافية ٣١
الخاتمة ٣٢

المقدمة

تشهدُ المملكة تحولاً واسع النطاق في استخدام أنظمة تقنية المعلومات سواءً في مقر العمل أو عن طريق الخدمات المقدّمة عن بُعد، كما تشهد نموًا مصاحبًا في الهجمات السيبرانية والاختراقات الأمنية، بالإضافة الى تهديدات مختلفة في تسريب البيانات الحساسة، وانتهاكات لخصوصية الأفراد والجهات.

ولأهمية المحافظة على الأمن السيبراني للمملكة وتعزيزه وحمايةً للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية؛ فقد أتى تأسيس الهيئة الوطنية للأمن السيبراني والموافقة على تنظيمها بموجب الأمر الملكي الكريم رقم ٦٨٠١ وتاريخ ١٤٣٩/٢/١١ هـ، وجعلها الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه.

ولرفع موثوقية وانسيابية المعلومات وأمانها وتكامل أنظمتها، فقد تم بناء الاستراتيجية الوطنية للأمن السيبراني التي تعكس الطموح الاستراتيجي للمملكة وبأسلوب متوازن بين الأمان والثقة والنمو، حيث وضعت مكوناتها وفقاً لإطار مرجعي مبني على أفضل الممارسات المحلية والعالمية وأهم المستجدات والتحديات التي تواجه الأمن السيبراني.

ولضمان تحقيق الأمن السيبراني في أي جهة، لا بد من تحقيق ثلاثة عناصر رئيسية: العنصر التقني، العنصر الإجرائي، والعنصر البشري، والأخير هو محور هذا الدليل ومحط تركيزه حيث تفيد إحصاءات الأمن السيبراني بأن مايقارب ٥٠٪ من الاختراقات التي تشهدها الجهات عالميًا هي بسبب الموظفين[١] بصفة عامة سواءً كانوا موظفين إداريين أو تقنيين أو مدراء تنفيذيين أو حتى مختصي الأمن السيبراني.

ومن أبرز أسباب التهديدات والاختراقات السيبرانية في بيئة العمل والمرتبطة بالعنصر البشري هي:

- ضعف الوعي بالأمن السيبراني
- إهمال وتساهل الموظفين بالالتزام بالإجراءات الأمنية
- عدم إدراك أهمية المعلومات التي يتعاملون معها ومسؤوليتهم تجاه حمايتها
- حدوث أخطاء أثناء التعامل مع البيانات مما قد يتسبب بتسريبها بشكل غير مقصود
- إساءة استخدام الصلاحيات
- التعرّض لهجمات الهندسة الاجتماعية والتصيّد الإلكتروني
- عدم تطبيق أفضل ممارسات الأمن السيبراني

١ إحصائية عالمية من عام ٢٠١٢-٢٠١٧:
https://www.statista.com/statistics/956269/insider-threats-element-of-cyber-breaches-worldwide/

ومن هذا المنطلق، تم إعداد هذا الدليل ليستهدف الموظفين على اختلاف أدوارهم في الجهات بهدف نشر الوعي بالأمن السيبراني ودعم جهود العاملين في الجهات العامة والخاصة في رفع الحس الأمني وحماية جهاتهم وبياناتهم من الهجمات والاختراقات والتهديدات السيبرانية، كما يستهدف الدليل عموم الموظفين سواءً كانوا يعملون في قطاع حكومي أو خاص أو في مؤسسات المجتمع المدني المختلفة.

وتأتي جهود المركز الوطني الإرشادي للأمن السيبراني (السيرت السعودي) ضمن اختصاص ودور الهيئة الوطنية للأمن السيبراني في "رفع مستوى الوعي بالأمن السيبراني" سعياً إلى تحقيق بيئة عمل آمنة وبناءة، مع مراعاة أن مسؤولية الهيئة لا تخلي أي جهة عامة أو خاصة أو غيرها مـن مسؤوليتها تجاه أمنها السيبراني، وهو ما أكّده الأمر السامي الكريم رقم ٥٧٢٣١ وتاريخ ١٤٣٩/١١/١٠هـــ بأن "على جميع الجهات الحكومية رفع مستوى أمنها السيبراني لحماية شبكاتها وأنظمتها وبياناتها الإلكترونية، والالتزام بما تصدره الهيئة الوطنية للأمن السيبراني من سياسات وأطر ومعايير وضوابط وإرشادات بهذا الشأن".

الفصل الأول: الممارسات الآمنة لعموم الموظفين

يستهدف هذا الفصل عموم الموظفين ويناقش مجموعة من الممارسات الآمنة والنصائح المطبقّة عادة والموجهة لكافة شرائحهم وتخصصاتهم والإدارات التي يتبعون لها، وهو الأساس الذي تُبنى عليه الممارسات الآمنة اللاحقة في هذا الدليل، وتعد هذه الممارسات إرشادات عامة وتذكيرية مع ملاحظة أهمية رجوع الموظف إلى إدارة الأمن السيبراني أو الإدارات المعنية في جهته للتأكّد من تطبيق سياسات الأمن السيبراني المعمول بها والالتزام الدائم بالضوابط الأمنية، كما يمكن تحقيق هذه الممارسات عن طريق التوعية الأمنية للموظفين وتحفيزهم لها، وفيما يلي تفصيل هذه الممارسات.

١. اتباع الاحترازات والإجراءات الأمنية في المرافق:

عند وجود قيود للدخول إلى بعض المرافق، قد يشعر الموظف بالحَرج مع ضيوفه أو مراجعيه في حال طلبهم منه أن يفتح الباب لهم (من خلال استخدام البطاقات الذكية أو البصمات أو ما شابهها) أو إسناد الباب حتى يدخلوا خلفه؛ لكن لابد للموظف أن يتجنب الاستجابة لمثل هذه الطلبات وألا يكون سببًا في تخطي الإجراءات، وفي حال وجود حرج بسبب النظام الأمني فيمكن للموظف طلب إجراء بديل من الإدارات المسؤولة.

٢. الالتزام بالسياسات والضوابط الأمنية:

وُضِعت السياسات والضوابط الأمنية في الجهات لتفادي المخاطر السيبرانية. من المهم تقيّد والتزام الموظف بتلك الضوابط وعدم محاولة تجاوزها لتفادي التسبب بحدوث ثغرات أمنية في الجهة؛ مثلًا، ألا يحاول الموظف ربط أجهزته الخاصة بالعمل بشبكات/خارجية، فمثل هذه الممارسات قد تكون سببًا في فتح ثغرات في غاية الخطورة للمخترقين على شبكة الجهة حيث تسمح بتخطي معظم الأنظمة الأمنية المعدة لحماية الشبكة الداخلية، وتُمكّن المهاجمين من الوصول إلى شبكة الجهة مما يعرّض الموظف للمساءلة في حال حدوث اختراقات لا سمح الله.

٣. حماية بيانات حساب المستخدم وكلمات المرور:

لابد أن يحرص الموظف على استخدام كلمات مرور قوية للأجهزة والحسابات البريدية وحسابات أنظمة العمل وعدم مشاركتها مع الآخرين، كما يمكن تخزينها في تطبيقات مشفرة للعودة إليها لاحقًا وإدارتها في حال مناسبة ذلك لسياسات الجهة. وينصح باستخدام خاصية التحقق الثنائي من خلال تفعيل رسائل التحقق على البريد الإلكتروني أو الهاتف المتنقل لضمان المحافظة على سرية البيانات الشخصية وبيانات الجهة.

٤. الاستخدام الآمن للإنترنت ووسائل التواصل الاجتماعي:

من المهم أن يتجنّب الموظف استخدام وسائل التواصل الاجتماعي عند تبادل البيانات أو الوثائق الخاصة بالعمل مهما كانت درجة أهميتها، وأن يحرص على عدم نشر المعلومات الحساسة أو الشخصية أو الوظيفية، عبر الإنترنت أو في مواقع التواصل الاجتماعي. ومن الأمثلة على ذلك رقم السجل المدني أو صورة الهوية الوطنية أو الرقم الوظيفي أو تاريخ الميلاد أو صور للمستندات الرسمية الأخرى مثل بطاقة العمل أو رخصة القيادة أو ما شابهها أو البيانات الطبية أو التعاميم و الخطابات السرية، حيث تعتبر تلك المعلومات بمثابة كنز في أيدي المتصيدين حيث يقومون بجمعها ثم استغلالها ضد الموظف في عمليات الهندسة الاجتماعية[٢] وحملات التصيّد الإلكتروني[٣] الموجهة للتواصل معه لإيهامه بأنهم ممثلين رسميين لجهة أو مصرف أو دوائر رسمية، ويستغلون كل تلك المعلومات التي جمعوها من شبكات التواصل الاجتماعي أو شبكة الإنترنت لكسب ثقة الموظف حتى يقع في شباك الاحتيال. هذه العمليات في ازدياد مستمر، وتتقمص بعض هذه الحملات شخصية شركات قد يكون الموظف على علاقة عمل معها لخداعه بتغيير وجهة إرسالية رسمية أو رسالة أو حوالة مالية.

٥. الحذر من حملات التصيّد الإلكتروني والهندسة الاجتماعية:

لابد للموظف أن يكون حذرًا من البريد التصيّدي والروابط غير الآمنة وتحميل المرفقات، وألا يثق بكل رسالة تصله. فقد شاعت في الآونة الأخيرة حملات الاختراق متعددة الخطوات التي تبدأ باختراق أجهزة زملاء الموظف أو حسابات التواصل الاجتماعي الخاصة بهم أو حساباتهم البريدية ومن ثم تراسل جميع معارفهم المسجلين لديهم لمحاولة اختراق أجهزتهم أيضًا. في حال تلقيّ الموظف رسالة مريبة من أحد معارفه أو زملائه من خلال أي قناة تواصل فمن الضروري أن يتأكد منها عن طريق التواصل المباشر مع المرسل.

