وجهات نظر ورؤى عالمية

الأمن السيبراني

الجزء 1: التهديدات السيبرانية في عالم معزز بالذكاء الاصطناعي

الجزء 2: ضمان المرونة السيبرانية

الجزء 3: إنشاء حدود جديدة لانعدام الثقة

قام بترجمة هذه الوثيقة الى اللغة العربية فريق عمل من جمعية المدققين الداخليين في لبنان برئاسة عضو مجلس الحكام الأستاذ ناجي فياض

The Institute of Internal Auditors

الجزء 1

التهديدات السيبرانية في عالم معزز بالذكاء الاصطناعي

نبذة عن الخبراء

أنطونيو كاتشيابوتي، وكالة المخابرات المركزية

أنطونيو كاتشيابوتي هو رئيس التدقيق الداخلي في Eurizon Capital S.A. Luxembourg ، شركة إدارة الأصول التابعة لمجموعة Intesa Sanpaolo.

برادلي نيدزيلسكي، محاسب قانوني

برادلي نيدزيلسكي هو شريك التدقيق والتأكيد وقائد التحول المالي والذكاء الاصطناعي في Deloitte & Touche LLP ، حيث يخدم الشركات العامة والخاصة في قطاع الخدمات المالية.

في العام الماضي، ترك التقدم في الذكاء الاصطناعي (الذكاء الاصطناعي) المؤسسات تتدافع لمواكبة وفهم الفرص والتهديدات التي تمثلها هذه التقنيات. كجزء من هذا الجهد، تحتاج الشركات إلى النظر في الخطر المتزايد الذي يمكن أن يشكله الذكاء الاصطناعي على جهودها الأمنية، خاصة بالنظر إلى اعتماد الشركات شبه الكامل على المعلومات والمعاملات عبر الإنترنت. سرعان ما تحولت الجهات السيئة إلى استخدام أدوات محسنة بالذكاء الاصطناعي لتحسين قدرتها على اختراق الدفاعات الإلكترونية للشركات. يدرس هذا الموجز كيف تغيرت التهديدات في عالم يحركه الذكاء الاصطناعي وكيف يمكن للتدقيق الداخلي أن يساعد الشركات على تطوير مناهج جديدة للأمن السيبراني استجابة لذلك.

تطور في الجرائم الإلكترونية

في حين أن الدفاعات السيبرانية القوية كانت دائما حاسمة، إلا أن مجرمي الإنترنت يستخدمون الآن الذكاء الاصطناعي لشحذ وتوسيع قدرتهم على التغلب على دفاعات المؤسسات. "الذكاء الاصطناعي ليس نوعا جديدا من الهجمات الإلكترونية، إنه تطور"، كما يقول أنطونيو كاتشيابوتي، رئيس التدقيق الداخلي في Eurizon Capital S.A. لوكسمبورغ. يستخدم الذكاء الاصطناعي بطرق أكثر تقدما من الهجمات الإلكترونية التقليدية من حيث السرعة والحجم والتعقيد والقدرة على التكيف. بالإضافة إلى ذلك، " فإنه يبني مقاومة بمرور الوقت، مثل الفيروس، مما يجعله أكثر خطورة"، كما يقول.

يتم استخدام الذكاء الاصطناعي في الهجمات التي تتراوح من التركيز الضيق إلى المدمرة على نطاق واسع. على سبيل المثال، في حين أن الكثيرين في عالم الأعمال يستخدمون الآن بانتظام المستندات التي تم إنشاؤها بواسطة الذكاء الاصطناعي لرسائل البريد الإلكتروني أو التقارير، فإن مجرمي الإنترنت يستخدمون أيضا المستندات التي تم إنشاؤها بواسطة الذكاء الاصطناعي لأغراض إجرامية، كما يقول برادلي نيدزيلسكي، شريك التدقيق في ديلويت في نيويورك.

على جبهة أخرى، تهدف هجمات التصيد الاحتيالي إلى اختراق الحواجز الأمنية والوصول إلى البيانات القيمة. على الرغم من أن التصيد الاحتيالي ليس جديدا، إلا أن مكتب التحقيقات الفيدرالي يحذر من هجمات التصيد الاحتيالي التي تعتمد على الذكاء الاصطناعي "تتميز بقدرتها على صياغة رسائل مقنعة مصممة خصيصا لمتلقين محددين وتحتوي على قواعد وتهجئة مناسبة، مما يزيد من احتمالية الخداع الناجح وسرقة البيانات".

يتم تخصيص التصيد الآلي المركز spear phishing، على سبيل المثال، لشخص واحد أو مجموعة ويهدف إلى سرقة المعلومات الحساسة أو الوصول إلى نظام. يوضح Cacciapuoti: "يمكن ل الذكاء الاصطناعي تحليل وسائل التواصل الاجتماعي وأنماط الاتصال والبيانات المتاحة حول الهدف، ثم صياغة رسائل من المرجح أن تخدع المستلمين للكشف عن معلومات حساسة أو النقر فوق الروابط الضارة". في الوقت نفسه، في حين أنه ربما كان من الممكن الوثوق بمقطع فيديو أو مكالمة في الماضي بناء على معرفة صوت الشخص أو ميزاته، مع التزييف العميق (مقاطع فيديو محاكاة لفرد) والقرصنة الصوتية، التي تكرر صوت الشخص، فمن الممكن خداع أهداف محددة والتلاعب بها.

هذه ليست التهديدات الوحيدة المتعلقة بالذكاء الاصطناعي التي تواجهها المؤسسات. يمكن للبرامج الضارة التي تعمل بواسطة الذكاء الاصطناعي التكيف وتغيير سلوكها بناء على البيئة المستهدفة، مما يجعل من الصعب على نظام الأمان التقليدي اكتشافه، وفقا ل Cacciapuoti. يقول: "يمكنه بسهولة الهروب من الاكتشاف الأساسي واستخدام تقنيات متعددة الأشكال لتغيير رمزه وحتى تحليل التدابير الدفاعية لتجنبها". والأهم من ذلك، أنه يمكن أن يدخل البيانات المسمومة في نموذج التعلم الآلي للذكاء الاصطناعي المستخدم في نظام الكشف عن الاحتيال، مما يؤدي إلى قيام الذكاء الاصطناعي بعمل تنبؤات غير دقيقة والتغاضي عن بعض مؤشرات الاحتيال.

باستخدام الاستخراج الذكي للبيانات، يمكن للذكاء الاصطناعي تحليل البيانات المسروقة والملكية الفكرية في الوقت الفعلي وتحديد أولويات المعلومات الأكثر قيمة للتسلل. يمكنه بعد ذلك تشفير هذه المعلومات والمطالبة بفدية لتحريرها، كما يقول "يمكن للهجمات التي تعتمد على الذكاء الاصطناعي أيضا أن تعرض بيانات الاعتماد التي تصادق على المستخدمين الصالحين للخطر، مما يمكنهم من التنقل عبر النظام."

تعد مخاطر الهجمات الإلكترونية التي تعتمد على الذكاء الاصطناعي مهمة لأن المخاطر كبيرة للغاية. قد يؤدي تسرب المعلومات الحساسة أو إساءة استخدامها إلى الإضرار بالمكانة التنافسية للمؤسسة أو تعريضها لعقوبات لعدم الامتثال للوائح خصوصية البيانات. يمكن أن يؤدي أي خرق إلى فقدان العملاء وشركاء الأعمال للثقة في المؤسسة. يمكن لهجمات برامج الفدية الضارة أن تعطل العمليات وتغلق الأنظمة الهامة.

لم يكن من الممكن تصور العديد من الاستخدامات منذ وقت ليس ببعيد، لكنها تلعب في الوقت الفعلي اليوم. على سبيل المثال، دفع موظف في شركة متعددة الجنسيات في هونغ كونغ عن غير قصد 25 مليون دولار للمحتالين بعد إقناعه بالقيام بذلك من خلال محاكاة التزييف العميق للمدير المالي للشركة في مكالمة فيديو، وفقا لشبكة سي إن إن.

