IDB.52/33

Distr.: General
20 September 2024
Arabic
Original: English

منظمة الأمم المتحدة للتنمية الصناعية

مجلس التنمية الصناعية

الدورة الثانية والخمسون

فيينا، 25-27 تشرين الثاني/نوفمبر 2024

البند 4 (و) من جدول الأعمال المؤقَّت

الإدارة العامة للمخاطر

تحديث بشأن الإدارة العامة للمخاطر

تقرير من المدير العام

دعت لجنة البرنامج والميزانية، في استنتاجها 8/2016، "المدير العام إلى أن يُقدِّم إلى مجلس التنمية الصناعية ولجنة البرنامج والميزانية في دورتيهما المقبلتين تقريرا عن استراتيجية اليونيدو العامة لإدارة المخاطر وأن يقترح تدابير شاملة لمعالجة الأثر المالي والإداري الناجم عن مغادرة دول أعضاء للمنظمة، وكذلك من أجل عكس اتجاه الانسحاب".

وتُقدِّم هذه الوثيقة تحديثاً للتقرير الذي قُدِّم في الدورة الأربعين للجنة (IDB.52/9-PBC.40/9)، وتسلِّط الضوء على إنشاء وحدة جديدة مكرَّسة لإدارة المخاطر والامتثال، في إطار مديرية الخدمات والعمليات المؤسسية، بما في ذلك المهام الإضافية المتعلقة بالأمن السيبراني.

أولا- مقدمة

1- موازاة مع صدور هيكل أمانة اليونيدو المعدل لعام 2024 (DGB/2024/03)، أنشأت اليونيدو وحدة إدارة المخاطر والامتثال. وتدعم هذه الوحدة الجديدة المدير الإداري لمديرية الخدمات والعمليات المؤسسية، بصفتها جهة التنسيق المعيّنة لإدارة المخاطر المؤسسية في اليونيدو، من أجل مواصلة تطوير وتنسيق وتنفيذ إطاري اليونيدو لإدارة المخاطر المؤسسية ومخاطر أمن المعلومات. كما أنها تدعم بنشاط الإدارة العليا من أجل تعزيز ثقافة قوية متعلقة بالمخاطر. وبالإضافة إلى مهمتي إدارة المخاطر والامتثال، تتعلق مهام الوحدة بحوكمة الأمن السيبراني.

2- وتسلط هذه الوثيقة الضوء على الإجراءات التي اتخذتها اليونيدو لإدارة المخاطر المتعلقة بالأمن السيبراني والحد منها.

لأغراض الاستدامة، لم تُطبع هذه الوثيقة. ويرجى من أعضاء الوفود التكرم بالرجوع إلى الصيغ الإلكترونية لجميع الوثائق.

الرجاء إعادة استعمال الورق

041024 041024 V.24-17133 (A)

ثانيا- إطار عمل الأمن السيبراني وتحسيناته

3- استجابةً لتوصية وحدة التفتيش المشتركة الواردة في تقريرها المعنون "الأمن السيبراني في مؤسسات منظومة الأمم المتحدة" (JIU/REP/2021/3)، تقدم اليونيدو لمحة شاملة عن التدابير المنفذة المتعلقة بإطار الأمن السيبراني لديها. وتوجز هذه اللمحة العامة، الواردة في ورقة الاجتماع IDB.52/CRP.14، العناصر الحاسمة والإجراءات المتخذة لحماية المنظمة من التهديدات السيبرانية وضمان تنفيذ ممارسات أمنية قوية.

4- وقد أحرزت اليونيدو تقدماً كبيراً في تعزيز إطارها الخاص بالأمن السيبراني، حيث وَاءمَته مع توصيات مراجع الحسابات الخارجي ووحدة التفتيش المشتركة وأفضل الممارسات المعتمدة في هذا المجال. فقد أرست المنظمة أساساً متيناً للأمن السيبراني من خلال تحديد إطار الحوكمة وإنشاء نظام إدارة أمن المعلومات (المتوافق مع معيار المنظمة الدولية لتوحيد المقاييس 27001 (ISO 27001)) من خلال سياسة اليونيدو لأمن المعلومات (DGB/2023/01)، وكذلك الأمر الإداري المتعلق بعملية إدارة مخاطر أمن المعلومات (AI/2024/01)، الذي يصف العملية التي ترمي إلى ضمان استبانة مخاطر أمن المعلومات وتقييمها وإدارتها والتخفيف من حدتها بطريقة فعالة ومنظمة ومناسبة من حيث التوقيت.