٦. حماية البريد الإلكتروني:

يعدّ تجنب استخدام بريد العمل للأغراض الشخصية في غاية الأهمية، ويجب التأكد من حمايته بتفعيل خاصية التحقق الثنائي، بالإضافة إلى عدم كتابة بريد العمل في نماذج التسجيل الإلكترونية (Registration Form) أو مواقع وسائل التواصل الاجتماعي تفاديًا لتسريبه والاستفادة منه في التخطيط للاختراق. وفي حال الحاجة لإرسال ملفات مصنفة عبر البريد، لابد للموظف أن يطلب خصائص وأدوات التشفير من الإدارات ذات العلاقة.

٢ الهندسة الاجتماعية: الاحتيال على المستخدمين، وخداعهم للكشف عن معلومات حساسة وخاصة بهدف استغلالها لاحقاً لتنفيذ الهجمات على الأفراد والجهات.

٣ التصيّد الإلكتروني: أن يقوم المهاجمين بإيهام المستخدمين بمعرفة معلومات كافية عنهم للاستجابة لمتطلباتهم إما للحصول على معلومات حساسة أو تحويل الأموال لهم وغيرها.

٧. تحميل البرامج والأدوات الأصلية وتحديث الأنظمة:

على الموظف تجنّب تثبيت البرامج المقرصنة أو المجانية المشبوهة على أجهزة الجهة الرسمية أو الأجهزة الشخصية الموصلة بشبكتها، فقد تحوي بداخلها برمجيات تجسسية قد تكون وسيلة لاختراق جهاز الموظف وشبكة الجهة ككل، كما من الضروري أن يتأكد الموظف من وجود برنامج حماية على جهازه وأن يتم تحديثه بشكل دوري بحيث يتابع الموظف عملية التحديث التلقائية التي تصل لجهازه من إدارة تقنية المعلومات للتأكد من أن نظام التشغيل محدث بآخر نسخة، وألا يقوم بتعطيله لأي سبب كان.

٨. تصنيف ومشاركة الملفات:

لحماية الملفات ووثائق الجهة ورسائل البريد الإلكتروني وغيرها ومشاركتها بشكل سليم لا بد من وضع تصنيف واضح للملفات، مثل: متاح، أو سري، أو مقيّد وغيرها، ويمكن الرجوع للإدارة المعنية حول آلية تبني هذا التصنيف، وفي حال وجوده ينبغي للموظف أن يتأكد من صحة تصنيف الملفات المتداولة، كما يجب اتّباع البروتوكولات لمشاركة الملفات قبل تداولها والتي تحدد نطاق المشاركة المسموح بها على الملف من ولعل من أشهرها بروتوكول الإشارة الضوئية(TLP[٤]).

٩. النسخ الاحتياطي للبيانات ونقلها من مكان لآخر:

للمحافظة على المعلومات، لابد من عمل نسخ احتياطية منها دوريًا بالطرق المتاحة في جهتك وتخزينها في مكان آمن، وفي حال استخدام أجهزة التخزين الخارجية لحفظ النسخ، فمن المهم تشفير البيانات على تلك الأجهزة لمنع الوصول إليها لاحقًا من قبل أشخاص غير مصرّح لهم وخصوصًا عند فقدانها أو تعرضها للسرقة. كما من المهم الحذر من توصيل أي أجهزة وسائط تخزين غير آمنة بالجهاز لنقل الملفات إليها، مثل أجهزة ذاكرة البيانات (Flash Drives)، فهذه حيلة شهيرة للمخترقين حيث يتركون هذه الأجهزة في مكان عام ليغلب الشخص الفضول ليقوم بتوصيلها على غفلة بالجهاز الرسمي، وكثيرًا ما تحوي برامج خبيثة ولا تتطلب سوى توصيلها في الجهاز كي يصاب. وقد اشتهرت عمليات الاختراق لكبرى الجهات الخاصة والعامة الدولية من خلال هذه العملية البسيطة والتي أصبحت تعرف اليوم بمسمى "حملات الطُعم" (Baiting). فلا بد للموظف ألا يثق بتلك الأجهزة حتى وإن جاءت من شريك عمل أو ممثل رسمي لإحدى الشركات المعروفة، وفي حال استخدام وسائط التخزين الشخصية لابد من الحرص على فحصها ببرامج معتمدة لكشف البرمجيات الضارة قبل قراءة البيانات منها.

٤ TLP:Traffic Light Protocol

١٠.استخدام الخدمات السحابية:

على الموظف تجنّب وضع الملفات المصنفة لمشاريع وملفات ووثائق العمل في مواقع التخزين السحابية غير المعتمدة من قبل الجهة، وأن يستخدم الخدمات المعدّة من قبل الجهة، وفي حال عدم توفرها لابد من استخدام مزودي خدمة تنطبق عليهم المواصفات الأمنية اللازمة، ويمكن العودة إلى ضوابط الهيئة في الحوسبة السحابية[٥] للاستزادة.

١١. برامج الاجتماعات الافتراضية والعمل عن بُعد:

في بيئة الاجتماع عن بُعد والمستخدمة للتواصل مع الآخرين وأداء الأعمال دون الحضور لمقر العمل، قد ينسى البعض مراجعة إعدادات برامج الاجتماعات لتفعيل خواصها الأمنية، لذا:

- على الموظف تجنّب استخدام الخدمات المجانية العامة المستضافة خارج الوطن للنقاش أو للاجتماعات عن بُعد حول المشاريع الحساسة أو لتبادل ملفاتها قدر المستطاع، والحرص على التواصل مع إدارة الأمن السيبراني في الجهة لإيجاد البديل الآمن لتلك الخدمات.
- التأكد من مراجعة الخلفية الظاهرة عند تشغيل للكاميرا حتى لا تُكْشف أسرار الجهة دون علم الموظف، وتجنّب إرسال روابط الاجتماعات غير المحمية بكلمات مرور عبر وسائل التواصل غير الآمنة.
- التأكد من استخدام كلمة مرور قوية وتفعيل خاصية التحقق الثنائي لضبط الإعدادات على منصات الاجتماعات.
- التواصل مع الإدارات المعنية للتأكد من وجود أنظمة وتطبيقات معتمدة من الجهة والتي تتيح الوصول عن بعد والتعامل مع الملفات مثل "برامج الشبكة الخاصة الافتراضية" (VPN[٦]) وغيرها.

١٢. أجهزة العمل أثناء التنقل والسفر:

لابد من التأكد مما يلي:

- عدم الاتصال بالإنترنت من خلال شبكات مجانية سواءً كانت الشبكة اللاسلكية (Wi-Fi) أو شبكات الاتصالات التابعة للمرافق العامة أو الفنادق. وإذا دعت الحاجة لذلك فلابد من تفعيل خاصية "الشبكة الخاصة الافتراضية" (VPN) للجهة قبل نقل أي بيانات أو البدء في العمل عن بُعد من خلال تلك الشبكات غير الآمنة.

٥ ضوابط الأمن السيبراني للحوسبة السحابية https://www.nca.gov.sa/pages/ccc.html

٦ VPN: Virtual Private Network

- عدم شحن الأجهزة الذكية من محطات شحن عامة مجانية من خلال أسلاك المنافذ التسلسلية الشاملة (USB) الرباعية والمعدة لنقل البيانات، والاقتصار عند الضرورة على شحنها من خلال الأسلاك الثنائية المخصصة للشحن فقط دون نقل البيانات.

- إطفاء كافة خدمات الاتصالات وتشغيلها عند الضرورة فقط، مثل الشبكة اللاسلكية (Wi-Fi)، وتقنية الاتصالات الدانية (NFC[٧])، واتصالات البلوتوث (Bluetooth)، ونقاط البث (Hotspot)، فقد تفتح ثغرات يمكن للمخترقين استغلالها.

١٣. أمن الأجهزة الشخصية المتنقلة:

وتشمل أجهزة الحاسب المحمولة والأجهزة اللوحية والهواتف الذكية، حيث أصبحت سياسة السماح بإحضار الأجهزة الذكية إلى بيئة العمل (BYOD[٨]) مألوفة عند الكثير من الجهات، ولكن على الموظف التواصل مع إدارة الأمن السيبراني أو إدارة أمن المعلومات في الجهة لضمان التقيّد بسياساتها وضوابطها الأمنية ولضمان الاستفادة من الصلاحيات التي يمكن منحها للوصول إلى خدمات الجهة من خلال تلك الأجهزة بسهولة وأمان، كما يمكن الاستفسار عن الخدمات الأمنية المجانية التي ستحصل عليها الأجهزة من خلال هذا الإجراء.

١٤. الاستخدام الآمن للطابعات اللاسلكية وأجهزة إنترنت الأشياء (IoT[٩]):

- للطابعات اللاسلكية: إطفاء خاصية الطباعة عبر الشبكة اللاسلكية (Wi-Fi) أو البلوتوث في حال عدم حاجتها؛ فقد تستغل من قبل المخترقين.

- أجهزة إنترنت الأشياء (IoT): تستهدف هذه الأجهزة موجة جديدة من الاختراقات مثل الساعات الذكية والكاميرات الشبكية والطابعات وأجهزة العرض الشبكية (Projector) والأجهزة الطبية الشبكية وكذلك أجهزة التلفاز الذكية، لذا لابد من الحرص على تغيير الإعدادات المصنعية لتلك الأجهزة فور اقتنائها وضبط كلمة مرور جديدة لها بالاستعانة بالإرشادات المصنعية وبنصائح إدارة الأمن السيبراني في الجهة.