في مكان آخر، ذكرت The Drive أن مسؤولا تنفيذيا في فيراري تلقى مكالمة هاتفية من شخص يستخدم التزييف العميق أدعى أنه الرئيس التنفيذي للشركة. تم إحباط المحاولة عندما طرح المدير التنفيذي المشبوه سؤالا لا يمكن إلا للرئيس التنفيذي الإجابة عليه. وفي حالة ذكرتها Greylock Partners ، استخدم جاسوس كوري شمالي هوية مزيفة ليتم تعيينه من قبل شركة للأمن السيبراني، ثم قام على الفور بتثبيت برامج ضارة على أجهزة شركتها.

أفضل دفاع

لحسن الحظ، يمكن أن يساعد الذكاء الاصطناعي أيضا المؤسسات على إحباط هجمات مجرمي الانترنت. يقول Cacciapuoti: "لإيقاف الذكاء الاصطناعي، عليك استخدام الذكاء الاصطناعي". تحتاج المؤسسات إلى اعتماد تدابير أمن إلكتروني أكثر تعقيدا تعمل بطاقة الذكاء الاصطناعي لمواكبة التهديدات المتطورة. "إذا لم تكن لديك معرفة عميقة بالتكنولوجيا التي يستخدمها المجرمون، فكيف يمكنك إيقافهم؟" يسأل. يجب على المؤسسات التعرف على الأدوات والاستراتيجيات التي يستخدمها مجرمو الإنترنت وفهم الطرق العديدة التي يمكنهم من خلالها المساعدة في تعزيز الأمن السيبراني.

يحدد تقرير "الحاجة إلى الأمن السيبراني المدعوم من الذكاء الاصطناعي لمعالجة الهجمات التي تحركها الذكاء الاصطناعي" ، من ISACA، العديد من الطرق التي يمكن أن تساعد بها التقنيات المتقدمة في منع الهجمات:

طرق منع الهجمات

- تحليل مجموعات البيانات الضخمة لتحديد كيفية استخدام الموارد التنظيمية ، وتحديد المناطق المكشوفة ، وإنشاء مخزون للأصول ، وتحديد اتجاهات حركة مرور الشبكة وأنشطة / سلوكيات المستخدم.
- الكشف عن الحالات الشاذة ، بما في ذلك "عمليات تسجيل الدخول غير العادية ، وطلبات الوصول من موقع جغرافي جديد أو عنوان IP ، ووصول مستخدم جديد، وتغيير الأذونات على الملفات والموارد الأخرى ، واستخراج أو حذف كميات كبيرة من الملفات ، وزيادة هائلة في حركة المرور."
- استخدام الذكاء الاصطناعي لتأمين الجهات الفاعلة السيئة المشتبه بها أو تسجيل الخروج منها أو حظرها بشكل استباقي وتنبيه مسؤولي النظام إلى نشاطهم.
- أنظمة المراقبة المستمرة لتمكين الاستجابات السريعة.
- استخدام التحليل التنبؤي لتوقع التهديدات الأمنية المحتملة واتخاذ خطوات لمنعها.
- اكتشاف ومنع تهديدات يوم الصفر، أو الثغرات الأمنية الجديدة وغير المرئية.
- تقليل عدد التهديدات الإيجابية المحتملة الكاذبة.
- أتمتة تقييمات الأمان لتسريع الاستجابات وتقليل الأخطاء البشرية.
- التوسع للتكيف مع التطورات والبيئات الجديدة لتوفير الحماية المستمرة.

يقول Cacciapuoti إنه يمكن للمؤسسات الاستفادة من الذكاء الاصطناعي لتجميع البيانات من مصادر متعددة وتحليلها وربطها لإنشاء رؤى أعمق. يمكنهم أيضا استخدام معالجة اللغة الطبيعية (NLP) لتحليل البيانات النصية الكبيرة. على سبيل المثال، عندما يطلب من المدققين الداخليين تحليل العقود، يمكن للبرمجة اللغوية العصبية استخراج البيانات النصية المهمة للنظام لتحليلها.

معالجة اعتبارات الذكاء الاصطناعي

نظرا لأن المؤسسة لا يمكنها أبدا معالجة 100٪ من المخاطر، توصي Niedzielski بالبدء بتقييم التهديدات بشكل استراتيجي عبر مجالات مختلفة من العمل. وسيشمل ذلك تحديد نواقل الاحتيال المحتملة في الذكاء الاصطناعي وتقييم احتمالية تعرضها للهجوم والحجم والتأثير المحتملين. ويقول إن الخطوة التالية هي تحديد فعالية الضوابط الحالية.

كجزء من هذا الجهد، يوصي Niedzielski باستخدام قدرات GenAI الناشئة، مثل التفكير المتقدم والتعرف على الأنماط، للتعرف على التكتيكات الشائعة مثل محاولات التصيد الاحتيالي التي تم إنشاؤها بواسطة الذكاء الاصطناعي والتزييف العميق. تستخدم بعض الشركات البروتوكولات والتقنيات للتحقق مما إذا كان قد تم إجراء مكالمة من رقم داخلي أو خارجي.

يقول: "يمكن أن تساعد هذه التقنيات المتقدمة في تقليل المخاطر المرتبطة بها". ومع ذلك، في بعض الحالات، مثل اتخاذ قرار فوري بشأن ما إذا كان المتصل أو المشارك في الاجتماع مزيفا deepfake، قد يضطر الموظفون إلى الاعتماد على المشاعر الغريزية أو أن يكونوا مستعدين للتساؤل عن سبب اتصال الرئيس التنفيذي وطلب تحويل الأموال، على سبيل المثال. في هذه الحالات، يجب تشجيع الموظفين على الوثوق بغرائزهم والاتصال بالشخص مرة أخرى على رقم شركتهم، أو إذا كان المتصل المزعوم في نفس المكتب، فما عليك سوى السير في القاعة للتحقق من هويته.

يمكن لفريق متعدد التخصصات مكون من محترفين من مجالات مثل التدقيق الداخلي وإدارة المخاطر وتكنولوجيا المعلومات والأمن السيبراني والوظائف الأخرى ذات الصلة مراقبة التطورات في الذكاء الاصطناعي وتقديم تحديثات مستمرة لإدارة المخاطر وبروتوكولات الأمان وأنظمة الكشف عن الاحتيال. يمكن للفريق العمل معا لتحديد الجهود والاستجابة لها، مع الأخذ في الاعتبار قضايا مثل الضوابط التي ستمنع الضرر أو تحده بشكل أفضل، كما يقول Niedzielski.

كما يوصي الشركات بمشاركة تجاربها بانتظام ومناقشة نقاط الذكاء الاصطناعي التي واجهها الآخرون. "ليس فقط الجهود الناجحة، ولكن أيضا الأوقات التي حدث فيها خطأ ما وكيف تعلمت الشركة منه" ، كما ينصح. "إن تبادل المعرفة والتدريب والتقييمات المناسبة للمخاطر ستجعل من الممكن تقليل مخاطر الاحتيال الناجم عن الذكاء الاصطناعي."

في هذه البيئة، يجب أن يكون التدريب أولوية قصوى لزيادة وعي الموظفين بالأنشطة المشبوهة المحتملة مع تعزيز مسارات العمل المناسبة لمعالجة الانتهاكات، كما يقول Niedzielski. يلاحظ Cacciapuoti أنه من الممكن أيضا استخدام محاكاة الذكاء الاصطناعي لتوفير التدريب على الأمن السيبراني في الوقت الفعلي في مواقف العالم الحقيقي. يمكن للذكاء الاصطناعي تحليل سلوك الموظف الفردي في التدريب السيبراني وتقديم رؤى للتحسين.

