الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

X.1333
(2022/01)

ITU-T
قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

السلسلة X: شبكات البيانات والاتصالات
بين الأنظمة المفتوحة ومسائل الأمن

التطبيقات والخدمات الآمنة (2) – أمن شبكة الكهرباء الذكية

المبادئ التوجيهية الأمنية لاستعمال أدوات النفاذ عن بُعد في أنظمة التحكم الموصولة بالإنترنت

التوصية ITU-T X.1333

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.1-X.199
التوصيل البيني للأنظمة المفتوحة	X.200-X.299
التشغيل البيني للشبكات	X.300-X.399
أنظمة معالجة الرسائل	X.400-X.499
الدليل	X.500-X.599
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.600-X.699
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.600-X.699
الأمن	X.800-X.849
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.850-X.899
المعالجة الموزعة المفتوحة	X.900-X.999
آمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1000-X.1029
آمن الشبكة	X.1030-X.1049
إدارة الأمن	X.1050-X.1069
الخصائص البيومترية	X.1080-X.1099
تطبيقات وخدمات آمنة (1)	
آمن البث المتعدد	X.1100-X.1109
آمن الشبكة المحلية	X.1110-X.1119
آمن الخدمات المتنقلة	X.1120-X.1139
آمن الويب (1)	X.1140-X.1149
بروتوكولات الأمن (1)	X.1150-X.1159
الأمن بين جهتين نظيرتين	X.1160-X.1169
آمن معرفات الهوية عبر الشبكات	X.1170-X.1179
آمن التلفزيون القائم على بروتوكول الإنترنت	X.1180-X.1199
آمن الفضاء السيبراني	
الأمن السيبراني	X.1200-X.1229
مكافحة الرسائل الاقتحامية	X.1230-X.1249
إدارة الهوية	X.1250-X.1279
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1300-X.1309
آمن شبكات المحاسيس واسعة الانتشار	X.1310-X.1319
آمن شبكة الكهرباء الذكية	**X.1330-X.1339**
البريد المعتمد	X.1340-X.1349
آمن إنترنت الأشياء (IoT)	X.1350-X.1369
آمن أنظمة النقل الذكية (ITS)	X.1370-X.1399
آمن سجل الحسابات الموزع (DLT)	X.1400-X.1429
آمن التطبيقات (2)	X.1450-X.1459
آمن شبكة الويب (2)	X.1470-X.1489
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1500-X.1519
تبادل مواطن الضعف/الحالة	X.1520-X.1539
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1540-X.1549
تبادل السياسات	X.1550-X.1559
طلب المعلومات الحدسية والمعلومات الأخرى	X.1560-X.1569
تعرف الهوية والاكتشاف	X.1570-X.1579
التبادل المضمون	X.1580-X.1589
الدفاع السيبراني	X.1590-X.1599
آمن الحوسبة السحابية	
نظرة عامة على آمن الحوسبة السحابية	X.1600-X.1601
تصميم آمن الحوسبة السحابية	X.1602-X.1639
أفضل الممارسات ومبادئ توجيهية بشأن آمن الحوسبة السحابية	X.1640-X.1659
تنفيذ آمن الحوسبة السحابية	X.1660-X.1679
آمن أشكال أخرى للحوسبة السحابية	X.1680-X.1699
الاتصالات الكمومية	
المصطلحات	X.1701–X.1700
مولد الأعداد العشوائية الكمومية	X.1709–X.1702
إطار آمن شبكات توزيع المفاتيح الكمومية	X.1711–X.1710
تصميم آمن شبكات توزيع المفاتيح الكمومية	X.1719–X.1712
تقنيات آمن شبكات توزيع المفاتيح الكمومية	X.1729–X.1720
آمن البيانات	
آمن البيانات الضخمة	X.1759–X.1750
حماية البيانات	X.1789–X.1770
آمن الاتصالات المتنقلة الدولية–2020	X.1819–X.1800

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1333

المبادئ التوجيهية الأمنية لاستعمال أدوات النفاذ عن بُعد في أنظمة التحكم الموصولة بالإنترنت

ملخص

تستعمل أدوات النفاذ عن بُعد (RAT) على نطاق واسع في أنظمة التحكم للمراقبة والتحكم والصيانة بغية تقليل تكاليف الصيانة وتدنية وقت الاستجابة في حال حدوث عطل. وتقدم أدوات النفاذ عن بُعد القدرة على معالجة أنظمة التحكم عن بُعد، ولكن في الوقت نفسه، يمكن للتشكيلة غير الآمنة لأدوات النفاذ عن بُعد ونقاط الضعف في هذه الأدوات أن توسع كثيراً من جبهة الهجوم على أنظمة التحكم. وتكمن أخطر مشكلة في السطح البيني للنفاذ إلى نظام تحكم من شبكات خارجية يمكنه أن يمكِّن نفاذ المهاجمين إلى نظام التحكم من الإنترنت.