١٥. مغادرة المكتب:

عدم إتاحة الأجهزة أو الحسابات الإلكترونية بأنواعها للآخرين، فأي عمل تخريبي أو تجسسي يقع من خلال حسابات الموظف الإلكترونية في الجهة يعرضه إلى المساءلة النظامية لا قدر الله، لذا من المهم:

- تفعيل شاشة التوقف عند الغياب عنها مع ضبطها لتعمل تلقائيًا خلال دقائق معدودة مدعومة بكلمة مرور أو أجهزة التعرّف الذكية.

٧ NFC: Near Field Communication
٨ BYOD: Bring Your Own Device
٩ IoT: Internet of things

- اتّباع سياسة المكتب النظيف الذي لا يحتوي على أي معلومات تخص العمل أو صاحب المكتب مثل كلمات المرور أو أي وثائق سرية.

١٦. مراقبة علامات حدوث الخطر السيبراني:

هناك علامات مريبة قد تعني تعرّض الأجهزة للمخاطر السيبرانية، ومن المهم في حال ملاحظتها المسارعة في الكشف على الأجهزة وإبلاغ الإدارات المختصة في الجهة، ومن أبرزها:

- ارتفاع حرارة الجهاز على خلاف العادة
- فراغ البطارية سريعًا في الأجهزة المحمولة وعلى خلاف العادة
- ظهور رسائل غريبة وغير مألوفة ومفاجئة بطلب تحديث مريب، أو لتركيب برامج حماية، أو للتواصل مع الدعم المصنعي على هاتف دولي لوجود اختراق في الجهاز وما شابهها
- وقوع تغيير في البرامج أو الإعدادات بدون تدخل الموظف
- ظهور أدوات جديدة في شريط أدوات برنامج تصفح الإنترنت
- تحويل عمليات البحث في الإنترنت إلى مواقع أخرى لم يخترها الموظف
- تلقي أحد معارف الموظف رسالةً منه لم يرسلها
- تعطل صلاحية كلمة السر
- تعرّض شبكة الاتصال إلى بطء بدون سبب واضح
- تعطل برامج الحماية في الجهاز فجأة
- بطء غير معهود في الجهاز سواءً عند فتح المواقع أو الفيديوهات أو البرامج
- تعطّل البرامج تلقائيًا خلال عملها بدون سبب
- إعادة تشغيل تلقائية للجهاز بدون تدخل الموظف
- تفعيل تلقائي لملحقات الجهاز مثل الكاميرا أو الفأرة بدون تدخل الموظف
- عدم قدرة الموظف على فتح بعض ملفات العمل.

١٧. الإبلاغ عن الاختراقات والأحداث المريبة:

قد تكون السرعة في الإبلاغ سببًا للحد من تأثيرات الاختراق وتبعاته، لذا على الموظف مراقبة الأحداث المريبة والتبليغ عنها للإدارة المعنية بتلقي البلاغات السيبرانية في الجهة، ومن ضمن هذه الأحداث:

- تعطّل نظام إلكتروني تابع للعمل أو حصول تراجع في أداءه، وإن كان نظامًا غير أساسيًا
- تلقي أسئلة أو رسائل أو اتصالات مثيرة للريبة
- وجود شخص غير مصرح له بالدخول أو الزيارة أو غير متقيد بضوابط الزيارة
- وجود أجهزة غير مألوفة متصلة بالشبكة أو متروكة في أماكن مستنكرة
- مشاهدة مخالفات أمنية مثل وثائق أو معلومات مصنّفة في أماكن عامة أو كلمات سر مكشوفة أو أجهزة إلكترونية تعمل بدون وجود صاحبها أو أنظمة أمنية متعطلة مثل الأبواب الأمنية.

الفصل الثاني: الممارسات الآمنة للمدراء والقادة

من الضروري إلتزام المدراء والقادة بالممارسات الآمنة الخاصة بالموظفين والسابق ذكرها في الفصل الأول، إضافة إلى تبنّي الممارسات القيادية التي تمكّن منسوبي إداراتهم وتحفزهم على تعزيز ثقافة الحذر في بيئة العمل، ومنها ما يلي:

١. موازنة الإجراءات الأمنية مع إنتاجية الموظفين:

لابد للقائد أن يساعد في الموازنة، فالإجراءات الأمنية قيود في طبيعتها، ولكنها قيود حميدة وضعت للحماية ولمنفعة الموظفين و مصالح العمل، وهي ممارسات معتمدة ومقبولة لتمكين إتمام العمل بأقل قدر من المخاطر والتهديدات السيبرانية. كما أن إدارة الأمن السيبراني في الجهات ملزمة وحريصة على تقليل المخاطر. من المهم للقائد الاستماع إلى تجربة منسوبي إدارته لمعرفة ما إذا كانت الإجراءات الأمنية متوازنة مع أعمالهم وإنتاجيتهم، ومناقشتهم بشأن المخاطر والتهديدات الأمنية التي قد يتعرضون لها في الجهة، ثم يمكن الاجتماع بإدارة الأمن السيبراني لمناقشة ملاحظاتهم والبحث عن بدائل تجمع بين تحقيق الأمن السيبراني وتحقيق متطلبات الأعمال. مثال ذلك: قد تكون إدارة الأمن السيبراني حجبت الوصول إلى بريد العمل من خارج مقر العمل، ولكن يحتاج بعض الموظفين إلى تلك الخدمة من المنزل أو أثناء السفر أو التنقل، فبإمكان إدارة الأمن توفير تلك الخدمة للموظفين بأمان من خلال مجموعة من الأنظمة والتطبيقات التي تتيح الوصول الآمن بالإضافة إلى خدمة الشبكات الخاصة الافتراضية (VPN)، حيث قد يدفع انعدام مثل هذه البدائل البسيطة الموظفين إلى اللجوء إلى بدائل أكثر خطورة مثل التحاور حول مشاريع الجهة الحساسة من خلال البريد الإلكتروني المجاني أو وسائل التواصل الاجتماعي.

٢. استمرارية التحصين والتوعية:

على القائد فتح قنوات تعاون مستمرة مع إدارة الأمن السيبراني في الجهة تحقيقًا للأهداف التالية:

- توعية الموظفين الجدد فور التحاقهم بالعمل
- التوعية الدورية لكافة الموظفين بأبرز المخاطر الحديثة أو المستجدة
- إجراء التقييم واختبارات المحاكاة (Simulation Tools) للموظفين دوريًا لاختبار مدى وعيهم ويقظتهم في بيئات عملية
- اختبار معرفة الموظفين بالخدمات الأمنية في الجهة ومقدرتهم على الاستفادة منها
- مناقشة مرئيات الموظفين حول مدى سهولة استخدام الخدمات الأمنية الحالية وفرص التحسين
- مناقشة مدى إمكانية وضع جائزة عينية أو معنوية لأفضل إدارة ملتزمة بإرشادات وسياسات الأمن السيبراني في الجهة.

٣. تفقّد الممارسات والحرص على بناء القدوة:

من المناسب للمدراء خلق بيئة من الممارسات الأمنية المقبولة بين منسوبي إداراتهم وأن يكونوا قدوة للجميع في تبني هذه الممارسات، ومن ذلك تخصيص خمس دقائق في نهاية كل اجتماع:

- لمسح الملفات المؤقتة من الحاسبات المشتركة التابعة لغرف الاجتماعات
- لإزالة أو إتلاف الوثائق الورقية أو الإلكترونية التي أحضرها الموظفون للاجتماع
- لمسح ما تم كتابته على السبورة
- لتفريغ ما تم طباعته من الطابعة
- للتأكد من أن كلمات السر لأجهزة العرض وخلافه ليست متاحة للزوار.

٤. إدارة الحسابات والصلاحيات:

لابد من وضع توصيات يلتزم بها الموظفين فيما يخص الحسابات الإلكترونية الخارجية الموجهة إلى الجمهور أو الحسابات الداخلية الحساسة:

- الحذر من أن يشترك عدة موظفين في إدارة حساب واحد خارجي للجهة معد للتواصل مع الجمهور من خلال قنوات التواصل الاجتماعي مثل تويتر أو واتساب وغيرها، وذلك لحسن ضبط المسؤوليات. ولابد من استخدام البدائل لإدارة تلك الحسابات الخارجية الموحدة للجهة لدقة إدارة الصلاحيات التفصيلية لها، ولضبطها، ولتوثيق المسؤوليات والعمليات بوضوح، ويمكن الرجوع لضوابط الهيئة لحسابات التواصل الاجتماعي للمزيد من التفاصيل[١٠].

- عند الحاجة إلى التواصل مع الجمهور لأداء أعمال الإدارة، لابد من التنسيق أولًا مع إدارة الأمن السيبراني لاستخدام حلول بديلة وآمنة لتحقيق الهدف من التواصل مثل "النماذج الإلكترونية" المزودة بتقنيات حماية خاصة بدلًا من استخدام حسابات بريد إلكتروني مؤسسية، لأن ذلك سيجنب الجهة استقبال رسائل البريد الإلكتروني الاقتحامية (SPAM) أو المشبوهة. وفي حال الحاجة إلى نشر عنوان بريد إلكتروني رسمي في أماكن عامة مكشوفة، فلابد من استخدام عناوين قابلة للإتلاف والاستبدال لاحقًا بدلًا من حسابات موظفين محددين، أو الاستعانة بعنوان مُكنّى "alias" عن العنوان الحقيقي، عن طريق إعدادات البريد الإلكتروني.