مساهمة التدقيق الداخلي

> "لن يحل الذكاء الاصطناعي محل المدققين الداخليين أبدا، ولكن يمكن أن يكون مساعدا قويا."
>
> **- أنطونيو كاتشيابوتي ، مدقق داخلي مجاز**

يقول Cacciapuoti إن التدقيق الداخلي يمكن أن يساعد في ضمان توافق جهود المؤسسة مع تحديات الذكاء الاصطناعي، بما في ذلك تسخير الإمكانات مع التخفيف من المخاطر. يقول: "يجب أن يجري التدقيق الداخلي تقييما شاملا للمخاطر، وتدقيق أنظمة الذكاء الاصطناعي للأمن والأخلاقيات والامتثال ودعم الابتكار الآمن". "يمكن أن تشارك في تشكيل استراتيجية إلكترونية قوية بما يكفي للتعامل مع تهديدات الذكاء الاصطناعي."

بالإضافة إلى ذلك، في حين أن التدقيق الداخلي عادة ما يكون خط دفاع رئيسيا، يقول Cacciapuoti إنه يجب أن يكون أيضا بمثابة خط هجوم فيما يتعلق بالذكاء الاصطناعي، مع اتباع نهج ديناميكي في إدارة المخاطر. "لماذا تنتظر وصول المخاطرة بينما يمكنك مهاجمتها وجها لوجه؟" هو يسأل. وهذا يعني أن تكون في طليعة استخدام التقنيات الجديدة حتى تتمكن المؤسسة من زيادة الفرص مع ضمان ضوابط الحوكمة المناسبة والتحسين المستمر.

"لن يحل الذكاء الاصطناعي محل المدققين الداخليين أبدا، ولكن يمكن أن يكون مساعدا قويا"، وفقا ل Cacciapuoti "إن التدقيق الداخلي يمكن أن يستفيد من استخدام الذكاء الاصطناعي من أجل:

- القيام بتحليل كميات كبيرة من البيانات وتوسيع العينات في الاختبار لتكون قريبة جدا من حجم مجموعة المعلومات بالكامل.
- أتمتة إجراءات الاختبار ومراقبة عناصر التحكم الرئيسية، وتولي المهام المتكررة حتى يتمكن محترفو التدقيق الداخلي من التركيز على المهام ذات المستوى الأعلى.
- استخدام خوارزميات الذكاء الاصطناعي لمراقبة البيانات باستمرار بدلا من الاعتماد على عمليات التدقيق الدورية وتحديد الأنشطة غير العادية ومعالجتها في وقت أقرب بكثير.
- استخدام التحليلات التنبؤية لتوقع النتائج المستقبلية واتخاذ قرارات وتوصيات أكثر استنارة.
- القيام بتلخيص أوراق العمل بسرعة حتى يتمكن المدققون الداخليون من استخدامها في صياغة التقارير النهائية.

يسمح الذكاء الاصطناعي بإدارة أكثر اتساقا وكفاءة للنتائج عبر جميع وظائف التحكم. يقول Cacciapuoti: "في شركة كبيرة جدا، هناك العديد من الارتباطات من وظائف متعددة يجب مراعاتها". يمكن الذكاء الاصطناعي المدققين الداخليين من تجميع البيانات معا بطريقة موحدة لتجنب الازدواجية.

للتخفيف من المخاطر والاستفادة من القيمة، يوصي Niedzielski بأن يقوم المدققون الداخليون بتحديث معرفتهم باستمرار حول التقدم التكنولوجي. يقول: "هناك شيء جديد كل يوم". يجب أن تركز على تحديد الاستجابات الاستباقية - بدلا من رد الفعل - للمخاطر المحتملة. ويقول إنه بينما يحاول العالم تسخير التقنيات الجديدة، يجب على المدققين الداخليين أيضا التركيز على الحوكمة والامتثال للوائح الجديدة والمعايير الأخلاقية لحماية النزاهة التنظيمية.

"يجب على المدققين الداخليين أن يضعوا أنفسهم مكان الجهات السيئة"، وفقا ل Niedzielski.

"لا تسأل كيف سيتسلل مجرم ما إلى المؤسسة، اسأل ماذا ستفعل إذا كنت انت ذلك المجرم بناء

على ما تعرفه عن المؤسسة. لا تأخذ في الاعتبار الناحية الكمية فحسب، بل أيضا الناحية النوعية للمؤسسة ".

يقول كاتشيابوتي، الذي يوصي بالتنسيق مع جميع مزودي التأكيد وأصحاب المصلحة لمنع المخاطر والتخفيف من حدتها، بما في ذلك أولئك الذين يعملون في وظائف الرقابة والامتثال، وإدارة المخاطر ، والمدققين الخارجيين والمنظمين. يقول: "يعد التعاون بين أدوات الذكاء الاصطناعي والمتخصصين في الأمن السيبراني، جنبا إلى جنب مع إطار حوكمة قوي، أمرا ضروريا للتنقل في هذا المشهد والاستجابة للمخاطر الجديدة والناشئة".

التهديدات السيبرانية التي تعمل بالطاقة الذكاء الاصطناعي: حقائق سريعة

- يشعر 97٪ من المتخصصين في مجال الأمن بالقلق من أن مؤسساتهم ستتعرض لحادث أمن إلكتروني ناتج عن الذكاء الاصطناعي، حيث يستمر الذكاء الاصطناعي في التسبب في الإرهاق.
- اضطر 75٪ من المتخصصين في مجال الأمن إلى تغيير إستراتيجيتهم للأمن السيبراني في العام الماضي بسبب ارتفاع التهديدات السيبرانية التي تعمل بالطاقة الذكاء الاصطناعي.
- يرغب 73٪ من فرق الأمان في التركيز بشكل أكبر على قدرات الوقاية أولا.
- شهدت 61٪ من المؤسسات ارتفاعا في حوادث التزييف العميق خلال العام الماضي.
- 75٪ من هذه الهجمات انتحلت صفة الرئيس التنفيذي للمؤسسة أو عضو آخر في C-suite.

المصدر:الذكاء الاصطناعي العام في الأمن السيبراني: صديق أم عدو؟ صوت من SECOPS، الطبعة الخامسة 2024.

الجزء 2

ضمان المرونة السيبرانية

نبذة عن الخبراء

DC Chang ، CPA ، CDPSE ، CISSP ، CRISC ، CISA

دي سي تشانغ هو مدير التدقيق ، التكنولوجيا الرقمية والأمن السيبراني، في بونايتد إيرلاينز في دالاس، تكساس.

مايكل إيكولز، CISSP

مايكل إيكولز هو الرئيس التنفيذي لشركة ماكس سيبر سيكيوريتي ذ.م.م في واشنطن العاصمة.

جاستن هيدلي، CPA، CRISC ، CISA ، CISSP

جاستن هيدلي هو مدير أول في مجموعة خدمات استشارات المخاطر والضمان التابعة لشركة وارن أفيريت في برمنغهام ، ألاباما.

نظرا لأن المؤسسات تعمل على ضمان امتلاكها للأدوات الكافية لمنع الهجمات الإلكترونية، فمن المؤكد تقريبا أنها ستواجه خروقات أو توغلات بشكل ما. مع وضع ذلك في الاعتبار، يجب على الشركات أيضا التركيز على قدرتها على الاستجابة والتعافي بسرعة من الهجوم الإلكتروني. يناقش هذا الموجز أفضل السبل لفهم وغرس المرونة في مواجهة الهجمات ويصف دور المدقق الداخلي في تعزيز استجابة المؤسسة.

المرونة السيبرانية هي "القدرة على توقع الظروف المعاكسة والتعافي منها والتكيف معها وتحملها أو الضغوط أو الهجمات على الأنظمة التي تستخدم الموارد السيبرانية أو يتم تمكينها بواسطتها. تهدف المرونة السيبرانية إلى تمكين تحقيق أهداف المهمة أو الأعمال التي تعتمد على الموارد السيبرانية في بيئة إلكترونية متنازع عليها ".

