أمن المعلومات في الجامعات: حين لا تكفي الجدران النارية

فيليب وود



الملخص:

يناقش المقال تعرض مؤسسات التعليم العالي للمخاطر السيبرانية بوصفها منتجة للمعرفة وحافظة لأبحاث وبيانات ذات قيمة علمية واقتصادية واستراتيجية. ويقارن ثقافة الانفتاح والمشاركة في الجامعات بمتطلبات حماية المعلومات لدى شركائها، موضحًا صعوبة الموازنة بين تدفق المعرفة وتقييد الوصول. ويتناول التهديدات الداخلية والخارجية، والعامل البشري، وما تتيحه الأجهزة المحمولة والعمل عن بعد والسفر من مسارات لتسرب البيانات. ويرى أن السياسات والجدران النارية وحدها لا تكفي، ما لم يصاحبها فهم مشترك للمخاطر وتدريب وتنفيذ فعلي ومسؤوليات واضحة. ويؤكد أن حماية الأصول المعرفية تتطلب إدارة سلوك الأفراد وثقافة المؤسسة، مع المحافظة على إمكانات البحث والتعليم والتعاون وإدراك قدرة الخصوم على استغلال الثغرات التقنية والاجتماعية المتغيرة.

الكلمات المفتاحية: الأمن السيبراني، التعليم العالي، حماية المعلومات، العامل البشري، إدارة المخاطر

المعرفة أصل يحتاج إلى حماية:

يفتتح الأصل بفكرتين: يرى كريستيان نستيل بوفي أن الخوف يتناسب مع الجهل، ويسخر بول ر. إيرليخ من أن الخطأ بشري لكن الحاسوب قادر على تضخيمه. وتدرك الجامعات أن المعرفة قوة؛ فعليها تنمية القدرة الأكاديمية والمهنية والتساؤل والتقييم والتحليل، وزادت حديثًا مسؤوليتها عن تأهيل الخريج لسوق العمل. وهي تساعد على نضجه الفكري والشخصي في بيئة للتميز.

ولكي تزدهر بيئة التعلم، ينبغي تطوير المعرفة وتخزينها ونقلها. والبحث والملكية الفكرية المرتبطة به أساس الممارسة الأكاديمية المعتبرة، والأفكار والنظريات والاكتشافات قلب النشاط. لذلك تتدفق المعلومات باستمرار عبر تفكيك الحقائق والأفكار وتطويرها ومناقشتها ونشرها، وتُفرز البيانات وتُحلل وتُقيم لأسباب كثيرة. ويخدم بحث الدراسات العليا الفرد، وقد يضيف نتاجه إلى المعرفة الأوسع في تخصصه.

تجري معظم الجامعات بحثًا مع الصناعة والأعمال والمنظمات الحكومية وغير الحكومية ولحسابها. وتدرك الجهات الخارجية قوتها في التغيير والتقدم أو الميزة التنافسية، ولذلك يمولها أطراف متنوعون، ولا غرابة ولا ضرر في العمل مع مستثمرين متنافسين بالتزامن.

ولأن المؤسسة ذات قيمة ونتائجها قد تزيد الربحية أو التفوق أو تخدم المصلحة الوطنية، فأصولها المعرفية هائلة. وهي بؤر إبداع وابتكار ولديها كثير لتحميه. وتحدد (Universities UK) [1] خصوصًا بيانات تخضع للموافقة الأخلاقية فتكون حساسة، أو لالتزامات قانونية وتعاقدية فتترتب آثار اقتصادية على فقدها أو الوصول إليها، أو تحمل بذاتها قيمة اقتصادية أو سياسية.

وتجعل المعرفة وجمهورها النشط من الطلاب والباحثين والأكاديميين الجامعات أهدافًا جذابة. والتجسس وجمع معلومات المنافسين ليسا جديدين، لكن المؤسسات والأفراد يواجهون الآن مشهدًا غير مسبوق متغير الشكل، تقترن فيه حرية إنتاج المعلومات ونقلها بتهديد سيبراني.

