علي مصطفى*: نحو التحول الرقمي في العراق

ما تعريف التحول الرقمي؟

التحول الرقمي(Digital Transformation) :عملية تحويل نموذج أعمال المؤسسات الحكومية أو شركات القطاع الخاص إلى نموذج يعتمد على التقنيات الرقمية في تقديم الخدمات وتصنيع المنتجات وتسيير الموارد البشرية. ترصد الشركات الكثير من الاستثمارات والموارد لتحقيق أهدافها المتعلقة بالتحول الرقمي والتكنولوجي، لكنها لازالت تواجه صعوبات وتحديات كبيرة في إنجاح هذه العملية رغم قناعة أغلب الشركات بأن التحول الرقمي مسألة حيوية وبالغة الأهمية، لذلك نجد العديد من الشركات غير واثقة تماماً في قدرتها على النجاح في هذا التحول، ويظن معظم المسؤولين أن شركاتهم أو مؤسساتهم لا تتمتع بالمهارات والقدرات اللازمة لتحقيق طموحها الرقمي.(مؤسسة هارفرد للاعمال)

يعتمد التحول الرقمي على صياغة استراتيجية رقمية انطلاقاً من تشخيص الوضع الراهن وتحديد الفجوة بين القدرات الرقمية الحالية وما يجب أن تكون عليه في المستقبل، ثم العمل على تنفيذ الاستراتيجية من خلال تخصيص الموارد اللازمة سواء كانت مالية أو بشرية أو تجهيزات وآلات، ومراقبة تنفيذها والتقييم المستمر لنتائجها.

.ما معنى الأمن السيبراني؟

الأمن السيبراني :(Cybersecurity) يُطلق عليه أيضاً "أمن المعلومات" و"أمن الحاسوب"، وهو فرع من فروع التكنولوجيا يُعنى بحماية الأنظمة والممتلكات والشبكات والبرامج من الهجمات الرقمية، التي تهدف عادة للوصول إلى المعلومات الحساسة أو تغييرها أو إتلافها أو ابتزاز المستخدمين للحصول على الأموال أو تعطيل العمليات التجارية.

يعرّفه "إدوارد أموروسو (Edward Amoroso) "صاحب كتاب "الأمن السيبراني" الذي صدر عام 2007 بأنه "مجموع الوسائل التي من شأنها الحدّ من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو

الشبكات"، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات الرقمية ووقفها، وتوفير الاتصالات المشفرة.

مصطلحات مرتبطة بالأمن السيبراني

يتبّع الأمن السيبراني نهجاً محدّداً يتكون عادة من عدّة طبقات للحماية تُثبَت في أجهزة الكمبيوتر أو الشبكات أو البرامج أو البيانات التي ينوي المستخدم حمايتها. توجد العديد من المصطلحات المرتبطة بالأمن السيبراني نذكر منها:

- الفضاء السيبراني :(Cyberspace) عبارة عن بيئة تفاعلية رقمية تشمل عناصر مادية وغير مادية، مكوّنة من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين. ويُطلق عليه "الذراع الرابعة للجيوش الحديثة"؛

- الردع السيبراني :(Cyber Deterrence) يعرّف على أنه منع الأعمال الضارة ضد الأصول الوطنية في الفضاء الرقمي والأصول التي تدعم العمليات الفضائية؛

- الهجمات السيبرانية :(Cyber Attacks) أيّ فعل يقوّض من قدرات ووظائف شبكة الكمبيوتر لغرض شخصي أو سياسي، من خلال استغلال نقطة ضعف معينة تُمكّن المهاجم من التلاعب بالنظام؛

- الجريمة السيبرانية :(Cybercrime) مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية عبر شبكة الإنترنت، وتتطلب تحكماً خاصاً بتقنيات الكمبيوتر ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها.