وترسم التوصية ITU-T X.1333 صورة عامة لاستعمال أدوات النفاذ عن بُعد على نحو آمن لمراقبة الاتصالات والتحكم فيها وصيانتها. وتحدَد في هذه التوصية التهديدات لتشكيلة الشبكة بسبب استعمال أدوات النفاذ عن بُعد وتقدَّم المبادئ التوجيهية الأمنية لتكييف التشكيلة الآمنة وتدابير الأمن لاستعمال أدوات النفاذ عن بُعد في أنظمة التحكم الموصولة بالإنترنت.

ومن شأن تقديم ضوابط أمنية حسنة التنظيم بشأن استعمال أدوات النفاذ عن بُعد أن يساعد مقدمي الخدمات الرقمية الذين يقومون بتشغيل أنظمة تحكم لتقليل جبهة الهجمات والتهديدات الناجمة عن الشبكات الخارجية. وعلاوة على ذلك، سيستفاد من مواءمة مستويات الأمن بين البلدان المتقدمة والبلدان النامية، لأن المشكلة ليست مشكلة محلية، بل مشكلة عالمية.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1333	2022-01-07	17	11.1002/1000/14798

مصطلحات أساسية

نظام التحكم؛ مبادئ توجيهية؛ أداة النفاذ عن بُعد، الأمن؛

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة الأمم المتحدة المتخصصة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع/ حقوق ملكية برمجيات يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية الرجوع إلى قواعد البيانات المناسبة لدى قطاع تقييس الاتصالات المتاحة في الموقع الإلكتروني للقطاع في الموقع http://www.itu.int/ITU-T/ipr/.

© ITU 2022

جميع الحقوق محفوظة. لا يجوز استنساخ أي جزء من هذه المنشورة بأي وسيلة كانت إلا بإذن خطي مسبق من الاتحاد الدولي للاتصالات.

جدول المحتويات

الصفحة

التوصية ITU-T X.13331333

المبادئ التوجيهية الأمنية لاستعمال أدوات النفاذ عن بُعد في أنظمة التحكم الموصولة بالإنترنت

1 مجال التطبيق

تقدم هذه التوصية المبادئ التوجيهية الأمنية لاستعمال أدوات النفاذ عن بُعد (RAT) في أنظمة التحكم الموصولة بالإنترنت عبر شبكات الاتصالات. وتغطي التوصية ما يلي:

- تحديد التهديدات ضد التشكيلة غير الآمنة لأدوات النفاذ عن بُعد وأثرها على أنظمة التحكم الموصولة بالإنترنت؛
- الضوابط الأمنية وأسبابها المنطقية في التشكيلة الآمنة لأدوات النفاذ عن بُعد؛
- المبادئ التوجيهية للتنفيذ في كل تحكم أمني؛
- مثال على تشكيلة آمنة لأدوات النفاذ عن بُعد في التذييل.

2 المراجع

يتضمن ما يلي من توصياتٍ لقطاع تقييس الاتصالات بالاتحاد الدولي للاتصالات (ITU-T) وغيرها من المراجع أحكاماً تشكل بالإحالة إليها في النص الحالي أحكام التوصية الحالية. وعند نشر هذه التوصية، كانت إصدارات التوصيات والمراجع المشار إليها سارية المفعول. لكن لمّا كانت جميع التوصيات وغيرها من المراجع تخضع للمراجعة، تُشجَّع الجهات المستعينة بهذه التوصية على بحث إمكانية تطبيق أحدث إصدار من التوصيات وسائر المراجع المسرودة أدناه. وتُنشر بانتظام قائمة بتوصيات قطاع تقييس الاتصالات السارية. والإحالة إلى وثيقة ما في هذه التوصية لا تضفي على الوثيقة في حد ذاتها صفة التوصية.

لا توجد.

3 التعاريف

1.3 مصطلحات معرَّفة في مصادر أخرى

تستعمل هذه التوصية المصطلح التالي المعرف في مصادر أخرى:

1.1.3 السطح البيني للإنسان والآلة (HMI) [b-IEC 61924-2]: جزء النظام الذي يتفاعل معه المشغل. والسطح البيني هو مجموع الوسائل التي يتفاعل بها المستعملون مع آلة وجهاز ونظام. ويقدم السطح البيني وسيلة لإدخال المعلومات بما يسمح للمستعملين بالتحكم في النظام وخرجه، مما يسمح للنظام بإبلاغ المستعملين.

2.3 المصطلحات المعرّفة في هذه التوصية

لا توجد.