5- ومع مضي اليونيدو قدما في هذه المسألة، من الأهمية بمكان الحفاظ على نهج استباقي إزاء الأمن السيبراني. ويشمل ذلك إعادة تقييم المخاطر باستمرار، وتعزيز القدرات التقنية وتعزيز ثقافة الوعي بالأمن السيبراني في جميع أقسام المنظمة. ومن خلال هذه الجهود، لن تكون اليونيدو مجهزة فحسب لمواجهة التهديدات السيبرانية المتطورة وحماية أصولها المعلوماتية، بل إنها ستتمكن أيضا من دعم مهمتها الأوسع نطاقاً بمرونة وثقة.

6- وفي تقرير مراجع الحسابات الخارجي عن حسابات اليونيدو للسنة المالية من 1 كانون الثاني/يناير إلى 31 كانون الأول/ديسمبر 2023 (IDB.52/4-PBC.40/4)، الذي قُدِّم في الدورة الأربعين للجنة البرنامج والميزانية، أقرَّ مراجع الحسابات الخارجي بالتقدم الذي أحرزته اليونيدو في مجال الأمن السيبراني من خلال إقفال كافة التوصيات الخمس، التي ركَّزت على إنشاء وظيفة مكرَّسة للأمن السيبراني، وتطوير نظام إدارة أمن المعلومات، وتنفيذ عملية إدارة مواطن الضعف. كما تمت معالجة وتصحيح نقاط الضعف التقنية الحرجة التي استبانها مراجع الحسابات الخارجي. وقد كشف اختبار للاختراق الأمني أجري في عام 2023 وقادته اليونيدو بدعم من شركات خارجية متخصصة عن مشاكل إضافية أدرجت في خطة عمل خدمات الرقمنة والابتكار وتحسين التعاون التقني. كما حدد تقييم لمخاطر أمن المعلومات أجري في عام 2023 الأصول والمخاطر الرئيسية، مما أدى إلى وضع خطة شاملة لمعالجة مخاطر أمن المعلومات للفترة 2023-2024، وهي تتضمن 35 نشاطاً، تم الانتهاء من 15 نشاطاً منها وما زال العمل جارياً على الأنشطة المتبقية منها. وترد لمحة عامة عالية المستوى عن هذه الأنشطة في مرفق هذه الوثيقة. وتؤكد النتائج على فعالية وظيفة الأمن السيبراني في اليونيدو في استبانة المخاطر وإدارتها على نحو استباقي، فضلاً عن تعزيز أمن المنظمة وقدرتها على الصمود.

7- وتُستكمل هذه الوثيقة بورقة الاجتماع IDB.52/CRP.14، التي تصف العمليات التي تسهم في تحسين قدرة المنظمة على الصمود في المجال السيبراني.

ثالثا- الإجراء المطلوب من المجلس اتخاذه

8- لعل المجلس يود أن يحيط علماً بالمعلومات الواردة في هذه الوثيقة.

المرفق

حالة الأنشطة المدرجة في خطة معالجة مخاطر أمن المعلومات للفترة 2023-2024

الأنشطة المنجزة

1- اختبار الاختراق: التعاقد مع متعاقد خارجي بهدف إجراء اختبار شـــامل للاختراق من أجل محاكاة مهاجم لديه إمكانيات الوصـــول من الداخل. وقد أدى ذلك إلى تنقيح الضـــوابط وإدراج أنشـــطة جديدة في خطة معالجة المخاطر.

2- تنفيذ التوثيق الحديث لخادوم "Exchange Online": تنفيذ التوثيق الحديث لـــخادوم Exchange Online من أجل تعزيز أمن البريد الإلكتروني.