أهمية الأمن السيبراني

تنبع أهمية الأمن السيبراني من ثلاثة محاور رئيسية هي:

- السرية :(Confidentiality) أي التحكم في الولوج إلى البيانات وإتاحتها لم يُسمح لهم فقط؛

- السلامة :(Integrity) الحفاظ على سلامة البيانات والمعلومات وحمايتها من الهجمات التخريبية أو السرقة؛

- الجاهزية :(Availability) جاهزية جميع الأنظمة والخدمات والمعلومات وإتاحتها حسب طلب الشركة أو عملائها

فوائد الأمن السيبراني

يمكن تلخيص أهم فوائد الأمن السيبراني فيما يلي:

- حماية الشبكات والبيانات من الدخول غير المصرح به؛
- تحسين مستوى حماية المعلومات وضمان استمرارية الأعمال؛
- تعزيز ثقة المسهامين وأصحاب المصلحة في الشركة؛
- استرداد البيانات المُسرية في وقت أسرع في حالة حدوث خرق للنظام الأمني السيبراني.

اكتشف الباحث الأمني تروي هنت أحد أكبر كنوز البيانات الشخصية المسرية عبر الإنترنت على مر التاريخ، وهو يضم قرابة 773 مليون من حسابات البريد الإلكتروني وكلمات المرور المخترقة. فماذا عن تطوير الأمن السيبراني بشكل مستمر؟

لقد أكّد اكتشاف هنت أمراً كان ظاهراً للعيان منذ فترة من الوقت، وهو أنه لا يستطيع أحد ضمان أمن المعلومات بشكل كامل بمجرد إدخالها إلى العالم الرقمي.

إذاً، كيف نحل مشاكلنا الخاصة بالأمن السيبراني؟ يمكن ذلك بالاعتماد على كلمتين اثنتين تتعلقان بمعنى ال (Cybersecurity)أو "الأمن السيبراني" وهما: التريث قليلاً. ببسيط العبارة، حان الوقت لامتلاك سيطرة أكثر فعالية على المحتوى الذي ندخله للعالم الرقمي، ما يعني إبطاء عملية الاعتماد على تكنولوجيا الربط الشبكي من خلال إقرار قوانين ومعايير جديدة تهدف إلى رفع مستوى جودة وموثوقية أي جهاز يمتلك عنوان بروتوكول الإنترنت .(IP) وهذا يعني الحرص على الحفاظ على إمكاناتنا من التقنيات التناظرية، حتى في زمن اعتماد التقنيات الرقمية.

العجز في حماية الأنظمة الرقمية

إن الأدلة التي تثبت عجزنا عن تأمين الأنظمة الرقمية بشكل كامل كثيرة ويمكن ملاحظتها من خلال عدد الاختراقات التي تعرضت لها عديد من المؤسسات الحكومية بصورة مستمره خلال السنوات السابقة مع التركيز على وجود اي جهة حكومية تقوم باصدارارقام وتقارير بخصوص هذه الهجمات السيبرانية. في نوفمبر/تشرين الثاني من العام 2017، على سبيل المثال، أدت إحدى عمليات الاختراق إلى تسريب بيانات 52 مليون شخص في جوجل. وقبل ذلك بشهرين، تم تسريب 50 مليون من حسابات مستخدمي فيسبوك. تزامنت هاتين الحادثتين مع صدور تقرير لمكتب محاسبة الحكومة الأميركية في أكتوبر/تشرين الأول من ذات العام، تم التأكيد فيه على وجود خلل يمس الأمن السيبراني في جميع منظومات الأسلحة العسكرية الأميركية التي تم تطويرها. وإذا لم تستطع مؤسسات متقدمة مثل جوجل وفيسبوك والجيش الأميركي الحفاظ على أمن أنظمتها، فلن تستطيع الحكومة قياس مدى تامين البنية التحتية للتحولات الرقمية وفقا للمعطيات الحالية.