4 الاختصارات والأسماء المختصرة

تستعمل هذه التوصية الاختصارات والأسماء المختصرة التالية:

DDoS الحرمان من الخدمة الموزَّع (*Distributed Denial of Service*)

DMZ المنطقة منزوعة السلاح (*Demilitarized Zone*)

DNS خدمة اسم الميدان (*Domain Name Service*)

DoS الحرمان من الخدمة (*Denial of Service*)

EWS محطة العمل الهندسية (*Engineering Workstation*)

HMI السطح البيني للإنسان والآلة (*Human Machine Interface*)

ICMP بروتوكول رسالة التحكم في الإنترنت (*Internet Control Message Protocol*)

IDS نظام كشف الاقتحام (*Intrusion Detection System*)

IPsec أمن بروتوكول الإنترنت (*Internet Protocol Security*)

LAN شبكة المنطقة المحلية (*Local Area Network*)

MAC التحكم في النفاذ إلى الوسائط (*Media Access Control*)

MDM إدارة الأجهزة المتنقلة (*Mobile Device Management*)

MDMS نظام إدارة بيانات العداد (*Meter Data Management System*)

NAC التحكم في النفاذ إلى الشبكة (*Network Access Control*)

NFC اتصالات المجال القريب (*Near Field Communication*)

PIN رقم تعرّف الهوية الشخصي (*Personal Identification Number*)

PLC وحدة التحكم القابلة للبرمجة (*Programmable Logic Controller*)

RAT أداة النفاذ عن بُعد (*Remote Access Tool*)

RFID التعرف بواسطة الترددات الراديوية (*Radio Frequency Identification*)

SIEM إدارة المعلومات والأحداث الأمنية (*Security Information and Event Management*)

SSH درع آمن (*Secure Shell*)

SSL طبقة المقبس الآمن (*Secure Socket Layer*)

TLS أمن طبقة النقل (*Transport Layer Security*)

URL محدد مواقع الموارد الموحد (*Uniform Resource Locator*)

VM الآلة الافتراضية (*Virtual Machine*)

VPN شبكة افتراضية خاصة (*Virtual Private Network*)

5 الاصطلاحات

تستعمل هذه التوصية الاصطلاحات التالية:

وتشير كلمة "**ينبغي**" إلى متطلَّب يُوصى به لكنه ليس ملزِماً إلزاماً مطلَقاً.

وكلمة "**يجوز**" تدل على مطلب اختياري مسموح به دون أن ينطوي على أي توصية به.

وفي متن هذه التوصية، تظهر في بعض الأحيان كلمة "**يمكن**". وفي هذه الحالة يكون تأويلها بمعنى فعل "**يستطيع**" أو "**استطاع**".

ويأوّل انتفاء القصد المعياري عند ظهور العبارات "يجب" و"ينبغي" و"سوف" في التذييل I على أنها إعلامية.

6 نظرة عامة – أدوات النفاذ عن بُعد في أنظمة التحكم الموصولة بالإنترنت

تُستعمل أنظمة التحكم لتحقيق هدف صناعي مثل التصنيع ونقل المادة أو الطاقة. ويتولى نظام التحكم مسؤولية ضمان النتيجة المرجوة أو أداء الهدف الصناعي. ولضمان أداء نظام التحكم، يراقب المشغلون المعلومات والبيانات من أجهزة الاستشعار في الشبكات الميدانية (انظر الشكل 1). واستناداً إلى البيانات والمعلومات، يمكن للمشغلين التحكم في النظام عند الحاجة. وللحفاظ على نظام التحكم أو حل المشاكل التقنية، يمكن لمهندسي الصيانة من بائعي نظام التحكم النفاذ إلى نظام التحكم.