3- إيقاف تشـــغيل نظام مشـــاركة الملفات xFiles: تم بنجاح وقف تشـــغيل نظام اليونيدو القديم لمشـــاركة الملفات وتنفيذ حل حديث لمشاركتها استنادا إلى Microsoft 365 (OneDrive)، مما قلص مساحة الهجوم.

4- تحسين توثيق Microsoft Teams: تنفيذ التوثيق المتعدد العوامل لـــتطبيق Teams من أجل التخفيف من مخاطر سرقة إثباتات الهوية.

5- تحسين السياسات الخاصة بكلمات السر: تطوير الإجراءات وتطبيق إجراءات جديدة بشأن سياسات شاملة خاصة بكلمات السر ومراقبة التزويد والامتثال المتعلقين بها.

6- تحســـين التوثيق وتجربة المســـتخدم والأمن: الانتقال إلى الدخول بتوقيع واحد (SSO) اســـتناداً إلى Microsoft 365 Azure AD، مما يعزز المراقبة والمرونة والتوافر.

7- تنفيذ التوثيق المتعدد العوامل بالنسـبة للنظم السـحابية: إتاحة إمكانية التوثيق المتعدد العوامل بالنسـبة لجميع الخدمات التي تستخدم التوثيق السحابي لتعزيز الأمن.

8- أداة وعملية إدارة مواطن الضعف: تنفيذ أداة لإدارة مواطن الضعف تغطي الموارد الحساسة مثل النظم المعدة لاســتخدام الجمهور والخواديم الحســاســة ومحطات عمل مديري هذه النظم (administrators). كما تم تطوير عملية وإجراءات إضافية، بما يتماشى مع توصيات مراجع الحسابات الخارجي والممارسات الفضلى.

9- تعزيز مراقبة الامتثال: تحسـين مراقبة الامتثال لضـوابط الأمن السـيبراني الرئيسـية، بما يتماشـى مع المعيار الأدنى الأساسي لدى الأمم المتحدة والممارسات الفضلى لدى مايكروسوفت.

10- تحســـين أمن نظم Microsoft 365: تنفيذ الدخول الســـلس بتوقيع واحد بالنســـبة لنظم Microsoft 365 المختارة، مما أدى إلى تحسين تجربة المستخدم والأمن.

11- التدريب الداخلي المخصـص لمسـؤولي تكنولوجيا المعلومات: أجري تدريب داخلي شـامل لمسـؤولي تكنولوجيا المعلومات وقدمت دورات متخصصة للمستخدمين الامتيازيين.

12- اســتعراض تخزين الملفات لدى المكاتب الميدانية: اســتكمل اســتعراض للأذونات وتقييم نقل الملفات المشارَكة لدى المكاتب الميدانية إلى نظام Teams من أجل تحسين الأمن.

13- تحســين العمليات والســياســات الأمنية: تعزيز العمليات والســياســات المتعلقة بحقوق الوصـــول، والفصل بين الواجبات والتشكيلات الآمنة، والحد من حالات الخروج عن الممارسات المعيارية.

14- تحسين عمليات أمن المعلومات: اعتماد وتكييف أفضل الممارسات الحالية في مجال أمن المعلومات بغية تحسين الوضع الأمني للمنظمة.

15- استعراض أمن تطبيق Teams: إجراء استعراض لإعدادات الأمن والأذونات داخل Teams.

الأنشطة قيد التنفيذ

16- استعراض الحسابات على أساس مبدأ الحاجة إلى المعرفة وأدنى امتياز: الاستعراض المتواصل للحسابات الامتيازية وحسابات الخدمة، وحقوق الوصول إلى مشاركة الملفات وتنفيذ تدابير مثل حل كلمة السر الخاصة بمديري النظم المحليين.

17- تطبيق خاصية حماية إثباتات الهوية: يجري حالياً تطبيق خاصية حماية إثباتات الهوية على كل من الخواديم والمحطات الطرفية بغية تعزيز الأمن وتقليص مخاطر اختراق الإثباتات.