في ظل الوضع الراهن، لا مجال للتأكد من سلامة وأمن أي شيء بمجرد تحويله إلى شيفرة على نظام الكمبيوتر، من خلال الكاميرات أو أجهزة التسجيل أو لوحات المفاتيح أو المستشعرات، حيث يمكن لكيانات لا تمتلك صلاحية الوصول إلى المعلومات أن تقوم بعرضها أو تخريبها أو استخدامها بطرق تنتهك خصوصية الأفراد الذين ينشرون هذه المعلومات أو تزعزع ثقتهم.

يطلق على الوضع الحالي المتدني الذي يعاني منه أمننا السيبراني الجماعي اسم "فلات لايت (Flat light)"، وهو مصطلح مقتبس من عالم الملاحة الجوية. ويشير مصطلح فلات لايت في أوساط الطيّارين إلى مستوى متدنّ جداً من التأثيرات بحيث تبدو جميع الاتجاهات متشابهة، وهو ظرف ينطبق الآن على المؤسسات والمشرعين والمستهلكين على حد سواء ضمن العالم الرقمي. فجميعنا لا نعرف على ماذا نركز، وما الإجراء الدقيق الذي ينبغي الدعوة إليه، أو كيف نحمي المعلومات التي نقوم بنشرها، سواء بصفتنا كأفراد أم شركات.

السيطرة على الإنترنت

لم تُعتمد أي تكنولوجيا في التاريخ الإنساني بنفس السرعة التي أُعتمد فيها الإنترنت، حيث استغرق الهاتف 100 عام بعد أن تم اختراعه عام 1876 قبل أن يتم اعتماده بشكل شبه عام في الولايات المتحدة. ثم تبع ذلك اعتماد الكهرباء والسيارات خلال فترات زمنية مماثلة. ولكن الأمر تطلب عشرة أعوام فقط ليمتلك

أربعة من كل خمسة أميركيين تقريباً هاتفاً ذكياً. تخمن شركة سيسكو بان عدد الأجهزة المربوطة شبكياً 27.1 مليار جهاز في 2021، بمعدل نمو سنوي يبلغ 25.%

والطريقة الوحيدة لاستعادة السيطرة على هذه البيئة هي الإدارة الفعالة للمحتوى الذي ندخله إلى العالم الرقمي، أي التقليل الحذر من سرعة اعتماد تكنولوجيا الربط الشبكي. ففي بيئة اقتصادية تكافؤ السرعة في التسويق أكثر من أي شيء آخر، يجري التقليل من أهمية أمن برمجياتنا على نحو مستمر، إن لم يتم تجاهله ببساطة، بينما تستمر معدلات اعتماد التكنولوجيات الحديثة في الارتفاع. ويعتبر إبطاء معدل الاعتماد من خلال إقرار قوانين ومعايير جديدة والتأكد من الاحتفاظ ببدائل تناظرية لبعض التكنولوجيات، الطريقة الأفضل للاحتفاظ بمستوى من الأمن في بيئتنا السيبرانية التى تزداد تعقيداً. بهذا فقط يمكننا على الأقل أن نفهم طبيعة الأمور ونمتلك بعض السيطرة على اعتمادنا المتنامي على التقنيات الرقمية.

يقع عبء استعادة السيطرة على بيئة الأمن السيبراني على عاتق الحكومات والشركات والأفراد على حد سواء.

في بادئ الأمر، يجب أن تشترط القوانين على كل نظام يمتلك إمكانية الربط الشبكي أن يكون له عمر محدود أو أن يقبل بإدخال التحديثات، حيث يزداد في زمننا هذا عدد الأجهزة التي يتعذر تحديثها بعد اكتشاف خلل فيها. على سبيل المثال، جرى الإبلاغ عن عدم إمكانية تحديث 25% من الأجهزة التي استخدمت نظام تشغيل أندرويد التابع لشركة جوجل في العام 2016.

يمكن لجهات اجرامية السيطرة على الأجهزة التي تعاني من مشاكل، أو استخدامها لأهداف خبيثة، كما كان الحال مع برمجية البوت نت "ميراي" في عام 2016 عندما تسببت بقطع خدمة الإنترنت عن الكثيرين. إن بقاء هذه المشاكل مع عدم توفر الإمكانية لعلاجها هو أمر لا يطاق على المستوى الاجتماعي، ويجب أن يصبح غير قانوني أيضاً.