- المعهد الوطني الأمريكي للمعايير والتكنولوجيا

تمهيد الطريق للتعافي

في أفضل حالاتها، لا تعد المرونة السيبرانية مجرد رد فعل على وضع شديد الصعوبة. إنها سلسلة متصلة من الممارسات - التخطيط والعمليات والتحليل والتدريب والخدمات الحيوية والإدارة - التي تضمن قدرة المؤسسة على الحفاظ على العمليات، وفقا لمايكل إيكولز ، الرئيس التنفيذي لشركة Max Cybersecurity LLC. تتيح هذه الممارسات استعادة الوظائف التنظيمية أو الحفاظ عليها بعد الهجوم، ولكن يجب وضعها في مكانها قبل وقت طويل من حدوث المشكلة.

على سبيل المثال، عملت Echols مع عميل شركة محاماة تلقى جميع إحالاته من خلال موقعه على الإنترنت. عادة ما تتلقى العديد من الإحالات يوميا، ولكن في مرحلة ما ، مر يومان إلى ثلاثة أيام قبل أن تلاحظ الشركة أنها لا تتلقى أيا منها وتدرك في النهاية أنها تعرضت للاختراق. يقول: "كان يجب أن يكون لدى الشركة بالفعل عملية للمراقبة المستمرة ونوع من الإخطار" حول انخفاض غير عادي في إحالات االويب،لأنها كانت المصدر الرئيسي لأعمال الشركة (وظيفة حاسمة) ، كما يقول.

ستكون المشكلات التي يجب تحديدها - مثل انخفاض حركة المرور على الويب - مختلفة لكل عمل ومن المحتمل أن يكون هناك أكثر من واحدة. في كثير من الحالات، سترغب المؤسسات في الاستعداد لحادث سيؤثر على إمدادات الطاقة الخاصة بها ، على سبيل المثال، مع خطوات لنشر مولدات مستقلة عن العمل الرئيسي، حتى لا تتأثر بالهجوم، كما يقول إيكولز.

يتطلب الاستعداد لليوم التالي، وضع بيئة الأمن السيبراني الحالية في سياقها، وفقا ل DC Chang ، مدير التدقيق، التكنولوجيا الرقمية والأمن السيبراني، في United Airlines. قبل عشرين عاما، كان لدى المؤسسات مراكز بيانات خاصة بها، وكان الأمن السيبراني، إلى حد ما، مسألة قفل الخوادم خلف الأبواب والنوافذ المادية. اليوم، يتم تخزين البيانات في بيئة افتراضية يمكن أن تكون عرضة للجهات الفاعلة السيئة في جميع أنحاء العالم.

يقول تشانغ: "هناك الآلاف من النوافذ والأبواب التي نحتاج إلى تتبعها الآن بعد أن أصبحنا رقميين، ويتم إضافتها وإزالتها على أساس يومي". تحتاج المؤسسات إلى أن تكون على دراية بوتيرة ونطاق التسريع الرقمي لتطوير المرونة التي ستحتاجها في الأزمات.

الحوكمة والثقافة

تلعب الحوكمة دورا رئيسيا في بناء المرونة السيبرانية، وفقا لجاستن هيدلي، المدير الأول في مجموعة خدمات استشارات المخاطر والتأكيد التابعة لشركة Warren Averett. يقول: "نسمع باستمرار أن الموظفين هم نقطة الضعف لأنهم يستخدمون كلمة مرور ضعيفة أو ينقرون على روابط مشبوهة". "ولكن إذا لم يعط القادة المثل الصالح، فلا يمكنك أن تتوقع من الموظفين القيام بدورهم."

من نواح كثيرة، لا يعد الأمن السيبراني مشكلة تقنية بالكامل، بل هو مصدر قلق ثقافي. يقول إيكولز: "إذا غيرت رأي 90٪ من الأشخاص في المؤسسة وفتح شخص واحد رابطا في رسالة بريد إلكتروني، فقد يؤدي ذلك إلى إغراق الشركة". توضح الثقافة المدركة للأمن السيبراني توقعات المؤسسة وتطمئن المستهلكين وشركاء الأعمال. يقول: "كانت البنوك من أولى المجموعات التي أصبحت مرنة عبر الإنترنت"، لأنها تعتمد على ثقة أصحاب المصلحة.

يوصي هيدلي القادة بتعزيز ثقافة الأمن السيبراني التي تتجاوز الأساليب القياسية مثل رسائل البريد الإلكتروني الفصلية التي تحتوي على نصائح السلامة السيبرانية أو التدريب الأمني السنوي البدائية. تشمل الخطوات التي تتخذها مؤسسته إرسال رسائل بريد إلكتروني تصيد مزيفة خاصة بها إلى الموظفين، ثم توفير التدريب لأولئك الذين ينقرون على الروابط المشبوهة المضمنة. يقول: "عليك أن تظهر كيف تعمل الحوكمة السيبرانية عمليا، وليس فقط من الناحية النظرية".

يمكن للقادة أيضا تقديم خطوات محددة لاتخاذها في الهجوم. "يمكن للمؤسسة إيقاف الهجوم والتعافي إذا كانت هناك سياسات وإجراءات عملية وقابلة للتكرار يجب اتباعها في حالة الخرق"، وفقا لهيديلي. إذا شارك القادة عند اختبار هذه الخطوات وشاركوا في حل مكامن الخلل، فإنهم يظهرون التزامهم بالجهد المبذول، والذي يمكن أن يلعب دورا كبيرا في إنجاح استراتيجية الأمن السيبراني الخاصة بهم.

- 68٪ من الانتهاكات تضمنت عنصرا بشريا غير ضار، مثل وقوع شخص في هجوم هندسة اجتماعية أو ارتكاب خطأ.
- كان متوسط الوقت الذي يستغرقه المستخدمون من خلال رسائل البريد الإلكتروني المخادعة أقل من 60 ثانية.
- 15٪ من الانتهاكات تضمنت طرفا ثالثا أو موردا ، بما في ذلك سلاسل توريد البرامج وشريك الاستضافة

للبنى التحتية، أو أمناء البيانات.

المصدر: خرق بيانات Verizon Business 2024
تقرير التحقيقات

تأثير التنظيم

بموجب القاعدة النهائية "إدارة مخاطر الأمن السيبراني ، والاستراتيجية ، والحوكمة ، والإفصاح عن الحوادث "، رفعت لجنة الأوراق المالية والبورصات الأمريكية توقعات المؤسسات من خلال مطالبة الشركات العامة بالكشف عن حوادث الأمن السيبراني المادية وإجراء إفصاحات دورية حول كيفية تقييم المخاطر السيبرانية وتحديدها وإدارتها. يقول تشانغ إن القاعدة "تسلط الضوء على قضية رئيسية تتعلق بالرهانات على الطاولة يجب على كل كيان على هذا الكوكب مراعاتها".

من بين المتطلبات الأخرى، تجبر القاعدة المؤسسات على ضمان تشغيل ممارساتها السيبرانية، كما يقول هيدلي. ويشير إلى أن وظيفة تكنولوجيا المعلومات غالبا ما تعمل داخل صومعة، مع ثقة ضمنية من القادة الذين قد لا يفهمون أعمالها تماما. يقول: "يجب أن يتغير ذلك". يجب أن يكون هناك فهما على مستوى المؤسسة لكيفية التعامل مع البيانات الداخلية وبيانات العملاء ومعالجة المخاوف السيبرانية.

كما هو الحال مع العديد من اللوائح، "سيعود الأمر كله إلى الشفافية"، كما يقول إيكولز. "عندما يكون هناك خرق مادي، يجب أن يكون لدى الشركة عملية واضحة لكيفية تفاعلها مع هذا الخرق."

إضافة الذكاء الاصطناعي إلى المزيج

يمكن أن يكون الذكاء الاصطناعي أداة لا تقدر بثمن في تعزيز الوقاية من المشكلات السيبرانية والمرونة في أعقاب الهجوم. يقول هيدلي إن التكنولوجيا مثل جدران الحماية من الجيل التالي وأنظمة حماية النقاط تجعل من السهل فرز حركة البيانات والعثور على الحالات الشاذة التي يجب التحقيق فيها. "لقد أدى استخدام الذكاء الاصطناعي إلى تغيير قواعد اللعبة في السنوات العديدة الماضية، وسيستمر في مساعدة الشركات على التحسن في اكتشاف الهجمات والاستجابة لها."