- لابد من الحرص على عدم نشر حساب البريد الإلكتروني أو عناوين بريد منسوبي الجهة في أي وسيلة إلكترونية سواءً كانت تابعة للجهة أو تابعة لمؤتمر حضره الموظفين أو أي مناسبة أخرى، فيحصد المخترقون تلك العناوين من الإنترنت من خلال برامج آلية ثم يستهدفونها في حملات الاختراق لنشر البرامج الضارة والرسائل التصيدية.

١٠ ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات https://www.nca.gov.sa/files/OSMACC.pdf

- تحتّم طبيعة أعمال بعض الموظفين تملكّهم لحسابات إلكترونية خاصة ذات صلاحيات حساسة وذلك للدخول إلى أنظمة داخلية تخص أعمال الجهة أو للدخول إلى البنية المعلوماتية ذاتها أو للاطلاع على بيانات العملاء الحساسة. وكثيرًا ما تكون تلك الحسابات مستقلة عن حسابات الموظفين الاعتيادية. على القائد حثّ الموظفين على عدم استخدام تلك الحسابات إلا للضرورة القصوى ولأقصر الفترات الزمنية الممكنة وعدم مشاركتها مع زملائهم لأي سبب واتباع أفضل الممارسات الأمنية عند استخدامها. وألا تُستَخدم لتصفح الإنترنت أو للمراسلات البريدية مثلًا، لأن اختراقها أشد ضررًا وخطورة على الجهة من اختراق حسابات الموظفين الاعتيادية، حيث سيساهم ذلك في منع وقوع الأخطاء غير المقصودة من جانب الموظفين والتي تعد من أهم أسباب المخاطر السيبرانية في الجهات.
- التأكّد من تفعيل خواص التحقق الثنائي لجميع حسابات الجهة قدر المستطاع.

٥. إرسال المرفقات بأمان:

من الضروري أن يتجنّب القائد إرسال البيانات المصنّفة من خلال وسائل إلكترونية غير مشفرة وغير آمنة إلى فريقه أو إلى خارج الجهة. ويمكن الاجتماع مع منسوبي إدارة الأمن السيبراني في الجهة للاتفاق على قنوات آمنة لتبادل تلك الملفات مع الآخرين، إما من خلال بريد إلكتروني مشفر، أو من خلال مستودعات ملفات سحابية مشفرة مستضافة داخل الجهة أو داخل الوطن.

٦. الحد من عواقب السرقة والفقدان لأجهزة العمل:

على القائد التنسيق مع إدارة الأمن السيبراني في الجهة لضمان تفعيل خواص التشفير الداخلية لبيانات الأقراص (Hard Disk) لكافة الأجهزة المحمولة ضمن الإدارة، مع تفعيل خواص تتبع الأجهزة أيضًا. ولابد من معرفة أن وجود كلمة سر على تلك الأجهزة غير كافٍ لمنع سرقة المعلومات الحساسة من الجهة في حال نَزْع السارق القرص من داخل الجهاز وتثبيته في حاسب آخر، إلا إذا كانت البيانات مشفرة مسبقًا.

٧. إدارة الأطراف الخارجية:

على القائد التأكد من وجود سياسات للتعامل مع الأطراف الخارجية واتباعها، والتأكد من اختيار الأطراف الخارجية وفقًا لأعلى المعايير، والمحافظة على سياسات الخصوصية وحفظ الملكية الفكرية للأعمال، كما لابد من المحافظة على بيانات الجهة أثناء وبعد إنهاء الأعمال واتباع مبدأ "الحد الأدنى من الصلاحيات" (The Principle of Least Privilege) الذي يسمح للوصول للموارد ولكن بأقل صلاحيات ممكنة لحمايتها والتحكم بها بشكل أفضل.

الفصل الثالث: الممارسات الآمنة لموظفي تقنية المعلومات ومختصي الأمن السيبراني

تستند الممارسات الآمنة الموجهة للموظفين المختصين سواءً في تقنية المعلومات أو الأمن السيبراني على الممارسات المذكورة مسبقًا في الفصل الأول، لكنها تختلف حيث يتمتّع المختصون بوصولٍ مباشر للممتلكات والأصول التقنية والبنية التحتية للجهة وبصلاحيات للوصول قد تكون عالية للغاية، لذلك يستعرض هذا الفصل الممارسات الآمنة المناسبة لهم مع أهمية الرجوع للضوابط والإرشادات التي تصدرها الهيئة الوطنية للأمن السيبراني[١١] من النواحي التقنية لتحصين موظفي هذه الإدارات من المخاطر السيبرانية، فيما يلي نناقش بعضًا منها:

١. الحذر عند نشر السيرة الذاتية:

إذا نشر الموظف سيرته الذاتية في المواقع المهنية والمختصة في التوظيف لابد أن يحذر من كشف أسرار البنية المعلوماتية للجهات من خلال سرد المنتجات التقنية التي يتقنها والمقترنة بمسمى الجهة و المشاريع التقنية الحساسة التي عمل عليها. حيث يستغل المخترقون ذلك في مرحلة جمع وحصد المعلومات التمهيدية التي تسبق مرحلة التخطيط لاختراق الجهات.

٢. البرمجة الآمنة:

لابد للمبرمجين تجنّب زراعة حسابات رسمية وكلمات مرور بداخل النصوص البرمجية للتطبيقات الرسمية التي تطورها الجهات، فبإمكان المخترقين إعادة هندسة تلك البرامج وانتزاع تلك الحسابات من داخلها، واستغلالها لاختراق الجهة. لذا نوصي بتطبيق المبادئ الأساسية للبرمجة الآمنة التي تتبع المعايير الدولية لحماية البرمجيات أثناء مراحل التطوير.

٣. التخلّص الآمن من الأجهزة:

على الموظف أن يتأكد من سياسة الجهة حول إتلاف الأجهزة والمعدات التي لا يستفاد منها، وألا يتخلص منها بطرق غير آمنة، فقد تحتوي على بيانات يمكن للمخترقين أن يستعيدوها ويسيئوا استخدامها.

١١ ضوابط وإرشادات الأمن السيبراني https://www.nca.gov.sa/pages/legislation.html

٤. عدم تطبيق الأمن بالتجزئة:

تتبنى بعض الجهات مبادرات أمنية متفرقة عامًا بعد عام، لتنتهي بعد عدة سنوات كشبكة معقدة من أنظمة متفرقة مستقلة أو مرتبطة بصفة غير مثالية ببعضها البعض بجسور معلوماتية. لذا لابد من الحرص على تبني مبادرة شاملة للأمن السيبراني تحت غطاء أحد المعايير الدولية الشهيرة، ثم تصبح كل مبادرة جديدة جزءًا لا يتجزأ من المبادرة الموحدة، وأن يكون تصنيف البيانات والموارد دائمًا دافع لكل قرار وعمل، وليس العكس.

٥. شبكة الجهة وأجزاؤها الفرعية:

من الضروري تحسين وترسيخ القواعد الأساسية لشبكة الجهة قبل بناء أي أنظمة سيبرانية، وذلك لأن أي نظام إلكتروني أو إجراء أمني مهما كان ذكيًا يعتمد بصفة أساسية على جودة ما سبقه من أعمال الفصل والتخصيص للشبكات الفرعية للجهة. ولذلك فإن حسن التخطيط و التصميم لتلك الشبكات سيحد من حجم السجلات الواجب قراءتها من قبل أنظمة الأمن السيبراني الذكية وفريق المراقبة الأمنية، مع الحد أيضًا من التنبيهات الآلية الخاطئة. كما أن ذلك سيسهم في سد كثير من الثغرات التي يقع ضحيتها الكثير بسبب الثقة المطلقة بأنظمة الحماية الخارجية والتغافل عن الحماية الداخلية الاحترافية بين الأنظمة، وإن مجرد تطبيق أفضل التقنيات الحديثة الأمنية فورًا على شبكة قائمة بدون اتباع تلك الإجراءات أولًا سيؤدي إلى نظام أمني محدود الكفاءة ويرفع الحاجة إلى فريق مراقبة كبير مع ثغرات عديدة غير مكتشفة.

٦. فصل الشبكات لرفع مستوى الأمان:

من المعلوم أن كافة الشبكات بداخل أية جهة تحوي شبكات نمطية مثل شبكة المنطقة المحايدة (DMZ[١٢]) التي تحوي خادم موقع الإنترنت للجهة وخادم البريد المؤسسي وخادم المفوض الشبكي وخوادم الشبكات الخاصة الافتراضية (VPN) وغيرها. وأيضا الشبكة الداخلية التي تحوي أنظمة الأعمال الحساسة. والسؤال: هل تم تصميم وفصل الشبكة بموجب دراسة أولية متعمقة لخصوصية تصنيف موارد الجهة تحديدًا؟ إن كان الجواب "لا" فلابد من البدء بتأسيس قواعد متينة لأمن موارد الجهة من خلال اتباع الخطوات التالية:

١٢ DMZ: Demilitarized Zone (DMZ)

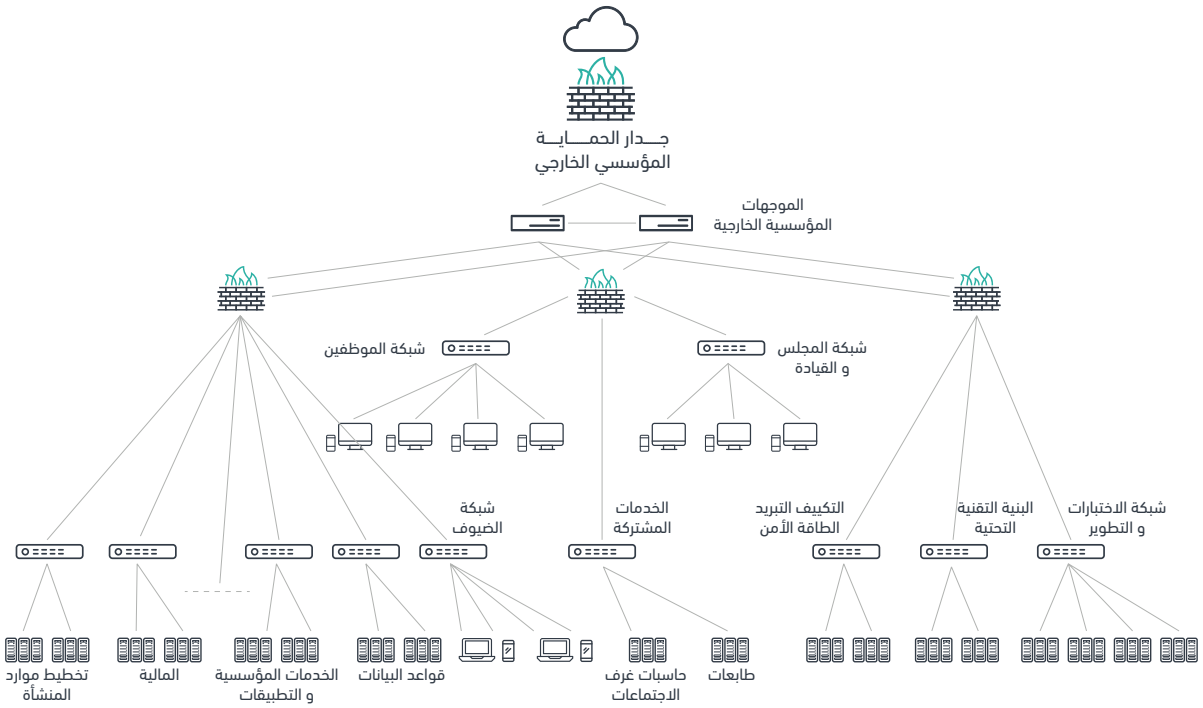
رسم توضيحي ١: دورة حياة هندسة وفصل الشبكات بموجب تصنيف الموارد والبيانات

- **التعريف:** تحديد وتوثيق الموارد الشبكية وأهمية كل منها للجهة، بالإضافة إلى مدى احتمال انتهاكها، وتتألف على الأقل من الأجهزة والبرامج والمعلومات.
- **التصنيف:** تصنيف شامل لكافة الموارد بداخل الجهة مرتبة حسب حساسيتها وأهميتها.
- **صياغة السياسة:** وتتم بموجب التصنيف الشامل السابق لموارد الجهة لجمعها ضمن فئات، ويمكن بعد ذلك الاسترشاد بتلك الفئات للتخطيط لحدود ومكونات الشبكات الفرعية الداخلية.
- **صلاحيات الوصول Access control:** حيث يتم أولًا تصنيف كافة الموظفين إلى فئات حسب أدوارهم ومسؤولياتهم، ومن ثم صناعة "جدول توزيع الصلاحيات" لربط كل فئة من الموظفين بفئات الموارد المناسبة لأدوارهم الوظيفية، شاملًا الصلاحيات المطلوبة لتحقيق ذلك.
- **التنفيذ:** في هذه المرحلة يتم التخطيط للتصميم الشبكي والأمني اللازم لتحقيق ما تم التوصل إليه في الخطوة السابقة على أرض الواقع، شاملاً تحديد الأجهزة والبرمجيات المطلوبة، والمخططات التقنية، ومتطلبات المراقبة الفعالة، والتنفيذ.
- **المراقبة:** وهي عملية مستمرة مبنية على الخطوات السابقة لضمان التقيد المستمر بكافة التصنيفات والصلاحيات المخطط لها في الخطوات السابقة على الدوام. وعلى قدر التأني والتفصيل في الخطوات السابقة ستكون عمليات المراقبة أكثر كفاءة ودقة وأقرب إلى الأتمتة الفعالة.

ومن المهم الإشارة إلى أنه لا ينبغي الاستعانة بكافة هذه الوثائق والإجراءات مرة واحدة في دورة حياة هذه الموارد ثم تخزينها بعيدًا عن الأنظار، بل لا بد من الاستعانة والاسترشاد بها وتحديثها باستمرار للمحافظة المستمرة على موارد الجهة وبنيتها التحتية.

من المهم أن تقود حساسية وتصنيفات الموارد للجهة التصميم الشبكي النهائي وتفريعاته، وليس العكس، فترتقي كفاءة كافة الإجراءات والأنظمة الأمنية الأخرى تلو ذلك. ومن أمثلة تلك الخطوات:

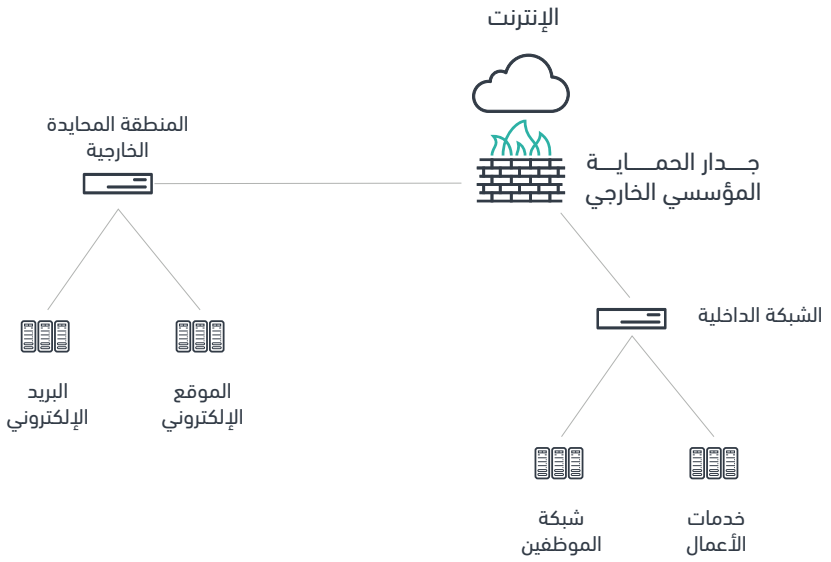
أ) فصل شبكة الخوادم إلى العديد من الشبكات الفرعية، (أنظر إلى شكل ٢) مثل: شبكة الأنظمة المشتركة لكافة الموظفين كبوابة العمل الداخلية، وشبكة الأنظمة المخصصة لإدارات بعينها مثل الإدارة المالية والتي لا ينبغي الدخول إليها إلا من قبل موظفي المالية، وشبكة لأنظمة مجلس الإدارة وبياناته، وشبكة لبيانات وأنظمة عملاء خدمات الجهة الأساسية، وربما شبكة لأنظمة الاجتماعات عن بُعد والتي قد تتطلب صلاحيات كثيرة ومتفرقة للمنافذ والبروتوكولات المفتوحة، وشبكة لأنظمة مركز المعلومات المخصصة للتبريد والمراقبة والإنذار والطاقة الاحتياطية، وشبكة لا يدخلها سوى مهندسو الشبكة والتي تحوي خوادم المراقبة الشبكية وخوادم إدارة أسماء النطاقات الداخلية وما شابهها، وشبكة لأنظمة قواعد البيانات، وشبكة الاختبارات والتي تحوي الأنظمة الإلكترونية عالية المخاطرة قيد التطوير والتي لم تخضع بعد إلى التحصين الأمني. من فوائد ذلك أنه في حال كانت كافة الخوادم في شبكة واحدة وتم اختراق خادم الاتصال عن بُعد -مثلًا- وبدأ المخترق في محاولة الانتقال منه إلى خادم الحسابات المالية، فغالبًا سيصعب اكتشاف ذلك من خلال الأساليب التقليدية. أما في حال عزل كلٍ منهما في شبكة فرعية متخصصة، وتحسين تصميم قواعد اتجاهات سيل البيانات وقائمة المنافذ الشبكية المسموح بفتحها، فستتنبه الأنظمة الآليةإلى أن محاولات الاتصال الأفقية بين الخوادم مستنكرة وغير مألوفة.



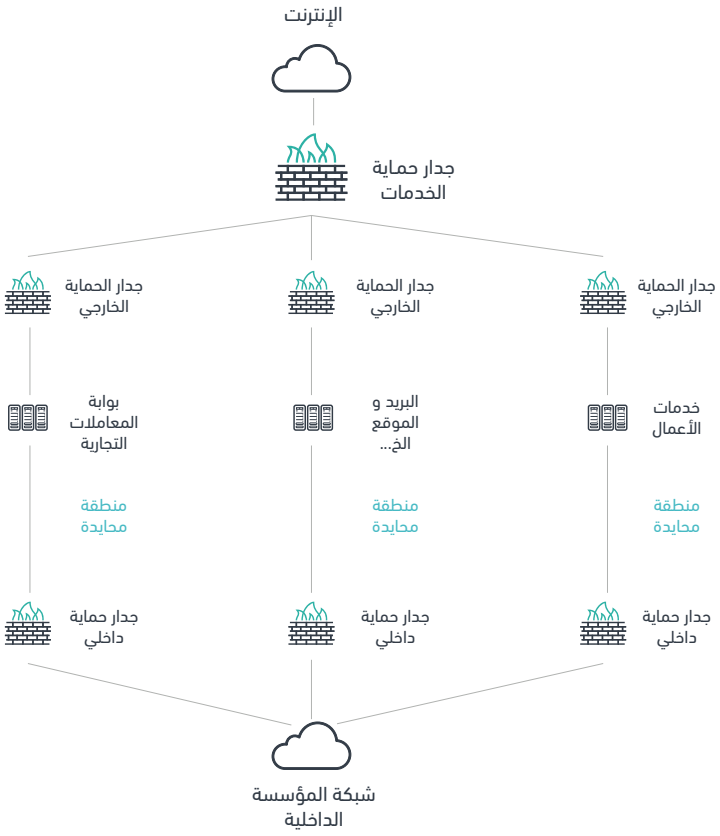
شكل ٢: أحد نماذج الطرق الممكنة للتقسيم التفصيلي للخدمات الداخلية للحد من التحرك الأفقي بعد الاختراق

ب) فصل شبكة الموظفين إلى شبكة لحاسبات الموظفين، وشبكة للطابعات وأجهزة العرض، وشبكة للحاسبات المشتركة لغرف الاجتماعات، وما شابه ذلك.