وحتى إذا كانت القوانين بطيئة في وضع هذا التشريع حيز التنفيذ، سيكون من الحكمة لو الحكومة باتخاذ قراراتهم بناء على الأمر التالي: إذا كان الجهاز الذي يريدونه لا يمكن تحديثه ولا تنتهي صلاحيته، يجب ألا يوضع في مؤسستهم (أو في منزلهم).

ثانياً، يجب أن تكون المسؤولية عن المشاكل والأخطاء واضحة، ويجب مساءلة صانعي البرمجيات الذين تتسبب شيفراتهم البرمجية بالخلل، كما هو الحال مع منتجي المنتجات الاستهلاكية أو الصناعية الأخرى. وفي يومنا هذا، ترتبط معظم العقوبات المترتبة على ضعف الأمن السيبراني بعدم الإبلاغ عن اكتشاف

ثغرات أو بوجود مغالطات في شروط الخدمة الخاصة بالمنتج. وكلا الأمرين لا يساهمان في وضع شيفرة أفضل.

مثلاً، تقوم التشريعات الخاصة بالإبلاغ بإلحاق العقوبة فقط بالمؤسسات التي لا تفصح عن وجود ثغرات بمجرد حدوثها. ويتجاهل الاعتماد على شروط الخدمة بين شركة البرمجيات والمستخدم النهائي، حقيقة أن المستخدمين لا يملكون حيلة عند ترخيص برمجية ما، إذ ليس بمقدورهم سوى القبول بالشروط المعروضة أو التخلي تماماً عن فكرة استخدام البرمجية. وهذا هو السبب الذي يكمن وراء ندرة مساءلة أي مؤسسة بعد إثبات عدم أمن برمجيتها. فمن شأن توضيح ماهية متطلبات الحد الأدنى للأمن السيبراني، كما فعلت كاليفورنيا بقانون جديد أصدرته في العام 2016، وتوحيد الالتزام عند مخالفة هذه المقاييس المعيارية، أن يساعد في إزالة البرمجيات الرديئة من السوق، وهو ما سيجعلنا أكثر أمناً في الوقت نفسه.

وختاماً، يجب أن تضمن الحكومات والمؤسسات الحفاظ على الإمكانات التقليدية المقابلة للرقمية حتى عند اعتمادنا على تكنولوجيات حديثة. ففي معظم الحالات، تتشارك آلية عمل البرمجيات في امكانية حدوث فشل مفاجئ، ما يعني أنه عند فشل خدمة ما، تفشل أخرى. والأمر ليس كذلك مع الخدمات التقليدية الموجودة.

وكذلك يجب أن نكثف جهودنا لضمان إيجاد طرق بديلة لتنفيذ الأنشطة المهمة بدلاً من التركيز على الجانب الأمني فقط، في حال تسبب عيب أمني بوقف تنفيذها. وعلى نحو مماثل، يجب أن تركز فرق أمن المعلومات العاملة في المؤسسات ليس فقط على حماية المؤسسات من هجوم اليوم، إنما على التأكد من وجود وسائل موازية تقليدية بديلة لتنفيذ العمل في حالة وقوع كارثة سيبرانية.

لقد أتى انتشار الأجهزة المربوطة شبكياً على إطار واسع بفوائد عديدة. ويجب ألا نتجاهل هذا التقدم، ولا نستطيع ذلك بطبيعة الحال.

لكننا عندما نعتمد التكنولوجيات الحديثة بسرعة بالغة، بامتلاكنا لأجهزة مرتبطة بالإنترنت، فإننا جميعاً نستطيع التغاضي عن المخاطرات التي قمنا بها، والمضي قدماً في سبيل تطوير الأمن السيبراني. لقد فضّلنا في السنوات العشر الأخيرة الاتصال والراحة على خيار الأمن والخصوصية. يجب ألا تكون هذه المقايضة دائمة. ما زال لدينا القدرة على اتخاذ القرار.