18- تنفيذ أحدث السياسات الخاصة بكلمات السر في جميع أقسام اليونيدو: تحديث السياسات الخاصة بكلمات السر والوصول الامتيازي استناداً إلى إجراءات السياسة المحدثة الخاصة بكلمات السر.

19- التحسينات الخاصة بإدارة التصحيحات: تهدف الجهود الجارية إلى تحسين إدارة التصحيحات وعمليات إصلاح الأعطال.

20- تحسين أمن نظام SAP: يجري تنفيذ تدابير للتعامل مع نتائج المراجعة وتحسين الصحة الأمنية داخل نظام SAP.

21- التحسينات الخاصة بجدار الحماية: التحسينات جارية بما في ذلك تنفيذ نهج انعدام الثقة وكذلك الشأن بالنسبة للاستعراض الكامل لهيكل جدار الحماية (firewall) وإدارته والسياسات الأمنية المتعلقة به.

22- استبدال أداة إدارة كلمات السر الخاصة بمديري نظم تكنولوجيا المعلومات: يجري استبدال أداة إدارة كلمات السر القديمة الخاصة بمديري نظم تكنولوجيا المعلومات.

23- تقييم نضج نهج انعدام الثقة: يجري تقييم شامل لنضج نهج انعدام الثقة بغية توجيه التحسينات المستقبلية.

24- إيقاف تشغيل النظم القديمة واستبدالها: الجهود جارية من أجل إيقاف تشغيل واستبدال النظم القديمة بغية تقليص مساحة الهجوم.

25- تحسين التعامل مع الحوادث الأمنية: يجري العمل على تعزيز عمليات وأدوات التعامل مع الحوادث باستخدام الموارد الداخلية والخارجية على حد سواء.

26- رصد الضوابط الرئيسية لنظام SAP: يجري العمل على رصد الامتثال للضوابط الرئيسية في إطار نظام SAP والعمليات الداعمة له، بما يتماشى مع توصيات مراجع الحسابات الخارجي.

27- الفصل بين الواجبات في إطار تكنولوجيا المعلومات الخاصة بنظام تخطيط الموارد المؤسسية: يجري العمل على تعزيز الفصل بين الواجبات في إطار تكنولوجيا المعلومات الخاصة بنظام SAP حسب ما تسمح به الموارد وبما يتماشى مع توصيات مراجع الحسابات الخارجي.

28- حسابات مخصصة لمديري النظم: يجري العمل على تنفيذ حسابات مخصصة ومنفصلة لمديري نظم تكنولوجيا المعلومات في مختلف النظم.

29- التوثيق التجريبي دون استخدام كلمة سر: يجري حالياً تقييم وتجربة طرائق توثيق مبتكرة دون استخدام كلمة سر من أجل تعزيز الأمن مع تبسيط الوصول في الوقت نفسه.

30- الاستعراض الخاص بموردي الإنترنت في المكاتب الميدانية: يتواصل استعراض نوعية خدمات الإنترنت في المكاتب الميدانية وعرض النطاق الترددي الخاص بها.

31- تعزيز التعاون مع الشركاء الخارجيين: يجري حالياً استكشاف فرص التعاون مع الشركاء الخارجيين من أجل تلبية الاحتياجات المعرفية والأمنية المتخصصة.

32- تطوير خارطة طريق خاصة بنهج انعدام الثقة: يجري العمل حالياً على وضع خارطة طريق خاصة بنهج انعدام الثقة بما يتماشى مع أولويات العمل وبيانات المخاطر.

33- التوثيق المتعدد العوامل لجميع الخدمات المتاحة للجمهور: يجري العمل على تنفيذ التوثيق المتعدد العوامل لجميع حالات الوصول الخارجي الامتيازي.

34- تحسين إدارة الأصول واكتشافها: يجري حالياً بذل جهود لتحسين إدارة الأصول وأدوات الاكتشاف، بما في ذلك توسيع نطاق جرد الخواديم وتحسين نشر التصحيحات.

35- النظر في إنشاء موقع للتعافي من الكوارث: يجري التخطيط لموقع ثانوي للتعافي من الكوارث والنسخ الاحتياطي للبيانات بغية ضمان استمرارية العمل.