ج) شبكة المنطقة المحايدة – (DMZ): وهي تحوي خوادم البريد الإلكتروني، وخوادم استضافة الموقع الخارجي، وخوادم أسماء النطاق الخارجية، وخوادم الهواتف الرقمية، ومفّوضات الإنترنت(Proxy) للجهة وما شابهها من خدمات، وهي بحاجة إلى التواصل مع العالم الخارجي والخدمات الداخلية بآن واحد (أنظر إلى شكل ٣). حيث أن المخاطر الحديثة قد دفعت مهندسي الشبكات إلى إعادة النظر في التصميم التقليدي والمتكون من وعاء واحد يحوي كافة تلك الخدمات، والتحول إلى تصاميم أكثر ضبطًا وأمانًا متمثلة بعدة شبكات فرعية يفصل بينها جدار حماية واحد أو أكثر مثل شبكة خوادم الموقع الإلكتروني والتطبيقات الخارجية، وشبكة قواعد البيانات الخارجية، وشبكة التحقق من الهوية، وشبكة خوادم الشبكة الافتراضية الخاصة، وشبكة البريد الإلكتروني والتطبيقات الذكية، وهكذا (أنظر إلى شكل ٤). لهذه الشبكات دراسات تفصيلية كثيرة يمكن للمهتم الخوض فيها، حيث يمكن فصل تلك الشبكات إلى شبكات متوازية أو طبقية تفصل بينها جدر حماية مستقلة. وتمنح كل تلك التصاميم مستويات إضافية من التحكم بالمنافذ الواجب فتحها أو أغلاقها وباتجاهات البيانات المنطقية المقبولة وما شابه ذلك.



شكل ٣: شبكة منطقة محايدة تقليدية



شكل ٤: إحدى طرق تنفيذ شبكة منطقة محايدة مقسمة

يتيح فصل الشبكات بناءً على الوظائف والتخصصات مستويات متميزة للتحكم في المنافذ والصلاحيات المطلوبة بينها من خلال جدار الحماية والبدالات الشبكية الداخلية (Switches) مع ضرورة التضحية ببساطة التصميم. فلن تحتاج شبكة الطابعات إلى صلاحيات الوصول لخوادم البريد الإلكتروني أو خوادم استضافة الموقع الإلكتروني الخارجي ومفوّضات الإنترنت (Proxy) مثلًا. ومثل هذا التقسيم يسهم في:

- التصدّي الفعال للتحركات الأفقية داخل الشبكة وبين الخوادم والأجهزة، ويعد هذا من أكبر الثغرات الحديثة التي ينبغي التركيز عليها من قبل كافة الجهات المختلفة. فقد أصبحنا نعيش اليوم في بيئة يصعب أن تُسْلم فيها أي جهة من محاولات اختراق، لكن من الممكن الحد من تأثيراتها من خلال مثل هذه الإجراءات.
- رفع كفاءة أداء أنظمة المراقبة الأمنية التقليدية أو المبنية على الذكاء الاصطناعي لتحليل سمات الاتصالات، فأي حياد عن تلك السمات النمطية الحصرية سيولد تنبيهًا مبكرًا للفريق الأمني. وقد أصبحت كثير من شركات الأمن السيبراني اليوم تركز على تقديم حلول متعددة لرصد التحركات الأفقية تحديدًا.
- حصر الاختراقات في مناطق ضيقة، ومضاعفة الجهد المطلوب من قبل المخترق للتحرك الأفقي بين الخوادم مما يزيد من فرص اكتشافه قبل تفاقم تبعات الاختراق.

- رفع القدرة على سرعة الاستجابة لعزل الشبكات المخترقة دون الحاجة إلى إيقاف كافة الخدمات.
- تسهيل مهام التحرّي بعد الاختراق لتتبع خطواته وأبعاده نظرًا إلى وجود العديد من المستويات والأجهزة التي تولد السجلات ذات العلاقة.

ومن المهم للجهات أن تجري الدراسات اللازمة لتبني التصاميم المذكورة سابقًا لوزن إيجابياتها مع سلبياتها في ضوء حساسية معلومات الجهة وأنظمتها المعلوماتية، حيث ستكون بعض التصاميم مكلفة ماديًا وتزيد من متطلبات دقة الهندسة والتصميم الأولية، وتزيد من مهام التنفيذ التأسيسية لقواعد النفاذ المسموحة أو المرفوضة ولقواعد المراقبة، وتزيد بطبيعة الحال من الأحمال على الأنظمة الأمنية خلال أدائها للمهام الشبكية اليومية.

٧. تطبيق استراتيجيات الأمن السيبراني:

من أهم الاستراتيجيات التي نوصي بتطبيقها أثناء تصميم وإعداد وبناء البنية التحتية للشبكة ومواردها هي استراتيجية "الدفاع العميق" (Defense in Depth) والتي تسعى إلى وضع سلسلة من الآليات الدفاعية لحماية البيانات والمعلومات القيمة، بحيث إذا فشلت إحدى الآليات، تتقدم الآلية الأخرى على الفور لإحباط أي هجوم. كما ترتبط هذه الاستراتيجية بمبدأ "الدفاع متعدد الطبقات" (Multilayered Defense) بحيث تكون هناك منهجية أمان للشبكات تستخدم عدة مكونات لحماية العمليات التي تجري في الشبكة. كذلك يمكن تطبيق مبدأ "التجزئة الدقيقة" (Micro Segmentation)، الذي يقسم الشبكة إلى قطاعات معزولة يمكن مراقبتها والتحكم في مرور البيانات من خلالها. ومن المناسب الاطلاع على هذه المبادئ ودراسة مدى جدواها لحاجة الجهة بحيث تمكّن المشرفين على الأمن والشبكات أن يراقبوا الموارد بطريقة أفضل.

٨. عدم جمع كافة المُورّدين في بوابة دخول واحدة:

تتعامل كل جهة مع أطراف خارجية مثل المورّدين وغيرهم لتقديم خدمات ضرورية لصحة وحيوية خدماتها وشبكاتها، بعضهم مورّدين للعتاد الشبكي، وبعضهم لمعدات البنية التحتية مثل التكييف أو أجهزة مكافحة الحرائق أو أجهزة الطاقة الاحتياطية، وبعضهم للبرمجيات وتطويرها ودعمها، وبعضهم لقواعد البيانات. ومن المهم منح كل مُورّد بوابة دخول مفصّلة لخصوصية احتياجاته وحده دون زيادة أو نقصان لمنع سوء الاستغلال في حال تسرب تلك الحسابات.

٩. الأصل هو الإغلاق (Block All Policy):

يجب أن تكون القاعدة "الأصل هو الإغلاق" لكافة المنافذ والشبكات والبروتوكولات في كافة الأجهزة الشبكية والمعلوماتية، ثم يبدأ الموظف في فتح ما يحتاج إليه للضرورة مع أهمية توثيق سبب كل سطر من الصلاحيات بداخل إعدادات كل جهاز، فعدم التوثيق قد يؤدي إلى فتح الثغرات لاحقًا، فلو تغير التوزيع الشبكي والخدمات الشبكية لاحقًا وتم إلغاء أو نقل بعض الخدمات فقد تبقى تلك الصلاحيات مفتوحة في إعدادات الأجهزة الشبكية بسبب استقالة الموظف المسؤول أو نسيانه لسبب وجودها.

١٠. صمام البيانات:

في حال وجود بيانات وأجهزة شديدة الحساسية بحاجة إلى التواصل مع العالم الخارجي ولكن حساسيتها لا تسمح بتبني الحلول الأمنية مثل جدر الحماية وأنظمة منع التسلل (IPS) أو نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM[١٣])، وما شابهها، فيمكن النظر في جدوى اللجوء إلى تقنية صمام البيانات وهي أجهزة تسمح بسيل البيانات باتجاه واحد فقط. فيمكن استغلالها مثلًا لفصل شبكات تقنيات التشغيل والتحكم عن شبكات مستودعات البيانات، مما يسهم بصفة إيجابية في أعمال الامتثال السيبراني. يجدر الذكر أن الشركات المحلية أصبحت تصنع هذه الأجهزة وطنيًا.

١١. التطوير المستمر للأدوات:

إذا كان الموظف لايزال يستعين بأنظمة كشف التسلل (IDS) وأنظمة منع التسلل (IPS) التقليدية فقد يستحسن أن يدرس مدى جدوى التحول إلى تقنيات (SIEM) الحديثة بدلاً منها نظراً لما لها من مميزات في شمولية الرؤية للشبكة والمقارنة بين الأحداث الصغيرة والمتفرقة في أماكن متعددة من الشبكة والتي في مجملها قد تدل على عملية اختراق قائمة.