تهديد واسع وعامل بشري:

تتزايد الأدلة على أن المشكلات السيبرانية أهم قضايا أمن المؤسسات، ولا سبب لتوقع تغير قريب. وتصنف استراتيجية الأمن الوطني البريطانية [2] الهجمات في المستوى الأول للتهديدات إلى جانب الإرهاب الدولي. وبمقياس إدارة المخاطر، يكون الإرهاب عادة قليل الاحتمال عالي الأثر، بينما تكون الهجمات السيبرانية عالية الاحتمال وقادرة على أثر شديد جدًا.

وخصصت الحكومة موارد كبيرة لاستراتيجية الأمن السيبراني حتى 2016 [3] بأربعة أهداف: جعل بريطانيا من أكثر أماكن الأعمال السيبرانية أمنًا؛ وزيادة الصمود وحماية المصالح؛ والمساعدة في فضاء مفتوح حيوي مستقر يدعم المجتمعات المفتوحة؛ وتنمية المعرفة والمهارات والقدرات الأمنية.

تعكس الأهداف قلق الحكومات والمؤسسات التي تدعمها وتحميها، والحاجة إلى الموازنة بين استخدام المعلومات وإدارتها الآمنة الفعالة. لكن المجال يظل سيئ الفهم رغم الموارد والالتزام؛ فالتهديد متغير وحاضر دائمًا وفاعلوه بلا وجوه واضحة، ودوافعهم الربح والتنافس أو استغلال معلومات الهدف لأغراض أوسع.

والحماية جزء من استراتيجية إدارة المعلومات. لكن المؤسسات لا تفهم التهديدات دائمًا، والأهم أنها لا تدرك أن الجهات والأفراد المستهدفين قد يضاعفون بأنفسهم أثر الهجوم. فتستغل الهجمات الفضول والطمع والنرجسية والرغبة في المعرفة عبر التقنية؛ وليس مصادفة أن تُستخدم رسائل بنكية مزيفة وإعلانات ومكافآت مغرية لاستدراج غير المنتبه والفضولي. ويشير المؤلف بسخرية إلى نصيب الجامعات من النوعين وحاجتها الجوهرية إلى الفضول.

اختلاف ثقافة الجامعات:

لا تختلف غالبية الجامعات هيكليًا وتشغيليًا كثيرًا عن مؤسسة تجمع بيانات ومعرفة مرتبطة بشركاء. وتكشف المقارنة مع شركات تعتمد أسرارها وخططها ومعرفتها السوقية للبقاء تفاوتات محتملة. فالشركات البارزة في المال والمصارف والطاقة والأدوية تستثمر وقتًا وجهدًا ومالًا في إدارة المعلومات وحمايتها، وتقتضي حوكمة البحث والتطوير تلبية متطلبات الأمن وجعل فهم مواطن الضعف جزءًا من تكوين المؤسسة. ورغم تفاوت التطبيق، يُتوقع الوعي والموارد لدى الجادين في التفوق والاستدامة المالية.

أما تكوين الجامعة فمختلف؛ فهي تحتاج مفكرين ومتحدثين وناشرين للأفكار المنفتحة. وينشر الأكاديمي ليختبر المعرفة ويضيف إليها ويظهر التميز ويتيح النجاحات والإخفاقات على نطاق واسع. لكن ذلك يتقاطع مع ما يعده (Edward Wilding) [4] قضية دائمة: أن المعرفة والمعلومات من أثمن أصول المؤسسة الحيوية للعمل التجاري، ومع ذلك كثيرًا ما تُحمى بصورة ضعيفة.

وقد تكون العواقب كارثية وأشد من السرقة المالية المباشرة، بخسارة السمعة والحصة السوقية وإنفاق جهد مفرط لاستعادة التشغيل. كما تخفي الطبيعة غير المادية للمعلومات طرائق تسربها، ويصعب تصنيف الفاعلين لتنوع الأصول والدوافع.