كيف تحسّن الأمن الرقمي لإي مؤسسة حكومية

يرى الكثير من المدراء الذين يهتمون بموضوع تحسين الأمن السيبراني أنّ الموظفين هم الحلقة الأضعف في مجال الأمن الرقمي للشركات، إلا أنني أراهم خط الدفاع الأفضل، وذلك في حال قدّمت لهم سياسات سهلة التنفيذ وأبعد ما تكون عن التعقيد. كما يجب أن يكون التدريب الأمني للموظفين وأفضل الممارسات مصممة بطريقة سهلة، يمكن تطبيقها وتنفيذها. ويجب على طريقة الاستعمال أن تكون بسيطة بدورها لتحقيق أقصى فعالية ممكنة من مميزات الأمن السيبراني.

لا يحتاج المخترقون الرقميون إلى مهارات متقدمة في القرصنة لاقتحام شبكات الشركات، بل يحتاجون فقط لتوفير حافز مغر للموظفين لفتح المرفقات والنقر على الروابط. وتُعتبر هجمات الاحتيال في الإنترنت السبب في 90% من جميع خروقات البيانات والحوادث الأمنية، وفقاً لأحدث تقرير نشرته فيرايزون حول خروق البيانات. ومن الواضح أنّ الموظفين هم الفئة الأساسية المستهدفة بهجمات المخترقين، وبالتالي يكون من المنطقي القول بأنهم خط الدفاع الأول. وجد تقرير فيرايزون أنّ الإخطار الذي يقدمه الموظفون حول الاختراقات الأمنية هو الطريقة الأكثر شيوعاً للمؤسسات لكشف الهجمات الرقمية. ولذلك، يُعتبر تزويد الموظفين بالمعلومات اللازمة لتحديد هكذا هجمات أمراً مهماً من برنامج الأمن العام للشركة، إلا أنه في الوقت نفسه، لا تقوم غالبية الشركات بهذا الأمر.

الطرق الأمنية المختصرة لتحسين الأمن السيبراني

من أبرز أسباب إخفاق قواعد الأمن في تنفيذ ما هو مأمول منها تعقيدها المبالغ فيه، والذي يدفع الناس في كثير من الأحيان إلى سلوك طرق مختصرة تلغي فائدة تلك القواعد. على سبيل المثال، تُعتبر سياسات كلمة المرور معقدة جداً وغير مريحة لدرجة قيام معظم الموظفين بتجاهلها. ويُطلب من الموظفين تغيير كلمات السر كل فترة، ولكن وجد الباحثون أنه عندما يطلب من الناس وضع كلمات مرور جديدة كل ثلاثة أشهر، يميلون للقيام بأمور مثل تغيير الحرف الأول فيها أو إضافة عدد في نهايتها لتوفير الوقت. وهذا يجعل كلمات السر أسهل كسراً على نحو متزايد. سيُستنزف الإبداع الذي لديك عندما يتوجب عليك القيام بنفس الأمر مراراً وتكراراً، وتجبر معظم الشركات موظفيها على القيام بذلك لأهداف أمنية.

وهناك مثال آخر على السياسات الأمنية التي تحرق نفسها بنفسها، وتتمثل بطلب كلمات مرور طويلة ومعقدة، حيث نُطالب دائماً بوضع كلمات مرور معقدة تتألف من مجموعة من الأرقام والحروف الكبيرة والصغيرة (في اللغة الإنجليزية) والرموز. وعندما يُطلب منا هذا، يتجاهل كثير من الموظفين ببساطة هذه

السياسة أو ينشؤون كلمة مرور طويلة لا يمكنهم تذكرها بسهولة ما يجعلهم يكتبونها على ورقة ويضعونها على الشاشة. من جديد، توفر هكذا ممارسات إحساساً زائفاً بالأمان للمؤسسة.