١٢. التأكد من سلامة النسخ الاحتياطية:

لا يتوقع أحد أن يُخترق وتتلف بياناته، لكن احتمالية الاختراق ستظل قائمة مهما وضعنا حلول أمنية وقائية، وقد تُمثّل القدرة على استعادة بيانات الجهة بعد هجمة ابتزازية أو تخريبية الفرق بين استمرار عملها من عدمه. لذلك لابد من اتباع أفضل الممارسات المعيارية لتصميم وبناء وتشغيل أنظمة النسخ الاحتياطي لبيانات العمل الحساسة. ولا ننسى أن كثير من تلك الأنظمة تفشل عندما يكون أصحابها بأمس الحاجة إليها، لذا من المهم الحرص على وضع خطة لاختبار تلك النسخ بصفة دورية وحفظها في بيئات آمنة معزولة عن مخاطر الشبكة الرئيسية.

١٣. النسخ الاحتياطي لإعدادات الأنظمة:

من القضايا التي يغفل عنها الكثير أو يستهين بها هي الوقت المطلوب لإعادة بناء بعض أو كل الخوادم المركزية بعد تعرضها إلى اختراق أو إتلاف، لذلك من المهم دراسة مدى جدوى حفظ نسخ احتياطية من إعدادات الأنظمة والتطبيقات المؤسسية التابعة لها (System and Application Image) لتسهم في القدرة على سرعة إعادة بناءها من الصفر في حال الحاجة إلى ذلك.

١٣ SIEM: Security Information And Event Management

١٤. تفعيل سجلات متابعة الأحداث:

من الضروري أن يكون هناك طريقة لتسجيل كافة الأحداث التي تتعرض لها الأنظمة والشبكات وكذلك الأجهزة طوال فترة عملها (Event logs)، وأن تكون هناك متابعة دورية لها للتأكد من سلامتها وقت الحاجة، سواءً لاكتشاف الأخطاء أو لمعرفة مسببات الاختراقات وغيرها من الاستخدامات.

١٥. سياسة التشفير:

دراسة مدى جدوى ومناسبة فرض سياسة التشفير على أجهزة الموظفين جميعًا أو أجهزة موظفين مخصصين ممن يملكون صلاحيات خاصة للوصول إلى بيانات حساسة، ويمكنك الاطلاع على المعايير الوطنية للتشفير الصادرة من الهيئة بهذا الخصوص[١٤].

١٦. تتبع الأجهزة عن بُعد:

تفعيل خاصية تتبع الأجهزة المتنقلة (Tracking) وخاصية مسح الأجهزة عن بعد (Remote Wiping)، وهذه الخصائص مضمنة في أشهر أنظمة التشغيل الحديثة مجانًا، وذلك لتلافي الأخطاء الناجمة عن ضياع أو سرقة الأجهزة.

١٧. الوعي من الميدان:

للمختصين في التقنية أو في الأمن السيبراني الذين يرأسون مجموعة من الموظفين لابد من الحرص على توعية وتدريب منسوبي إداراتهم باستمرار وليس من الضرورة أن يكون ذلك من خلال دورات داخلية أو خارجية مكلفة، ولكن هنالك العديد من الطرق الإبداعية التي لا تكلف شيئاً، ومنها أن تمد جسور التعاون مع الجهات المشابهة لتبادل التجارب والمعارف من حين لآخر من خلال اللقاءات وورش العمل، أو من خلال استحداث مجموعات إلكترونية مشتركة آمنة بين المختصين في تلك الجهات لبحث بعض القضايا والمستجدات وطلب الاستشارة والحلول.

١٨. عناوين شبكة الضيوف:

من أبسط الإجراءات التي يمكنك تطبيقها لعزل شبكة الضيوف ومنع التسلل منها إلى الشبكات الداخلية الحساسة الأخرى هي تغيير الترقيم الشبكي لتلك الشبكة ليكون مختلفًا عن ترقيم بقية الشبكات. فإذا كانت الشبكات الداخلية مثلًا تستخدم العناوين (192.168.10.X) فالأفضل أن تكون عناوين شبكة الضيوف (192.168.50.X) أو (10.0.0.X).

١٤ المعايير الوطنية للتشفير https://www.nca.gov.sa/pages/ncs.html

١٩. على الموظف أن يكون صديقًا:

ألا يفرض الموظف المسؤول الحلول على الإدارات فرضاً بل يشاركهم في القرار وفي الحلول ويحرص على توعيتهم بالمخاطر والتهديدات والحوادث السيبرانية المعلنة وكذلك بأسباب وأهداف كل إجراء أو قرار ليتبنونها عن قناعة ولا يقدمون على إهمال تطبيقها لاحقاً.

٢٠. مكافحة عمليات الاستكشاف ورفع البصمات:

إنّ أول خطوات الاختراق هي خطوة استكشاف شبكات وخوادم الضحايا، حيث يسعى المخترقون إلى جمع أكبر قدر ممكن من المعلومات حول شركات تصنيع أجهزة الجهة الشبكية وأنظمة تشغيل الخوادم وإصداراتها ونوع برنامج النشر على الويب وإصداره ونوع وتفاصيل موزع الأحمال(Load Balancer) أو الجهاز الشبكي المستهدف وغيره، وفي الغالب يتم التعبير عن هذه المرحلة "بمرحلة رفع البصمات". توجد اليوم العديد من البرامج المجانية والمؤتمتة مفتوحة المصدر لجمع تلك البيانات بفاعلية، وهي متنوعة مع تخصص كل منها بمستوى مختلف من المكونات الشبكية، على الموظف أن يستخدم تلك الأدوات قبل المخترقين لكشف أي تسربات في معلومات وهويات مكونات الشبكة، ثم يقوم بتغييرها للتمويه على المخترقين وتصعيب مهمتهم. فكثيرًا ما ينتقل المخترق من ضحية إلى أخرى فقط بسبب صعوبة جمع البيانات الأولية الممهدة للاختراق.

٢١. الامتداد الآمن لأسماء النطاقات:

إن من أكثر الأساليب فاعلية للاختراق وحصد الحسابات هي اختراق خادم أسماء النطاقات للجهة الضحية. فحينها يمكن تحويل كافة طلبات المواقع الإلكترونية إلى مواقع محتالة تشابه الموقع الحقيقي تمامًا ولكنها تحصد حسابات الضحايا ليتمكّن المخترقون من استغلالها لاحقًا لاختراق الجهة بكافة خدماتها بدون عناء. ومن أنجح الطرق لمكافحة مثل هذه الهجمات: تبنيّ تقنية الامتداد الآمن لأسماء النطاقات (DNSSEC[١٥]). وتوجد حلول وطنية مفصلة وفعالة للاستفادة من هذا البروتوكول ويمكن الحصول على المزيد من المعلومات في ذلك من خلال التواصل مع المركز السعودي لمعلومات الشبكة[١٦]. كما أن لدى المركز معلومات ثرية حول التبني الفعال للإصدار السادس من عناوين بروتوكول الإنترنت (IPv6) والذي يحتوي على العديد من المزايا الأمنية السيبرانية لتحصين الشبكات.

١٥ DNSSEC: Domain Name System Security Extensions

١٦ المركز السعودي لمعلومات الشبكة https://nic.sa

٢٢. تحصين خدمة توقيت الشبكة:

من ضمن الخدمات الشبكية التي يستهين بتحصينها الكثير من المختصين، خدمة بروتوكول التوقيت الشبكي (NTP[١٧]) وهذه الخدمة جذابة للمخترقين لقلة حصانتها في العادة وسهولة تعطيل خدمات الجهات في حال إغراق خوادمها بطلبات خارجية، ولوجود طرق لاستغلال ذلك البروتوكول في مراحل "المصافحة Handshake" بين تطبيقات العميل والخوادم المركزية والتي قد تتيح تقمص شخصية أحدهما أو سرقة حساباته. هناك العديد من الإجراءات الوقائية الممكن تطبيقها للحماية من ذلك كله، على رأسها الربط بالخدمة الوطنية للتوقيت الشبكي والتي تشرف عليها الهيئة السعودية للمواصفات والمقاييس والجودة[١٨]، ومن ثم اتباع أفضل الممارسات السيبرانية لتحصين تلك الخدمة مثل إغلاق المنفذ 123 باتجاه الإنترنت وإطفاء أمر monlist وغيرها.

٢٣. برمجيات الفدية والاختراقات من الداخل وإنترنت الأشياء (IoT):

تتعدّد أساليب الاختراق وتتحوّر يومًا بعد يوم، ولكن من أبرزها وأسرعها نموًا اليوم كمًّا ونوعًا وأكثرها فاعلية: برامج الفدية والاختراق من الداخل، سواءً المباشرة أو التي تتم من خلال التصيّد والخداع، لذلك من المهم بناء خطط التوعية وبرامج التدريب وأنظمة الأمن السيبراني في الجهة في ضوء تلك الحقائق.

٢٤. تنامي هجمات إنترنت الأشياء (IoT):

إن هجمات الاختراق على أجهزة إنترنت الأشياء في نمو ملحوظ على الصعيد الدولي مؤخرًا، لذلك من المهم تضمينها في الخطة الأمنية. مثلًا: هل لدى الجهة أجهزة تلفاز ذكية في المكاتب أو غرف الاجتماعات؟ هل لدى الجهة كاميرات شبكية (IP Camera)؟ هل يعلم الموظفون أنها من أكثر الأجهزة الشبكية عرضة للاختراق أو التصنت من خلال الميكروفونات الداخلية؟ إضافة إلى ذلك، لابد من مراجعة أنظمة التكييف الشبكية الذكية، وأنظمة الإنارة الشبكية الذكية، وحصر كافة أجهزة "إنترنت الأشياء" بداخل الجهة ودراسة حالتها الأمنية ومن ثم وضع سياسة مناسبة لتحصينها.