يمكن أيضا استخدام الذكاء الاصطناعي كسلاح ضد المؤسسات. يقول إيكولز: "إذا كانت لديك نقاط ضعف تم تجاهلها، فسيساعد الذكاء الاصطناعي المتسللين في العثور عليها".

من بين الاعتبارات الأخرى، سيتعين على المؤسسات تحقيق التوازن بين الدافع لتحقيق قدر أكبر من الكفاءات مع الأدوات الجديدة مع الحاجة إلى حماية الأمن والخصوصية، وفقا لهيديلي. تساعد التقنيات الجديدة المؤسسات على التخلص من المهام القابلة للتكرار، والتي غالبا ما تتضمن تغذية البرامج بمعلومات حساسة. في الوقت نفسه، "ما زلنا نرى هجمات مستهدفة على هذه التقنيات لأن الجهات الفاعلة السيئة تعرف أن الناس لا يفهمون التكنولوجيا تماما"، مما قد يجعل البيانات الحساسة التي تحتويها البرامج عرضة للخطر بشكل خاص.

في بناء المرونة، سيتعين على المؤسسات تدريب موظفيها على التقنيات المتطورة والتأكد من أن استخدام التكنولوجيا يتوافق مع رغبة المخاطرة لدى المؤسسة. يقول هيدلي: "يمكن أن تمتلك الشركة أفضل التقنيات والمهارات، ولكن قد لا يزال المستخدم يسرب البيانات عن غير قصد أو في بعض الأحيان عن قصد عبر الباب الأمامي باستخدام أداة GenAI".

يجب على المؤسسات أيضا الحرص على عدم إهمال مناهج الهجمات الإلكترونية التقليدية. يقول إيكولز إن العديد من المشكلات السيبرانية ناتجة عن مشاكل ليست جديدة، مثل التكوينات الخاطئة أو الفشل في اتباع ممارسة راسخة. ويقول إن العديد من الانتهاكات تتعلق بنقاط الضعف المعروفة التي لم يتم إصلاحها مطلقا أو التصحيحات التي لم يتم تثبيتها. نتيجة لذلك، يعد تثقيف المستخدمين النهائيين حول التهديدات الجديدة والحالية أمرا مهما بشكل خاص. يقول: "يجب على المدققين النظر بكل الجوانب المخفية وطرح الأسئلة الصحيحة على العملاء للكشف عن نقاط الضعف الخفية الناتجة عن اللامبالاة".

تمد أصحاب المصلحة ، وخاصة مجلس إدارة
ؤسسة والإدارة العليا ، على خدمات التأكيد
ستقلة والموضوعية والمختصة للتحقق مما إذا
ت ضوابط الاستجابة للحوادث السيبرانية
عافي مصممة بشكل جيد ونفذت بفعالية
اءة. تضيف وظيفة التدقيق الداخلي قيمة إلى
مؤسسة عندما تقدم هذه الخدمات بما يتفق مع
ايير ومع إشارات إلى أطر الرقابة المقبولة
ى نطاق واسع، ولا سيما تلك المستخدمة
احة في تكنولوجيا المعلومات و في وظائف
المعلومات".

در: دليل التدقيق التكنولوجي العالمي: مراجعة الاستجابة
ادث السيبرانية والتعافي منها، الطبعة الثانية، دليل الممارسات

كيف يمكن أن يساعد التدقيق الداخلي في تعزيز المرونة

في هذه البيئة، يجب أن يكون التدقيق الداخلي مستعدا لتأطير نتائج عمليات التدقيق الخاصة بهم لتعزيز المرونة وتحديد نقاط الضعف بطرق تساعد العملاء على فهم العواقب المحتملة للتراخي في الأمن السيبراني، كما يقول إيكولز. في حين أن العملاء قد يفترضون أن الأسوأ لا يمكن أن يحدث لهم أبدا، يجب أن يكون المدققون الداخليون قادرين على عدم الركون لهذا الافتراض السائد، مما سيمكنهم بشكل أفضل من تخيل ما لا يمكن تصوره. على سبيل المثال، كان لدى Echols عميل لديه أفضل الممارسات التي تحظر استخدام عناوين البريد الإلكتروني للشركات في حسابات وسائل التواصل الاجتماعي، لكنها لم تكن سياسة رسمية. أصبح خطأ هذا النهج واضحا عندما عانت MGM من خرق كبير للبيانات في أواخر العام الماضي. وبحسب ما ورد كشف التحقيق في الخرق أن موظفا كان يستخدم بريده الإلكتروني للعمل على منصة وسائط اجتماعية. عثر المتسللون على معلومات الموظف على LinkedIn وانتحلوا شخصية الموظف في مكالمة إلى مكتب مساعدة تكنولوجيا المعلومات في MGM، وبالتالي الحصول على بيانات اعتماد للوصول إلى أنظمة MGM وإصابتها. يقول إيكولز: "أفضل الممارسات مستمدة من تجارب الكثيرين ويجب أن تكون بمثابة سياسة متبعة، عندما يكون ذلك ممكنا".

يجب أن يفهم المدققون الداخليون أيضا أن جانب الامتثال في التدقيق ليس سوى الخطوة الأولى في المساعدة في بناء المرونة السيبرانية. يقول إيكولز: "الامتثال ليس أمانا". يجب أن يركز المدققون الداخليون على ترجمة النتائج التي توصلوا إليها إلى رؤى أكبر يمكن لفريق العميل استخدامها لتعزيز الأمان وعلى طرح الأسئلة التي قد لا يتمكن الفريق من الإجابة عليها بعد.

"يجب أن تكون قادرا على إرشاد العميل إلى أن عدم البحث عن إجابة لهذا السؤال والعثور عليه يخلق في الواقع نقطة ضعف"، وفقا ل Echols.

يجب أن يبقي التدقيق الداخلي خطوط الاتصال مفتوحة من خلال جدولة الأوقات لتسجيل الوصول والتعرف على تحديات الفرق. يقول هيدلي: "عندما يكون المدققون الداخليون قادرين على وضع أنفسهم كمستشارين موثوق بهم، فإن ذلك يغير قواعد اللعبة تماما".

الشفافية أمر بالغ الأهمية. يجب أن يكون المدققون الداخليون واضحين بشأن النطاق وإجراءات الاختبار المخطط لها، وكذلك القضايا التي نشأت. يقول: "تأكد من التواصل مبكرا وفي كثير من االأحيان، خاصة عندما ينطوي الامر على مخاطر تكنولوجيا المعلومات". ينصح المدققين الداخليين بتجنب التسرع في الحكم على الفور، ولكن بدلا من ذلك إجراء محادثة مفتوحة حول عمليات تفكير فريق العميل وتشجيع التعاون.

يلاحظ هيدلي أن فرق تكنولوجيا المعلومات غالبا ما تتعثر في تلبية متطلبات خطوط الأعمال المختلفة، وتتحمل المسؤولية عن كل شيء بدءا من الحفاظ على تشغيل التطبيقات وتشغيلها إلى التعامل مع مواطن الخلل اليومية في الأجهزة. نتيجة لذلك، قد لا يكون الأمن السيبراني دائما أولوية قصوى. يمكن للمدققين الداخليين تعزيز الوعي بهذه التحديات وتثقيف الفرق حول فرص معالجتها، وبالتالي ضمان أن تكون عمليات التدقيق تمرينا حقيقية ذات قيمة مضافة.

يقول هيدلي: "يمكن للمدققين الداخليين أن يكونوا شركاء في المساعدة على تعزيز مرونة الشركات". من بين الخطوات الأخرى، يمكنهم المساعدة في تخفيف أي انفصال بين قادة الشركة وفرق تكنولوجيا المعلومات، الذين لا يتحدثون نفس اللغة في كثير من الأحيان. نظرا لأن المدققين الداخليين يفهمون كلا من مخاطر الأعمال ومخاطر تكنولوجيا المعلومات، فيمكنهم المساعدة في سد هذه الفجوة.