يتم حالياً تحدي هذه المبادئ التوجيهية التاريخية المتصلة بكلمة المرور نظراً لقلة نجاعتها المبرهنة لمعظم المؤسسات. وقد غيّر المعهد الوطني الأميركي للمعايير والتكنولوجيا مؤخراً مبادئه التوجيهية لتتماشى مع الواقع الجديد، حيث بات يوصي الآن بالتخلص من القواعد التي تعقّد ممارسات كلمة المرور للمستخدمين النهائيين، مثل طلب إعادة تعيين كلمة المرور بشكل متكرر، والسماح باستخدام برامج إدارة كلمات المرور، ولصق كلمات المرور في حقولها المخصصة. ويوصي المعهد أيضاً بالمصادقة متعددة العوامل، مثل إرسال رموز إلى الهواتف الذكية والأجهزة التي يتم وصلها بالحاسب للمصادقة.

التدريب والتعلم

لا يجب الاغفال من المسؤولين الحكوميين عن هذا الملف تخصيص موازنات من ضمن الموازنة الخاصة بتطوير تقنية المعلومات والتحول الرقمي لتطوير الكوادر المحلية في مجال الامن المعلوماتي على ان يكون التدريب رصيناً ويتجاوز اخطاء الماضي والتي ارهقت الموزانات ب حملات تدريب عشوائية بدون اي عائد على الاستثمار يذكر.

ومن باب التجارب التي مرت بها حكومات ومؤسسات عالمية سابقا فان من أسباب فشل ممارسات الأمن الرقمي الداخلي، خضوع الموظفين بشكل مبالغ فيه لتوجيهات ومعلومات حول الأمور التي عليهم القيام بها وتلك التي عليهم تجنبها، وتُعد الكثير منها لا يمكنهم تقبله، حيث يتم مثلاً نقلهم إلى دورات تدريبية أمنية إلزامية لمدة نصف يوم يقضونها في الغالب محدقين في هواتفهم أو يتظاهرون بالانتباه. إذ تحتوي تلك الدورات على الكثير من المعلومات التي يتوقع أن يستوعبها شخص ما ويتذكرها، وتتمثل فائدتها لقسم تقنية المعلومات في قيامهم بتقديم تقاريرهم أمام رؤسائهم تفيد بأنهم دربوا الموظفين على أفضل الممارسات الأمنية. إنه إجراء امتثال غير فعال ويضيع وقت الموظف.

أنصح المشرفين على تكنولوجيا المعلومات بدلاً من ذلك بفعل ما يفعله المخترقون لتحقيق فعالية أكبر. بمعنى آخر، تخصيص عملهم قدر الإمكان. على سبيل المثال، تُعتبر أخطر رسائل البريد الإلكتروني الاختراقية تلك التي تستهدف الموظفين ذوي المرتبة الإدارية العالية، حيث تصمم بشكل يخدع الشخص المستهدف بالضبط. وتكون أمور على غرار طلبات الحصول على معلومات ضريبية وطلبات تحويل إلكتروني تبدو وكأنها مرسلة من الرئيس التنفيذي أو المدير المالي إلى شخص في الإدارة المالية باستخدام اللغة المناسبة. ويقع الناس في العادة ضحية تلك الفخاخ نظراً لقيام المهاجمين بتقديم التفاصيل الكافية

لذلك. إذاً، يجب على أقسام تكنولوجيا المعلومات اتباع نفس دليل التشغيل واستخدام التدريب والتوجيه المخصص بدلاً من التدريبات العامة والشاملة لجميع الموظفين. وأشير إلى هذه التقنية بأنها "لحظات يمكن التعلم منها" لأنها توفر معلومات محددة لأفراد محددين بطريقة ووقت هم أكثر احتمالاً فيها على تقبلها والتعلم منها.