من يهدد المعلومات:

تأتي المخاطر من الداخل والخارج. فقد يسرق موظف للربح أو الإضرار أو الاستخدام الشخصي، وقد يحتفظ بالمعلومات أو يكشفها بلا قصد. وقد يجمع الخارج معلومات للتنافس أو الإيذاء، فضلًا عن التجسس الاقتصادي أو الصناعي المدعوم حكوميًا والإعلام وجماعات الاحتجاج والنشاط. وقد وصف المؤلف في تدوينة في السنة السابقة [5] خصومًا يملكون الدافع والوسيلة وينتظرون الفرصة.

ولا يقتصر التهديد على مستوى مؤسسي واحد، وتضاعف أنشطة الجامعة مواطن الضعف. ولارتباطها بجهات قد تتوقف أعمالها عند فقد معلوماتها، تصبح الجامعة جزءًا من مشكلة الخطر السيبراني لدى شركائها أيضًا.

والمعضلة أن تقييد الوصول قد يخنق تدفق المعرفة والأفكار، بينما تحتاج المعلومات إلى الاستخدام والمعالجة كي تنفع. لذلك يلزم تقدير ما يُستخدم ومتى وأثر سوء الاستخدام والفقد. وقد تقتضي الموازنة بين «الحاجة إلى المعرفة» و«الحاجة إلى التدفق» تنازلات تحفظ طرق العمل وحريته. وهي ضرورية وربما طبيعية في التعليم، لكنها تفتح فرصًا للخصوم؛ فاحتياجات الانفتاح والمشاركة نفسها تبقي مسارات التسرب مفتوحة.

السياسات ليست تنفيذًا:

تقترح أدلة الأمن عادة إجراءات وحوكمة واستثمارًا تقنيًا وهياكل رصد وإبلاغ. وهي منطقية لحماية الأمن والاستمرارية والصمود. والركن الآخر ثقافة فهم المعلومات وحمايتها. ويؤكد دليل (Universities UK) [6] اعتماد تقييم المخاطر والممارسات الآمنة على فهم مشترك للتهديدات، وعلى سياسات استخدام للشبكات يفهمها جميع المستخدمين وينفذونها.

المشكلة ليست في النصيحة بل في «الفهم والتنفيذ»، أصعب عناصر المتطلب. فالمؤسسات تجيد إنتاج السياسات نسبيًا، لكن كيف تحولها إلى ممارسات فعلية لدى عاملين يتنقلون ويفكرون ويبتكرون ويتواصلون، ويميلون بطبيعتهم إلى تجاوز الحدود المقررة؟

المعلومة خارج الأسوار:

أشد جوانب الإدارة إرباكًا ليس التقنية، ولا يلزم أن يستهدف الهجوم ما داخل الجدران. تقلل الجدران النارية وحماية الشبكات وكلمات المرور ومستويات الوصول الخطر، لكن انتشار أدوات يمكن إدخالها للعمل لتسهيل فقد المعلومات يتجاوز الحماية الصارمة يوميًا. فالهواتف وذاكرات الفلاش ومشغلات (MP3) والكاميرات تجتمع الآن في جهاز واحد قابل للاستخدام في السرقة.

ويسير العمل المنزلي والحوسبة المتنقلة التسرب أيضًا. نحمل معلوماتنا ومعلومات الشركاء إلى المقاهي ومكاتب غرفنا المنزلية، ونسافر بالأجهزة للعمل والعطلات عبر العالم، ونستخدم الشبكات اللاسلكية وشبكات الدول لمعالجة الأسرار وبيانات العاملين. ولا يمكن ضمان أمن هذه البيئات، وقد تكون معادية. ويلفت المؤلف إلى الفنادق والمطارات والمقاهي مواضع تعرض للمعلومات.

وتصعب حماية الوثائق والبيانات التي يحملها العاملون والمسافرون المتصلون، وتحتاج تدريبًا على مسارات الفقد عبر هذه الأدوات. لكن هل يلائم ذلك واقع عمل الجامعات؟

الأفراد يغيرون شكل الخطر:

يصنع الطلاب والموظفون والأكاديميون والإداريون نجاح الجامعة، وهم فضوليون ومتصلون ويحتاجون المعلومات ويحملونها معهم. وقد يغيرون الخطر بتجاوز الأنظمة وعدم الاستجابة للردع والدفاع. وقد ينقل احتياجهم للتدفق هجومًا عشوائيًا أو غير دقيق إلى مكان أشد ضررًا. وهذا سلوك بشري شائع ليس بالضرورة خبيثًا، لكنه قد يكون مؤذيًا جدًا.