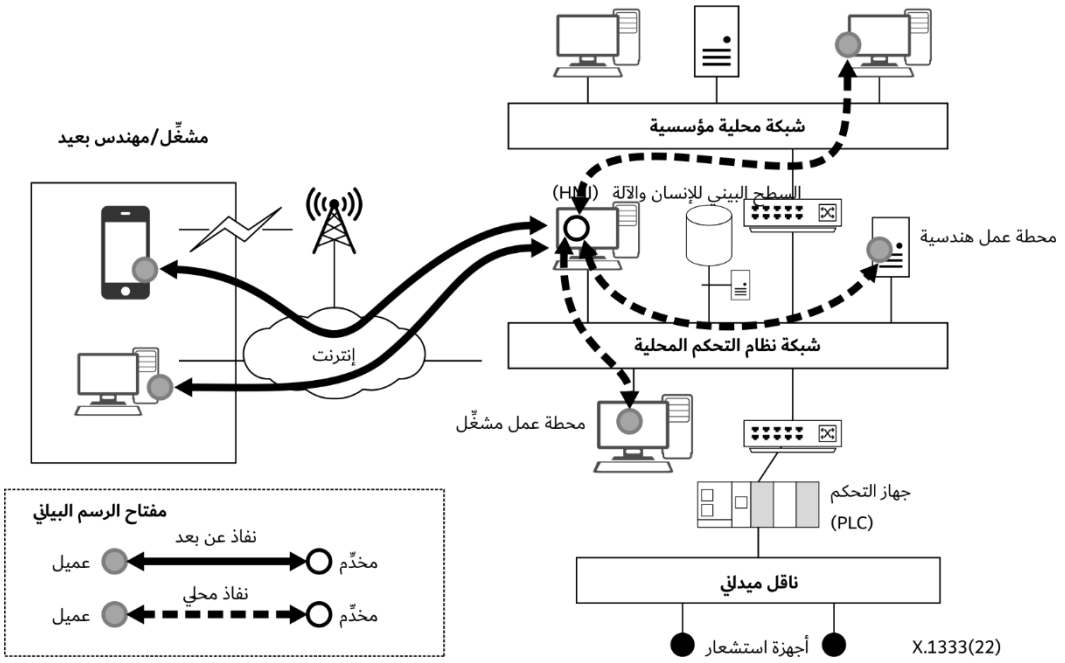
وتُستعمل أدوات النفاذ عن بُعد (RAT) على نطاق واسع في الشبكات الصناعية لمراقبة نظام التحكم والتحكم فيه وصيانته لخفض تكاليف الصيانة وتقليل زمن الاستجابة إلى أدنى حد في حال حدوث عطل. ووفقاً للمرجع [b-Kruglov et al.]، في النصف الأول من عام 2018، استعملت أدوات النفاذ عن بُعد في 31,6% من حواسيب نظام التحكم، ولم يشمل هذا الرقم عدد توصيلات سطح المكتب عن بُعد.

وفي معظم حالات أنظمة التحكم، يشيع استعمال أدوات النفاذ عن بُعد من أجل:

- مراقبة/التحكم في السطح البيني للإنسان والآلة (HMI) من محطة عمل مشغِّل؛
- مراقبة/التحكم في السطح البيني للإنسان والآلة (HMI) من محطة عمل هندسية؛
- توصيل مشغلين متعددين بمحطة عمل مشغِّل واحد؛
- توصيل المشغلين عن بُعد بمحطة عمل مشغِّل عبر شبكة خارجية؛
- تقديم صيانة نظام التحكم الموصول بالإنترنت من حاسوب مهندس صيانة لدى بائع نظام التحكم عبر شبكة خارجية.

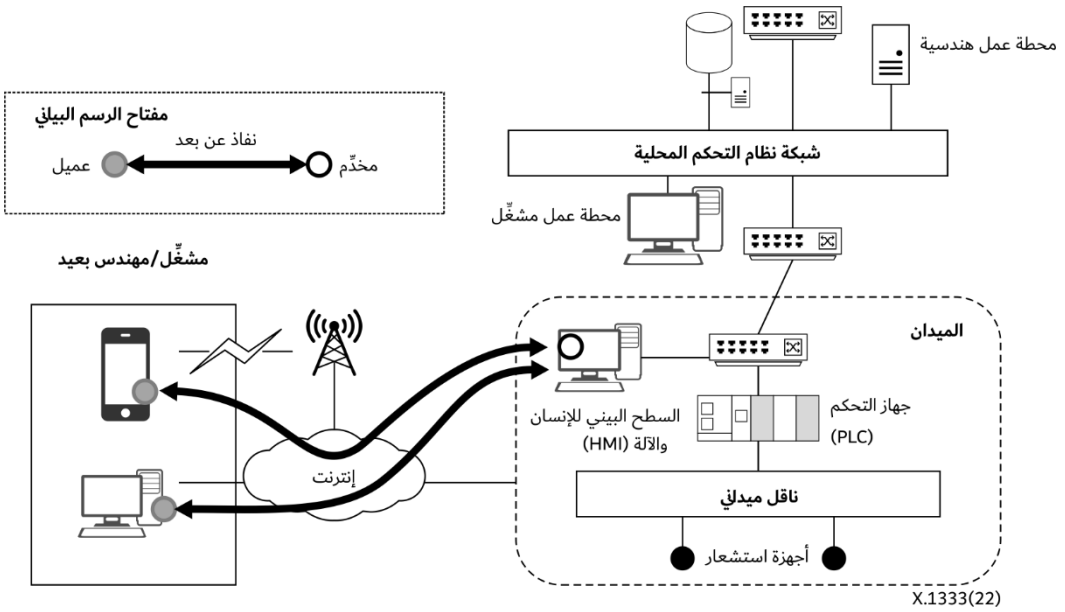
وتبين حالات الاستعمال هذه أن استعمال أدوات النفاذ عن بُعد في مراقبة نظام التحكم والتحكم فيه وصيانته قد يشكل متطلبات لا غنى عنها لتشغيل أنظمة التحكم. وعلاوة على ذلك، من شأن استعمال أدوات النفاذ عن بُعد أن يخفض تكاليف الصيانة. فعلى سبيل المثال، يمكن خفض عدد التراخيص لبرمجيات السطح البيني للإنسان والآلة (HMI) في النقاط الثلاث الأولى من بين حالات الاستعمال المذكورة أعلاه. وبالإضافة إلى ذلك، يمكن أيضاً استعمال الأجهزة الذكية الحديثة كعملاء أدوات النفاذ عن بُعد (RAT). ويمكن للعملاء النهائيين مراقبة خلاياهم الكهرضوئية (PV) والتحكم فيها، عن طريق استعمال أدوات النفاذ عن بُعد في هاتفهم الذكي على سبيل المثال.