تكون معظم اختبارات الأمن الداخلي واسعة جداً وغير مركزة. على سبيل المثال، تميل أقسام تكنولوجيا المعلومات إلى إجراء اختبارات التصيد عن طريق إرسال نفس البريد الإلكتروني المزيف لجميع الموظفين. وشخصياً، لا أعتقد أنّ هذا الأمر مناسب لجميع المؤسسات، إذ يتطلب "اختبار المستخدمين" الكثير من التأطير والمشاركة لضمان ألا يجعل الموظفين يشعرون بأنه غير موثوق بهم، وبالتالي تقليل علاقة الثقة لديهم مع فريقهم الأمني.

وينطبق نفس المبدأ على خدمات المشاركة والتعاون من الجهات الخارجية، مثل خدمتي Dropbox,Slack. عندما نحاول منع هذه الأدوات الشائعة، سنجد في كثير من الأحيان قيام المستخدم باكتشاف وسائل أخرى مختلفة يفشل قسم تكنولوجيا المعلومات في منعها. ولكن إذا قام قسم تكنولوجيا المعلومات بدلاً من ذلك بتحديد متى تُستخدم الخدمة، ووفر توجيهات واضحة حول كيفية استخدامها بشكل آمن، أو قدم اشتراكاً للشركات مع التعليم الأمني، سيُحدث ذلك أثراً أكبر بكثير.

يمكن القول أنّ أهم ما يمكن للادارات العليا تحسين العلاقة بين قسم تكنولوجيا المعلومات والموظفين، والذين هم الأقرب إلى البيانات والأجهزة، وبالتالي في أفضل وضع لاكتشاف والإبلاغ عن الحالات الأمنية والحوادث الشاذة، حيث سيزيد التعرف على الموظفين وأدوارهم، وكيفية استخدامهم للتكنولوجيا من فرص قيامهم بالإبلاغ عن القضايا الأمنية وإبداء رغبة أكبر في المساعدة على حلها. كما يمكن أن يساعدوا في تزويد قسم توفير تكنولوجيا المعلومات بالمعلومات التي يحتاجونها لتصميم التعليم الأمني واختبار الجهود بشكل أفضل. وسيؤدي تعاون مثل هذا داخل المؤسسة إلى تغيير عادات الناس بشكل كبير وإحداث فرق في الحفاظ على المؤسسات آمنة بسبب تحسين الأمن السيبراني فيها بشكل متواصل,

ثقافة الانفتاح

ومن الجوانب التي غالباً ما يتم تجاهلها في المؤسسات الحكومية هو اشراك المنظمات المتخصصة وشركات القطاع الخاص في نقاشات تطوير السياسات والاجراءات الخاصة بالتحول الرقمي والامن المعلوماتي , يحتاج القطاع الحكومي الى الاستفادة من تجارب الخبراء والمختصين خارج القطاع الحكومي والذين لديهم خبرات مسبقة في هذا المجال. ومن تجربتي السابقة فان هناك العديد من المسؤولين في

القطاع الحكومي هم من اشد المعارضين لاي عملية تحول رقمي وان كان بسيطا بل وحتى لاي عملية تلغي العمليات الورقية والروتين القاتل بحجُة التعليمات الحكومية والتي قد تعود الى ستينات القرن الماضي ولهذا فان على جهة انفاذ تعليمات التحول الرقمي الانتباه الى هكذا عقبة قد تواجه فرق التحول الرقمي داخل المؤسسات.

ان من واجب اعلى السلطات في الحكومة ايضا اقناع شركات التكنولوجيا العالمية بافتتاح فروع لها داخل العراق فبدون هذه الشركات فسيكون من الصعب جدا تغيير الثقافة المتندية السائدة داخل المؤسسات الحكومية وسيكون من الصعب جدا تنفيذ مشاريع تقنية كبرى بالاعتماد على شركات وسيطة من دول اخرى وقد نواجه مشاكل فنية وقانونية وادارية ستكون عقبة كبيرة في طريق التحول الرقمى للحكومة العراقية.

(*)استشاري امن معلومات/رئيس جمعية تدقيق ومراقبة نظم المعلومات