يقول تشانغ إن المدققين الداخليين يمكنهم أيضا تشكيل فهم المخاطر السيبرانية وحل المشكلات ذات الصلة بطريقة تخرج عن الممارسة السابقة. مع ابتعاد المؤسسات عن التخطيط التقليدي لاستمرارية الأعمال أو التعافي من الكوارث في الأعمال، يمكن للمدققين الداخليين مساعدتهم على تبني مناهج دقيقة ومتعددة الأوجه. يمكنهم تعزيز هذا الجهد من خلال القيام بدور الربط بمعالجة المعلومات ونقاط البيانات غير المتصلة وتجميعها معا في سرد مقنع يقود إلى اتخاذ قرارات أفضل.

تحسين الاحتمالات

في النهاية، تعني المرونة قبول حتمية الهجوم وافتراض أن الجدران الخارجية للمؤسسة يمكن اختراقها، يلاحظ إيكولز. كجزء من هذا الجهد، يجب على المنظمات أن تدرك أنها تخوض معركة غير عادلة. بينما تسعى المؤسسات جاهدة لمنع 100٪ من الهجمات التي تواجهها، يحتاج المتسللون فقط إلى فتح باب واحد لإحداث الفوضى، كما يلاحظ تشانغ. يقول: "من الأصعب بكثير أن تكون المدافع عن الجاني". يمكن أن يوفر التدقيق الداخلي الرؤى والمعلومات التي تحتاجها شركاتهم لتحسين احتمالات نجاح الأمن السيبراني.

وفقا لمسح لصناع القرار في مجال تكنولوجيا المعلومات وعمليات الأمن:

- يقول 2٪ فقط من المستجيبين إنهم يستطيعون استعادة بياناتهم واستعادة العمليات التجارية في غضون 24 ساعة من الهجوم الإلكتروني.
- يقول 69٪ إن مؤسساتهم دفعت فدية في العام الماضي ، على الرغم من أن 77٪ يقولون إن لديهم سياسة أو بروتوكولا محددا ضد دفع الفدية.
- يقول 42٪ إن مؤسساتهم يمكنها تحديد البيانات الحساسة والامتثال لقوانين ولوائح خصوصية البيانات المعمول بها. لا يمتلك البعض الآخر قدرات كافية في مجال تكنولوجيا المعلومات والأمان للقيام بالأمرين معا.

المصدر: تقرير المرونة السيبرانية العالمية للتماسك لعام 2024

الجزء 3

إنشاء حدود جديدة لانعدام الثقة (صفر ثقة)

نبذة عن الخبراء

آدم كونكي

آدم كونكي ، ومقره في ماديسون ، ويسكونسن ، هو مدير أمن المعلومات في شركة التصنيع الكيميائي Charter Next Generation.

خوليو تيرادو

خوليو تيرادو هو نائب الرئيس التنفيذي ومدير التدقيق الداخلي والامتثال في SpiritBank ومقرها تولسا ، أوكلاهوما.

يجب أن يكون المطلب الأساسي لكل مؤسسة أن يكون لديها عمليات وضوابط للحفاظ على أمان شبكاتها. ومع ذلك، فإن تقدم التكنولوجيا ونمو الشبكات بشكل أكبر ومعقد بشكل لا يسير غوره تقريبا، تغير معيار ما يشكل شبكة آمنة. يكمن أحد أهم التغييرات في الانتقال من نموذج أمان يركز على الموقع إلى نموذج أكثر تركيزا على البيانات. نسمي هذا النموذج "انعدام الثقة".

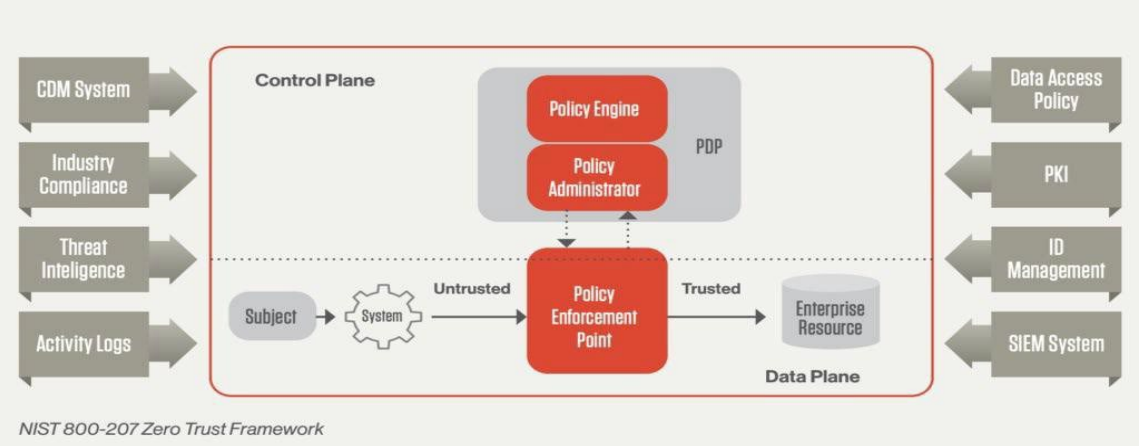
ما هو نظام انعدام الثقة؟

بشكل عام، يتطلب إطار عمل أمان انعدام الثقة مصادقة جميع المستخدمين الذين يعملون داخل الشبكة - داخل المؤسسة وخارجها - قبل الوصول إلى التطبيقات والبيانات، ثم التحقق من صحتهم بانتظام باستمرار. كما يوحي الاسم، فإن "الثقة" ، أو بشكل أكثر تحديدا "ثق ولكن تحقق"، لا تلعب أي دور في هذا النظام ويجب تبرير الوصول إلى أي شيء متعلق بالمؤسسة وتقييمه باستمرار بناء على سياسات المؤسسة.

تقليديا، تم بناء النماذج السيبرانية بالنظر لموقع الشبكة، ولكن في نظام انعدام الثقة، فإن ما يشكل "شبكة" أقل تحديدا، حيث يمكن أن تكون الشبكة التنظيمية محلية أو قائمة على سحابة أو هجينة من الاثنين. خاصة بعد جائحة COVID-19، الذي بشر بعصر جديد من العمل عن بعد، أصبحت الأنظمة الهجينة أو المستندة إلى السحابة بالكامل هي القاعدة، وكان على أطر الأمن السيبراني أن تتطور ايضا.

هناك العديد من أطر انعدام الثقة الرسمية الموجودة، بما في ذلك:

- المعيار 800-207 من المعهد الوطني للمعايير والتكنولوجيا (NIST). هذا هو الإطار الذي تم تفويضه للاستخدام من قبل الوكالات الفيدرالية الأمريكية منذ عام 2021 (انظر الشكل 1).
- Google BeyondCorp
- استراتيجية Microsoft Zero Trust
- نموذج نضج الثقة المعدومة Zero Trust Maturity Model من وكالة الأمن السيبراني وأمن البنية التحتية (CISA).



الشكل 1

المصدر: شبكات الثقة المعدومة | NIST

في حين أن جميعهم لديهم سماتهم الفريدة، إلا أنهم يشتركون في نفس المبادئ الأساسية، وهي:

- تحقق باستمرار من الوصول عبر جميع الموارد.
- تقليل منطقة التأثير في حالة حدوث خرق خارجي أو داخلي.
- استخدم البيانات السلوكية لجمع السياق من البنية الأساسية لتكنولوجيا المعلومات.

وفي حين أن الانتقال إلى مثل هذا النظام قد يبدو كبيرا، فمن المهم ملاحظة أنه لا يقصد به أن يكون بديلا عن النظم الحالية. يقول آدم كونكي، مدير أمن المعلومات في شركة التصنيع الكيميائي Charter Next Generation: "لا تسعى الثقة المعدومة إلى استبدال نماذج حماية الشبكة الحالية بالكامل أو حتى تغييرات البنية التحتية، بل إلى زيادتها لتعزيز حماية الشبكة. من المفترض أن يكون امتدادا لأن الأنظمة التقليدية مثل جدران الحماية ووكلاء الويب وآليات عزل الحدود لم تكن تعمل ".