ويبين الشكل 1 تشكيلة عامة لاستعمال أدوات النفاذ عن بُعد في أنظمة التحكم الموصولة بالإنترنت استناداً إلى حالات الاستعمال.



الشكل 1 – تشكيلة الشبكة لاستعمال أدوات النفاذ عن بُعد في أنظمة التحكم الموصولة بالإنترنت

وفي حالات أخرى، يمكن لنظام تحكم قيد التشغيل في منظمة أن يرفق أنظمة تحكم تقليدية بنظام تحكم صغير. فعلى سبيل المثال، يمكن لأي موقع يشغل مولد قدرة ضخم استعمال نظام خلية وقود جديد لزيادة سعته بطاقة نظيفة. وتتضمن أنظمة خلية الوقود حواسيب السطح البيني للإنسان والآلة (HMI) وأجهزة التحكم وأجهزة الاستشعار والبطاريات وغيرها من الأنظمة. وهكذا، يمكن في هذا المثال توصيل السطح البيني للإنسان والآلة (HMI) وأجهزة التحكم بنفس الشبكة الفرعية الواقعة في الجانب الميداني من نظام خلية الوقود. ويبين الشكل 2 تشكيلة استعمال أدوات النفاذ عن بُعد (RAT) للنفاذ إلى السطح البيني للإنسان والآلة (HMI) في الميدان.



الشكل 2 – تشكيلة الشبكة لاستعمال أدوات النفاذ عن بُعد في شبكة ميدانية لأنظمة تحكم موصولة بالإنترنت

تقدم أدوات النفاذ عن بُعد القدرة على التعامل مع أنظمة التحكم عن بُعد، وتساعد على خفض تكاليف الصيانة. غير أن التشكيلة غير الآمنة لأدوات النفاذ عن بُعد ومواطن ضعفها يمكن أن توسع كثيراً من جبهة الهجوم على أنظمة التحكم. وتتمثل أشد مشكلة في إمكانية استعمال أدوات النفاذ عن بُعد (RAT) كسطح بيني للنفاذ إلى نظام تحكم موصول بالإنترنت من الشبكات الخارجية يمكنه عادة النفاذ من الإنترنت. وبالتالي، بمجرد أن يتمكن الخصوم من تعريض عميل أدوات النفاذ عن بُعد للخطر في نظام تحكم موصول بالإنترنت، فقد يتسببون في حدوث خلل في النظام. علاوة على ذلك، يصعب كشف أنشطتهم. ومن ثم، تركز هذه التوصية على توصيلات أدوات النفاذ عن بُعد من خارج أنظمة التحكم الموصولة بالإنترنت.

7 التهديدات لاستعمال أدوات النفاذ عن بُعد في أنظمة التحكم الموصولة بالإنترنت

1.7 التهديدات لعملاء أدوات النفاذ عن بُعد (RAT)

يمكن تثبيت عميل أدوات النفاذ عن بُعد في حاسوب العميل في مكان بعيد أو جهاز متنقل يملكه مشغل بعيد أو مهندس صيانة عن بُعد. ويمكن أن يكون الموقع البعيد خارج الحماية المادية للمنظمة والحماية المنطقية لجدار الحماية الخاص بالمنظمة. وبالإضافة إلى ذلك، لا تتسنى إدارة حواسيب العميل إدارة جيدة فيما تدار حواسيب المنظمة عن كثب وتُغلق بإحكام. وبالتالي، فإن العديد من التهديدات لاستعمال أدوات النفاذ عن بُعد يمكن أن تأتي من الحواسيب التي يثبَّت عليها عميل أدوات النفاذ عن بُعد.