ولا يحتاج استغلال السلوك إلى استثمار مالي من الخصم؛ فالجامعة أنشأت بالفعل بنى وشبكات المعالجة والتخزين والإدارة، وما عليه إلا إيجاد مدخل وقد يتكفل الأفراد بالباقي. ومن دون إدارة سلوك الأفراد، نسلّم مفاتيح التحكم ونسهّل المهمة على الخصوم.

نحتاج إلى قواعد، لكنها لا تنفع إلا برغبة الأفراد في الامتثال وقدرتهم عليه. وقد غير ترسخ الشبكات الاجتماعية والاتصال ذلك؛ فيلزم اتفاق صارم واضح بين المؤسسة والموظف وإجراءات تأديبية وتدريب ووعي بالمخاطر والعواقب. والأهم تحديد من يتحمل مسؤولية إدارة الخطر، وهي قضية تمس المؤسسة بأكملها. ويشير تقرير (Harvard Business Review) [7] إلى فجوة بين ثقة المؤسسات في غرس ثقافة الخطر وتنفيذها الفعلي؛ فقد يتصور الرؤساء أنهم ينجزون جيدًا لمجرد الحديث والميزانيات.

مسؤولية مشتركة:

جامعاتنا جزء من مجتمع أوسع يواجه تحديات كبيرة، وعليها حماية أصولها لأن العواقب المحتملة شديدة. ويجعلها البحث والابتكار والوصول المركب إلى معلومات استراتيجية أهدافًا تحتاج إدراك الضعف وإدارته.

ورغم مخاطر التقنية، ينشأ الضعف المتطور من تكيف البشر وتحولهم النفسي والاجتماعي وحاجتهم الدائمة إلى المشاركة. انظر في القطار أو الشارع إلى حركة المعلومات: إنها ظاهرة اجتماعية سلوكية تتيحها تقنية تلبي حاجات الاعتراف والتحفيز والمشاركة والتخزين والوصول والتواصل، أي عمل التعليم والبحث نفسه.

يمكن فرض نظم وإجراءات وأطر على النشاط الفكري والمعلومات التي نملكها ونشاركها، لكننا نتعامل في التعليم العالي أيضًا مع معلومات لا نملكها وعلينا حمايتها، مع حاجتنا المستمرة إلى استخدامها وتبادلها. وتضيف أعراف التواصل الجديدة طبقة من الثغرات المتغيرة سهلة الوصول.

وقد يفترض المربي أحيانًا أن من حوله أقل ذكاء أو قدرة؛ وربما صح أحيانًا، لكن افتراضه سيبرانيًا خطر أمام خصوم شديدي المهارة ذوي موارد ضخمة في حالات كثيرة. العقل الأكاديمي رائع مبتكر يستحق الرعاية، وعقل الخصم الخطر قادر أيضًا على التفوق على أساتذة كثيرين باستمرار؛ والخصوم لا يأخذون عطلات طويلة.

المراجع:

1. Universities UK , Cyber Security and Universities; Managing the Risk . Industry Report , 2013 London , Universities UK .
2. HM Government , A Strong Britain in an Age of Uncertainty; The National Security Strategy , Policy Report , 2010 , London , Cabinet Office .
3. HM Government , The UK Cyber Security Strategy; Protecting and Promoting the UK in a Digital World , 2011 , London , Cabinet Office .
4. Wilding E , Information Risk and Security , 2006 , London , Gower .
5. Wood P , 1 August 2013 , Cyber Cyber Burning Bright , Bucks New University Security blog : http://buckssecurity.wordpress.com/2013/08/01/cyber-cyber-burning-bright (accessed 12 April 2014).
6. Universities UK , ref. 1 .
7. Harvard Business Review Meeting the Cyber Risk Challenge . Report by Harvard Business Review Analytic Services , 2013 , Watertown , Harvard Business Review .