وفقا لشركة IBM، بلغ متوسط تكلفة خرق البيانات الفردي في عام 2024 4.88 مليون دولار. بالإضافة إلى ذلك، كان متوسط دورة حياة الخرق 292 يوما كاملة من تحديد الهوية إلى الاحتواء. من الواضح أن الحماية التقليدية للشبكة لم تكن كافية وتتطلب اهتماما كبيرا.

دور التدقيق الداخلي

في حين أن التفاصيل يمكن أن تختلف، يمكن أن يكون لدى المدققين الداخليين مجموعة متنوعة من المسؤوليات المرتبطة بتنفيذ وصيانة نظام انعدام الثقة. للتوضيح، فيما يلي المجالات التي قد يكون لتقييم التدقيق الداخلي أكبر قيمة.

تحديد الأسطح المحمية

تقليديا، ركز نظام الأمن السيبراني جهوده على تحديد معايير الأمان حول شبكة المؤسسة. تم تصميم جدران الحماية وأنظمة VPN حول هذا المفهوم، مما يحافظ على البيانات الحساسة والمعلومات المعرضة للخطر بعيدة قدر الإمكان من محيط الشبكة.

> وينبغي أن يركز التقييم على فحص سياسات تصنيف البيانات الخاصة بالمؤسسة لتحديد ما إذا كانت الأنظمة والبيانات مصنفة بشكل مناسب، وما إذا كانت سياسات الحماية المعمول بها لكل منها مناسبة.
>
> **- خوليو تيرادو ، سبيريت بانك**

ولكن في نظام انعدام الثقة، وبدلا من العوامل المتغيرة (parameters) ، ينصب التركيز على مجموعات البيانات والتطبيقات والأصول والخدمات (DAAS)، والمعروفة مجتمعة باسم "حماية الأسطح".

يجب أن يكون ضمان تحديد هذه الأسطح بشكل مناسب أمرا أساسيا لتقييم التدقيق الداخلي الشامل.

وفقا لخوليو تيرادو، نائب الرئيس التنفيذي ومدير التدقيق الداخلي والامتثال في SpiritBank، "يجب أن يركز التقييم على فحص سياسات تصنيف البيانات الخاصة بالمؤسسة لتحديد ما إذا كانت الأنظمة والبيانات مصنفة بشكل مناسب، وما إذا كانت سياسات الحماية المعمول بها لكل منها مناسبة".

يقول تيرادو إن الخدمات المحمية لا تقتصر فقط على البيانات. يجب أيضا أن يكون للأصول المادية التي لها دور في الوصول إلى البيانات الحساسة عمليات وإجراءات لضمان جردها وتقييمها بشكل دوري.

التحقق من تدفقات حركات الخريطة

بمجرد التأكد من تحديد أسطح الحماية، فإن الخطوة التالية في عملية التقييم هي التأكد من وجود فهم لأصحاب المصلحة لكيفية تفاعل جميع أنظمة DAAS هذه مع بعضها البعض. يجب أن يكون لدى فرق تكنولوجيا المعلومات مخططات توثيق مفصلة مخصصة لرسم خريطة الشبكة المعقدة للمنافذ وخطوط الأساس لحركة مرور الشبكة والبروتوكولات التي تحدد بشكل جماعي كيفية وصول هذه الأنظمة إلى بعضها البعض وإلى أين يمكن أن يؤدي استخدامها.

على الرغم من أن وظيفة التدقيق الداخلي في معظم المؤسسات قد لا يكون لديها المعرفة أو الخبرة الكافية للتحقق من دقة هذه المخططات بمفردها، إلا أن كونكي يقول إن التدقيق الداخلي يمكن أن يعمل مع أصحاب المصلحة أو طرف ثالث موثوق به للتحقق من إجراء اختبارات التحقق للتأكد من أن ما تم تصويره كاف. يقول: "المهم هو أن DAAS ذات الصلة يتم أخذها في الاعتبار في كل رسم تخطيطي وإذا كانت هناك تفاصيل كافية وما إذا كانت سياسات الأمان الأولية المحددة في الخطوات السابقة قد تم تعديلها أو تتطلب ضوابط إضافية."

التحقق من إنشاء سياسات انعدام الثقة والتحسين المستمر لها

يجب أن تكون سياسات انعدام الثقة مفصلة لكل سطح وقائي ويجب أن تجيب على أسئلة مهمة مثل:

- من الذي يجب السماح له بالوصول إلى أنظمة DAAS للمؤسسة؟
- ما هي التطبيقات التي سيسمح لها بالوصول إلى أنظمة DAAS للمؤسسات؟
- متى يجب أن يحدث الوصول إلى أنظمة DAAS للمؤسسات أو يحدث؟
- أين توجد أنظمة DAAS للمؤسسات؟
- لماذا يجب الوصول إلى أنظمة DAAS للمؤسسة؟
- كيف ينبغي منح الوصول إلى أنظمة DAAS للمؤسسات؟

لتقييم أهمية وصلاحية سياسات انعدام الثقة التي تم إنشاؤها، يعد التفاعل المستمر مع أصحاب المصلحة في تكنولوجيا المعلومات أمرا بالغ الأهمية مع استمرار شبكة المؤسسة في التوسع والتطور. يقول تيرادو: "الثقة المعدومة ليست وجهة، بل عملية مستمرة، لذا يجب أن تتطور سياسة الأمان ومتطلبات حماية DAAS مع تطور العملية".

يقول تيرادو إن الهدف يجب أن يكون الحصول على سياسة تتحسن باستمرار مكرسة لمعالجة كل نوع من أنواع حركة المرور التي يمكن أن تدخل الشبكة وتخرج منها وتتجاوزها. يقول: "لا ينبغي أن يكون هناك أي شيء داخل الشبكة حيث لا يمكن تحديد المصدر أو الغرض". "يحتاج المدقق الداخلي في تقييمه إلى تحديد ما إذا كانت المراجعات قد أجريت، وما إذا كانت قد أجريت إلى حد كاف، وما إذا كانت السياسات المعمول بها تتناول بدقة ما يجده."

مراقبة بنية انعدام الثقة

> يجب إجراء المراقبة على شبكاتك لقياس الأداء وتحديد جميع الأجهزة المتصلة بشبكتك واكتشاف الأجهزة المارقة والأنشطة الضارة.
>
> **— المركز الوطني للأمن السيبراني**

وكما تشير الأمثلة السابقة، فإن الرصد المستمر أمر بالغ الأهمية لنجاح إطار انعدام الثقة. على عكس النظام التقليدي، حيث تركز المراقبة على معايير الأمان، فإن أنظمة المراقبة لنظام انعدام الثقة ستتمحور حول المستخدمين والأجهزة والخدمات. "يجب إجراء المراقبة على شبكاتك لقياس الأداء، وتحديد جميع الأجهزة المتصلة بشبكتك، واكتشاف الأجهزة المارقة والنشاط الضار"، كما يقول المركز الوطني للأمن السيبراني في إرشادات انعدام الثقة. هذا صحيح بشكل خاص إذا كنت تستضيف خدمات محلية، ولكن نظرا لأنه أصبح أكثر شيوعا، يجب مراعاة إدارة الأجهزة المحمولة بنفس القدر.

يقول تيرادو: "ستنشر شركات مثل شركتي برامج إدارة الأجهزة المحمولة التي ستوفر قدرا للتحكم في هذا الجهاز المعين، طالما أن المستخدم يقبله". "سوف يراقب النشاط، ويساعد في تقييد المواقع الخطرة، وتقييد بعض البرامج التي يمكن تثبيتها على الجهاز، ويوفر التحكم في نشر التحديثات على هذا النظام المعين"

بالإضافة إلى ذلك، يجب أن يشمل الرصد ليس فقط الاستخدام الفعلي للأنظمة، ولكن أيضا مدة استخدامها. كما ذكر المركز الوطني للأمن السيبراني، "سلوك المستخدم، مثل ساعات العمل العادية أو موقع العمل العادي، هو مقياس مهم يجب مراقبته".