وينبغي النظر في التهديدات التالية التي تتعرض لها حواسيب العملاء وعملاء أدوات النفاذ عن بُعد:

- (التهديد 1) يمكن للمهاجم أن يستغل نقاط الضعف في حواسيب العملاء أو عملاء أدوات النفاذ عن بُعد لخرق حواسيب العملاء أو عملاء أدوات النفاذ عن بُعد (RAT). وحالما يتمكن المهاجمون من التحكم الكامل في حاسوب العميل أو عميل أدوات النفاذ عن بُعد (RAT)، يمكنهم التوصيل بنظام التحكم عن طريق أدوات النفاذ عن بُعد.
- (التهديد 2) يمكن لخصم استغلال الانقسام النفقي في حاسوب العميل. وعادة ما تكون حواسيب العملاء موصولة ليس بمخدمات أدوات النفاذ عن بُعد (RAT) فحسب، بل أيضاً بأية أنظمة أخرى موصولة بالإنترنت. ومن ثم، يمكن لأحد الخصوم الذي يتحكم تحكماً كاملاً في حاسوب العميل أن يرسل المعلومات الحرجة المستقاة من نظام التحكم عن طريق توصيل غير محمي بالإنترنت.

- (التهديد 3) يمكن للمهاجم تثبيت برمجيات ضارة مستهدِفة في حاسوب العميل، وتحديد المعلومات الحساسة (مثل هوية تسجيل الدخول وكلمة المرور) وسل المعلومات إلى الخارج. وحالما يحصل المهاجمون على المعلومات، يمكنهم النفاذ إلى مخدم أدوات النفاذ عن بُعد باستعمال عميل أدوات النفاذ عن بُعد المثبَّت على أي آلة أخرى بدلاً من حاسوب العميل.
- (التهديد 4) يستطيع مهاجم أن يشن هجوم القوة العمياء، أو هجوم القاموس، أو فك كلمة المرور مدعوماً باستخدام أدوات مفتوحة المصدر للنفاذ إلى مخدم أدوات النفاذ عن بُعد (RAT).
- (التهديد 5) يمكن للخصوم إخفاء أنشطتهم على حواسيب العملاء من خلال حذف بيانات السجل. وبسبب ذلك، تعجز منظمة تشغل نظام التحكم عن تتبع أنشطة الخصم عندما تحقق المنظمة في الحادث.
- (التهديد 6) يمكن لأحد الخصوم أن يستغل النفاذ المادي إلى حواسيب العملاء.

2.7 التهديدات لمخدمات أدوات النفاذ عن بُعد

يمكن تثبيت مخدم أدوات النفاذ عن بُعد على آلة السطح البيني للإنسان والآلة (HMI) في نظام تحكم موصول بالإنترنت. وبما أن المخدِّم ينبغي أن يفتح خدمة موصولة بالإنترنت، يمكن لأحد الخصوم أن يستغل المنفذ للخدمة. وإذا لم تكن الخدمة محمية بشكل آمن، يمكن للمهاجم النفاذ إلى نظام التحكم عن طريق الخدمة.

وينبغي النظر في التهديدات التالية التي تتعرض لها حواسيب العملاء وعملاء أدوات النفاذ عن بُعد:

- (التهديد 7) يمكن لمهاجم أن يستغل نقاط الضعف في مخدم أدوات النفاذ عن بُعد أو في آلة جرى تثبيت مخدم أدوات النفاذ عن بُعد فيها لاختراق الآلة أو مخدم أدوات النفاذ عن بُعد. ويمكن أن يؤدي هذا النوع من الهجمات المهاجم إلى السيطرة الكاملة على نظام التحكم. فبمجرد تمكن المهاجمين من النفاذ إلى الآلة أو مخدم أدوات النفاذ عن بُعد على سبيل المثال، يمكنهم الارتقاء بحقهم في الجهاز أو اكتساب السيطرة الكاملة على مخدم أدوات النفاذ عن بُعد.
- (التهديد 8) يمكن لخصم شن هجمات الحرمان من الخدمة الموزَّع (DDoS) والحرمان من الخدمة (DoS) ضد مخدم أدوات النفاذ عن بُعد.

3.7 التهديدات لقناة الاتصالات بين العميل والمخدمات

نظراً لأن مخدم أدوات النفاذ عن بُعد والعميل موصولين عبر الإنترنت في نظام تحكم موصول بالإنترنت، يمكن لأي جهات أخرى النفاذ إلى قناة الاتصالات. وإذا كانت الاتصالات غير مجفّرة أو مجفّرة بأساليب ضعيفة تحتوي على نقاط ضعف معروفة للعموم، يمكن لخصم الاستفادة منها والنفاذ إلى المعلومات والقنوات المنقولة.