٢٥. الاتصالات الرجعية (Callback):

ليس من الحكمة التصّور بأنه من المستحيل تسلل برمجيات ضارة إلى أجهزة الموظفين. خصوصًا إن كانت تلك الأجهزة متنقلة ويتم حملها خارج نطاق الجهة أو الدولة باستمرار، لذلك من المفيد تطبيق أنظمة داخلية للأمن السيبراني لرصد عمليات "الاتصالات الرجعية" (Callbacks) التي تجريها البرمجيات الضارة المتسللة إليها محاولة منها للتواصل مع خوادم القيادة والتحكم (C&C[١٩]) لإخطار المخترقين بجاهزيتها لاستقبال الأوامر لشن الهجمات من الداخل وكثيرًا ما

١٧ NTP: Network Time Protocol

١٨ تمتلك الهيئة نظاماً لتوليد التوقيت الشبكي بأقوى معايير التوقيت الدولية على الإطلاق، على مستوى Stratum 0

١٩ C&C: Command and Control

تستنسخ تلك البرامج كل ما أدخله مالكها من خلال لوحة المفاتيح – شاملًا حساباته وكلمات السر– لبثّها لاحقًا إلى تلك الخوادم المركزية. وأحيانًا يصعب كشف هذه الاتصالات نظرًا لمحدودية بياناتها واستغلالها لبروتوكولات بريئة للاتصال الخارجي، علمًا بأن هناك منتجات تجارية فعالة ذات تخصص دقيق في كشف وإيقاف هذه الاختراقات تحديدًا.

٢٦. المصائد الشبكية:

هنالك حلول تقليدية شديدة الفاعلية ولكن لا تطبقها كثير من الجهات وعلى رأسها حلول خوادم التصيد وشبكات التصيد (Honeypot/Honeynet)، وهي عبارة عن خوادم وهمية لا تستخدم لأي غرض من أعمال الجهة الرسمية ولكنها تبدو جذابة أمام المخترقين، وفي عصر الخوادم الافتراضية فإن الموارد المبذولة لإنشاء مثل هذه الخوادم والشبكات محدودة جدًا، إلا أنها ذات فاعلية عالية فأي اتصال يتم من أو إلى هذه الخوادم مهما كانت صفته يعد جرس إنذار بوجود مخترقين داخل الشبكة، هناك العديد من المنتجات التجارية الجاهزة لبناء مثل هذه الحلول، بالإضافة إلى الحلول المجانية ومفتوحة المصدر والتي يمكن دراسة فاعليتها وجدواها للجهات.

٢٧. الأمن السحابي:

يشهد عالمنا اليوم توجهًا واضحًا نحو خدمات الحوسبة السحابية، المدفوعة الأجر أو المجانية. ومنها خدمات تخزين الملفات السحابية وخدمات البرامج المكتبية السحابية وخدمات الاجتماعات عن بعد السحابية والبريد الإلكتروني المجاني وغيرها من الخدمات المشابهة، تمثل كل تلك الخدمات تهديدًا أمنيًا على البنية المعلوماتية وبيانات أعمال الجهة، لذلك علينا الحرص على ضم هذه الفئة من الخدمات ضمن الاستراتيجية الأمنية لتحديد المناسبة منها والمرفوضة والضوابط الواجب فرضها في حق كل منها حسب سياسات الجهة وتصنيفات مواردها والضوابط والسياسات ذات العلاقة. كما من الضروري أن يكون هناك اتفاقية مستوى الخدمة (SLA) مع الجهات الخارجية لضمان مستوى أمان الخدمة، و لابد من الاطلاع على ضوابط الأمن السيبراني للحوسبة السحابية[٢٠] للتأكد من تحقيق مستوى الأمان المطلوب.

٢٨. سياسة الموظفين:

من الضروري وضع سياسة محكمة ومفصلة للتعامل مع كافة التغيرات في حالة الموظفين، مثل التعيين، الاستقالة، أو الانتقال إلى إدارة أخرى، أو الإعفاء من منصب، أو الإعارة وغيرها. لا بد أن تكون هذه السياسة تفصيلية بحيث تدرس كافة المجموعات البريدية المشتركة ذات العلاقة وكافة المجلدات المشتركة، وكافة الصلاحيات على أنظمة الأعمال، وكافة الحسابات الإلكترونية الخاصة الممنوحة وما شابهها من موارد مؤسسية وصلاحيات. ثم يتم التنسيق مع إدارة الموارد البشرية لدمج هذا الإجراء مع إجراء "تغيير الحالة الوظيفية" لدى تلك الإدارة، بحيث يتم تطبيقه فور تغيير حالتهم الوظيفية. وذلك لضمان عدم بقاء صلاحيات وحسابات ذات مخاطر أمنية على الجهة بعد تلك التعديلات الوظيفية. مثال

٢٠ ضوابط الأمن السيبراني للحوسبة السحابية https://www.nca.gov.sa/files/ccc-ar.pdf

ذلك: مجلد شبكي مشترك مخصص لأعمال إدارة "أ"، وتستمر صلاحيات الموظف عليه حتى بعد نقله إلى إدارة "ب" أو بعد إعفاءه من مهامه الإدارية، إلخ. مثال أخر: تكون لدى الموظف صلاحية على حسابات تواصل خارجية لأداء مهامه الرسمية، ولكن بعد استقالته يتم إغلاق حسابه الشخصي دون سحب صلاحياته على حساب التواصل الخارجي الخاص.

٢٩. مراجعة الحسابات ذات الصلاحيات العالية:

وضع إجراء دوري لحصر وتوثيق ومراجعة الحسابات ذات الصلاحيات الخاصة أو العالية من حين لآخر لضمان استمرار الحاجة إليها، واستمرار مناسبة نطاق صلاحياتها، وضمان اقتصارها على الموظفين المصرحين.

المصادر والمراجع الإضافية

نوصي باطّلاع عموم الموظفين ومدراء تقنية المعلومات والأمن السيبراني على الضوابط المنشورة من قبل الهيئة الوطنية للأمن السيبراني، والتي لها علاقة مباشرة بهذا الدليل:

١. الضوابط الأساسية للأمن السيبراني.
٢. ضوابط الأمن السيبراني للأنظمة الحساسة.
٣. ضوابط الأمن السيبراني للعمل عن بعد.

كما نوصي بالاطّلاع على المنشورات الصادرة من المركز الوطني الإرشادي للأمن السيبراني (السيرت السعودي) ذات العلاقة بالأمن السيبراني في بيئة العمل، ومنها:

١. دليل إرشادي بعنوان مسارك الآمن للعمل عن بعد
٢. إرشادات لموظفي الأمن السيبراني
٣. أفضل الممارسات للموظفين
٤. حماية بيانات المنشأة
٥. كيفية تمييز روابط التصيّد
٦. نصائح أمنية للحفاظ على أمان أجهزة المنشأة
٧. العامل البشري سببٌ للاختراق
٨. الموظف خط الدفاع الأول
٩. إرشادات لموظفي الأمن السيبراني
١٠. اجعل نفسك هدفاً صعباً للتصيّد!
١١. هل ضغطت على رابط تصيّدي؟
١٢. كيف تحافظ على سرّيتك وخصوصيتك في الاجتماعات عن بُعد؟ (كمشارك في الاجتماع)
١٣. كيف تدير اجتماعاتك عن بُعد بسريّة وخصوصية؟ (كمستضيف للاجتماع)
١٤. كيف تجعل منشأتك أكثر أماناً؟
١٥. كيف يحاول المهاجم أن يخدعك؟
١٦. كيف تحمي كلمة المرور الخاصة بك؟
١٧. عادات تحميك من عمليات التصيّد والهندسة الاجتماعية

كما نوصي بالاشتراك في القائمة البريدية الخاصة بالمركز للاطّلاع على أحدث المنشورات التوعوية، وزيارة الصفحات المخصصة للتوعية الأمنية على موقع المركز الإلكتروني.

الخـاتـمة

لقد سعينا من خلال هذا الدليل لتقديم الإرشاد إلى عدد من الممارسات المثلى التي نستهدف بها الموظفين على اختلاف مهامهم وأدوارهم لزيادة الحصانة الأمنية في الجهات ولرفع قدرتها على التصدي للتهديدات السيبرانية أو الاستجابة لها أو التعافي من بعدها. وما ذلك كله إلا ثمرة واحدة من بستان الهيئة الوطنية الأمن السيبراني الوارف والمتنامي يومًا بعد يوم، والذي يسعى إلى فضاء سيبراني آمن وموثوق يمكن النمو والازدهار. لذا نهيب بالموظفين أن يتابعوا كل جديد في هذا الشأن من خلال متابعة موقع الهيئة الوطنية للأمن السيبراني[٢١] والمركز الوطني الإرشادي للأمن السيبراني[٢٢] والاستفادة من كافة الموارد المتجددة المتاحة من خلالهما والمسخّرة لهم لنكون يدًا واحدة في حماية بيانات وموارد وطننا الغالي.

٢١ الهيئة الوطنية للأمن السيبراني https://nca.gov.sa

٢٢ المركز الوطني الارشادي للأمن السيبراني (السيرت السعودي) https://cert.gov.sa/ar

المركز الوطني الإرشادي
للأمن السيبراني
SAUDI CERT

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

https://cert.gov.sa/ar/

https://nca.gov.sa/

@SAUDICERT

@NCA_KSA