هناك العديد من أنظمة المراقبة المتاحة المصممة لتلبية الاحتياجات المحددة للشبكة المعنية، ولكن بشكل عام، ستنقل هذه الأنظمة البيانات التي تم جمعها إلى موقع مركزي حيث يمكن تحليلها بعد ذلك.

بمرور الوقت، سيتم إنشاء "خط أساس" لما يشكل سلوكا طبيعيا فيما يتعلق بالمتغيرات مثل حجم المعاملات، واتصالات الأصول، ونشاط المستخدم.

ويمكن للمراجعين الداخليين، من خلال تقييماتهم، أن يكفلوا إجراء مراجعات منتظمة لهذه البيانات - وأن الإدارة تتولى الملكية المناسبة لهذه المهمة - وأن النتائج التي توصلوا إليها تخلق خط أساس يعكس بدقة واقع الشبكة.

يقول تيرادو: "بالنسبة للمدققين الداخليين، فإن الامر يعتمد في الكثير منه إلى الحوكمة". "يجب إبلاغ الإدارة بالدور الذي تلعبه في تأمين النظام، لأن النظام لن يقف طويلا بمفرده. يتم تحديد التغييرات في سياسات الأمان من خلال ما يحدده خط الأساس على أنه "عادي" و "غير طبيعي". تضع مراجعات الإدارة خط الأساس ".

إنشاء خط أساس

مثل العديد من عناصر الأمن السيبراني، أو إدارة المخاطر، لا يوجد نموذج "مقاس واحد يناسب الجميع"، وعلى هذا النحو، فإن كيفية مساهمة وظيفة التدقيق الداخلي في ذلك ستختلف اختلافا كبيرا. يقول تيرادو: "هذا يعتمد على الموارد". "يعتمد ذلك على حجم المؤسسة. يعتمد ذلك على تفويض فريق التدقيق الداخلي ".

ويقول إن المكان الجيد لإنشاء خط أساس هو رسم عملية لتوفير التأكيد لا تختلف عن أي نظام تدقيق آخر. يقدم: "على سبيل المثال، فكر في Sarbanes-Oxley". "يجب على كل شركة عامة رسم الضوابط الداخلية المتعلقة بالبيانات المالية، وتطوير هذه المصفوفة. وكجزء من هذا الرسم، ستقوم بإنشاء إجراءات اختبار خلال فترة معينة - مثل سنة معينة. ستتبع نفس النهج مع انعدام الثقة، وتقسيم التأكيد إلى قطع على مدار العام، مع مراعاة حجم الشركة والموارد وما إلى ذلك.

ومع ذلك، فإن الخط المشترك بين جميع الحالات هو التزام التدقيق الداخلي بدعم التنفيذ والتحسين المستمر لنظام انعدام الثقة. هناك مجموعة متنوعة من الموارد في السوق التي تساعد في هذه المهمة، بناء على العنصر الذي يركز عليه نموذج انعدام الثقة. على سبيل المثال، فيما يتعلق بمخاطر برامج الفدية، يستخدم Tirado InfraGard ، وهي أداة مجانية لمشاركة المعلومات تم تطويرها من خلال شراكة مع مكتب التحقيقات الفيدرالي وأعضاء القطاع الخاص. في بضع دقائق فقط في بداية كل يوم، يمكن ل Tirado استخدام الأداة للاطلاع على أحدث هجمات برامج الفدية وخروقات البيانات داخل وخارج صناعته. ويشرح قائلا: "إن حجم هذه الهجمات يستدعي نهجا يتجاوز نموذج الأمان القائم على المحيط". "إن إبقاء أصحاب المصلحة على اطلاع بما تبدو عليه بيئة المخاطر وما هو على المحك هو الأولوية الأولى للتدقيق الداخلي."

بالإضافة إلى ذلك، من المهم ملاحظة أن هذا ليس انتقالا يجب أن يحدث دفعة واحدة. يقول تيرادو: "حتى في الشكل الجزئي، فإن نموذج انعدام الثقة له قيمة هائلة". "في نهاية المطاف، يتلخص نموذج انعدام الثقة في جدول بيانات من عناصر التحكم. ربما يكون مكونا من 20 عمودا، وربما 10 أو 12 فقط. حسنا، هذا أفضل من خمسة ".

تتضمن أمثلة الضوابط البسيطة التي يجب مراعاتها في المراحل الأولى من نموذج انعدام الثقة ما يلي:

- تشفير البيانات.
- التدريب على التوعية الأمنية.
- خطط الاستجابة للحوادث.
- أنظمة الكشف عن نقاط النهاية والاستجابة.
- التجزئة Mico-segmentation
- رصد الامتثال
- التحليل السلوكي و تحليلات سلوك كيان المستخدم

الأساس موجود بالفعل

على الرغم من التغيير الأساسي في الشبكة، يجب على المدققين الداخليين أن يدركوا أنه بمجرد فهم انعدام الثقة، يجب ألا تختلف مسؤوليات الوظيفة نفسها تماما عما كان متوقعا منهم من قبل. لا يتطلب تنفيذ انعدام الثقة في حد ذاته أي تغييرات في البنية التحتية خارج إمكانية اعتماد أدوات تجارية معينة، لذلك لا تتطلب الأنظمة التي توفر ضمانا لها أي تغيير.

في الواقع، تشمل المبادئ الرئيسية لأي عمل تدقيق تحديد الهوية والتواصل والتأكيد، وتظل كل من هذه المسؤوليات على حالها. مع التصميم الثابت، والالتزام بالمعايير العالمية للتدقيق الداخلي™، والاستعداد للتعلم، فإن الانتقال إلى بنية شبكة انعدام الثقة ليس شيئا يجب أن تخشاه المؤسسة.

الإصدارات السابقة

للوصول إلى الإصدارات السابقة من وجهات النظر والرؤى العالمية ، قم بزيارة theiia.org/GPI.

ملاحظات القارئ

أرسل أسئلة أو تعليقات إلى globalperspectives@theiia.org.

نبذة عن المعهد الدولي للمدققين الداخليين IIA

المعهد الدولي للمدققين الداخليين IIA هو جمعية مهنية دولية غير لا تبغي الربح تخدم أكثر من 235 ألف عضو عالمي وقد منحت أكثر من 190,000 شهادة مدقق داخلي معتمد CIA في جميع أنحاء العالم. تأسس المعهد الدولي للمدققين الداخليين IIA في عام 1941 وهو معترف به في جميع أنحاء العالم باعتباره الرائد في مهنة التدقيق الداخلي في المعايير، الشهادات، التعليم، البحث، والارشاد التقني. لمزيد من المعلومات، قم بزيارة **theiia.org**

اخلاء المسؤوليه

ينشر المعهد الدولي للمدققين الداخليين IIA هذه الوثيقة لأغراض إعلامية وتعليمية. لا تهدف هذه المواد إلى تقديم إجابات نهائية لظروف فردية محددة وعلى هذا النحو يُقصد منها فقط استخدامها كقيادة فكرية مستنيرة من الأقران. إنها ليست توجيهات رسمية من المعهد الدولي للمدققين الداخليين (IIA). يوصي المعهد الدولي للمدققين الداخليين بالتماس مشورة الخبراء المستقلين فيما يتعلق مباشرة بأي حالة محددة. لا يتحمل المعهد الدولي للمدققين الداخليين IIA أي مسؤولية عن أي شخص يعتمد فقط على هذه المواد.

حقوق النشر

يناير 2025

قام بترجمة هذه الوثيقة الى اللغة العربية فريق عمل من جمعية المدققين الداخليين في لبنان برئاسة عضو مجلس الحكام الأستاذ ناجي فياض

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101