وينبغي النظر في التهديدات التالية التي تتعرض لها حواسيب العملاء وعملاء أدوات النفاذ عن بُعد:

- (التهديد 9) يمكن لخصم أن يستفيد من الاتصالات غير المحمية، ويحصل على معلومات حساسة (مثل هوية تسجيل الدخول وكلمة المرور)، ويستعمل المعلومات للنفاذ إلى مخدّم أدوات النفاذ عن بُعد (RAT). وعندما تكون قناة الاتصالات محمية بتجفير ضعيف، يمكن أن يحصل الخصم على نفس النتيجة. وحالما يتمكن الخصوم من النفاذ إلى مخدم أدوات النفاذ عن بُعد (RAT)، يمكنهم التحكم تماماً في نظام التحكم.
- (التهديد 10) يستطيع المهاجم أن يستفيد من بروتوكول ضعيف يتضمن مواطن ضعف معروفة للعموم وأن يتمكن من النفاذ إلى مخدم أدوات النفاذ عن بُعد أو أن يتسبب في الحرمان من الخدمة لمستعملي مخدمات أدوات النفاذ عن بُعد.

8 المبادئ التوجيهية الأمنية لاستعمال أدوات النفاذ عن بُعد في أنظمة التحكم الموصولة بالإنترنت

1.8 المبادئ التوجيهية الأمنية لعملاء أدوات النفاذ عن بُعد (RAT)

1.1.8 تحديث البرمجيات

التحكم الأمني

ينبغي تحديث برمجيات أدوات النفاذ عن بُعد ونظام التشغيل وأي برمجيات أخرى تقع على جانب العميل.

الغرض

قد تتخلل البرمجيات ثغرات أمنية مجهولة نظراً إلى تقدم تقنيات الهجوم. وعند الإعلان عن ثغرة أمنية جديدة، تكون ثغرة أمنية في يوم صِفر (يوم–0). ويمكن للمهاجمين استغلال الثغرة الأمنية في يوم–0 لاختراق جهاز عميل أدوات النفاذ عن بُعد. وازداد مؤخراً عدد الثغرات الأمنية المتعلقة ببرمجيات أدوات النفاذ عن بُعد (RAT). وفي عام 2019، اكتُشفت 31 ثغرة أمنية في برمجيات شبيهة بحوسبة الشبكة الافتراضية (VNC). وسيقدم بائعو برمجيات أدوات النفاذ عن بُعد برمجية أمنية تصحيحية عند صدور ثغرة أمنية جديدة، ويستطيع المستعملون التخفيف من هذه الثغرة من خلال اعتماد البرمجيات الأمنية التصحيحية. ويعد تحديث البرمجيات من أسهل الطرق للحفاظ على أمن أجهزة العملاء.

المبادئ التوجيهية للتنفيذ

للحفاظ على مواكبة البرمجيات لآخر المستجدات، فإن أهم شيء هو التحقق بانتظام مما إذا كان هناك تحديث جديد. ولسوء الحظ، لا يسهل على المستعملين إجراء هذا التحقق المنتظم، وبالتالي ينبغي النظر في النهج التلقائي التالي لتحديث البرمجيات.

أ) ينبغي إطلاق أسلوب التحقق من التحديث الأمني عند تنفيذ برمجيات عملاء أدوات النفاذ عن بُعد (RAT).

ب) إذا كان هناك إصدار جديد من البرمجيات أو تحديث أمني جديد، ينبغي تطبيقه على برمجيات العميل قبل تنفيذها.

ج) يمكن أيضاً إطلاق أسلوب التحقق من التحديث الأمني بانتظام أثناء تشغيل عميل أدوات النفاذ عن بُعد (RAT).

د) في حال وجود إصدار جديد من البرمجيات أو تحديث أمني جديد، ينبغي تطبيقه على برمجيات العميل عند إنهائها.

وفي بعض الحالات، تنبغي إعادة بدء تشغيل جهاز عميل أدوات النفاذ عن بُعد عقب تثبيت برمجية تعزيز الأمن. وخلافاً للحاسوب النمطي للعميل، تتعذر إعادة تشغيل عميل أدوات النفاذ عن بُعد (RAT) في نظام التحكم في ذلك الوقت لأن المشغل/المهندس البعيد ينبغي أن يراقب نظام التحكم باستمرار. وفي هذه البيئة، تثبّت طريقة التحقق من التحديث الأمني التحديثات بعد الحصول على تأكيد المستعمل.

بالإضافة إلى ذلك، ينبغي أيضاً تحديث نظام التشغيل وأي برمجية أخرى في برمجية عميل أدوات النفاذ عن بُعد المشغِّلة للجهاز. وينبغي تمكين قدرة التحديث التلقائي لأنظمة التشغيل. وينبغي التحقق من التحديث الأمني لكل تطبيق بانتظام وتطبيق البرمجيات الأمنية التصحيحية على الفور عند تيسرها.

2.1.8 سلامة البرمجيات

التحكم الأمني

تنبغي حماية سلامة برمجيات أدوات النفاذ عن بُعد (RAT) الواقعة في جانب العميل.

الغرض

يمكن تثبيت نسخة معدلة من برمجيات أدوات النفاذ عن بُعد في جانب العميل. ويمكن للمهاجم اختراق مخدم التحديث أو يمكنه توزيع تحديثات غير عادية عن طريق التصيد الاحتيالي بالبريد الإلكتروني. وبرمجيات أدوات النفاذ عن بُعد (RAT) المصابة بشفرة ضارة تتصرف بشكل طبيعي، ولكن الشفرة الضارة تعمل على تسريب المعلومات أو إنشاء توصيل مع المهاجم عند الضرورة. ومن ثم، لمنع سوء سلوك برمجيات RAT الخبيثة، تنبغي حماية سلامتها.

المبادئ التوجيهية للتنفيذ

نظراً لأن المهاجمين، كما ذكر أعلاه، يستطيعون توزيع برمجيات RAT الخبيثة عبر سلسلة توريد رسمية، ثمة إشكالات تعترض المستعمل في تحديد ما إذا كانت البرمجيات معدلة أم لا. ومن ثم، ينبغي استعمال إجراء التحقق التلقائي من السلامة لحماية سلامة برمجيات أدوات النفاذ عن بُعد (RAT).

وفي إجراءات التحقق التلقائي من السلامة، ينبغي النظر في النهج التالي:

أ) ينبغي الشروع في إجراء التحقق من السلامة عند تنفيذ البرمجيات أو عند بدء إجراء التحديث.

ب) ينبغي بدء تشغيل البرمجيات أو إجراء التحديث في غياب أي دليل على تغيير البرمجيات.

ج) ينبغي أن تظهر حالة إجراء التحقق من السلامة على الشاشة، بحيث يعرف المستعمل أن هذه البرمجية على ما يرام.

د) ينبغي إنشاء قيمة سلامة البرمجيات بأسلوب تجفيري لضمان عدم تعديل أي شخص آخر للبرمجيات. ولهذا الأسلوب، ينبغي استعمال خوارزمية تجفيرية آمنة.

3.1.8 التشكيلة الآمنة لعملاء أدوات النفاذ عن بُعد (RAT)

التحكم الأمني

ينبغي للتشكيلة في جانب عميل أدوات النفاذ عن بُعد أن تلتزم بالسياسة الأمنية للمنظمة التي تملك نظام التحكم الموصل بالإنترنت.

الغرض

على الرغم من أن برمجيات أدوات النفاذ عن بُعد تقدم القدرات الأمنية للاتصالات الآمنة، فإن أدوات النفاذ عن بُعد لا يمكن استعمالها بشكل آمن إلا عند تشكيلها على الوجه الصحيح. وبشكلٍ عام، يرغب المستعملون في تجنب أي إرباك، وبالتالي فهم لا يريدون تمكين ميزات الأمن واستعمال كلمة مرور قوية. وعلاوة على ذلك، فيما يتعلق أمن بروتوكول الإنترنت (IPsec)، حيث لا يعرف المستعمل تفاصيل التشكيلة الصحيحة. وستزيد هذه التشكيلات الخاطئة من إمكانية إساءة استعمال برمجيات عملاء أدوات النفاذ عن بُعد.

المبادئ التوجيهية للتنفيذ

لتقليل احتمال الخطأ في تشكيلة عميل أدوات النفاذ عن بُعد (RAT)، من الأفضل أن تقوم منظمة تشغّل نظام تحكم بتشكيل العميل. وفي إدارة المنظمة لتشكيلة عملاء أدوات النفاذ عن بُعد (RAT)، ينبغي النظر في النُهج التالية:

أ) استعمال بروتوكول الإنترنت (IP) الساكن لمخدم أدوات النفاذ عن بُعد (RAT): إذا استُعمل موقع الموارد الموحد (URL) للنفاذ إلى مسيِّر شبكة افتراضية خاصة (VPN) أو مخدم أدوات النفاذ عن بُعد (RAT)، قد يتعرض المشغلون/المهندسون عن بُعد لعدة هجمات مثل التصيد الاحتيالي وانتحال خدمة اسم الميدان (DNS) وتسميم ذاكرة التخزين المؤقت لنظام أسماء الميادين (DNS). ومن شأن استعمال عنوان بروتوكول الإنترنت (IP) الساكن أو عنوان IP المشفَّر ضمن شفرة المصدر في جانب المخدّم أن يمكّن من التخفيف من تلك التهديدات وتقديم استيقان المخدم للمشغلين/المهندسين عن بُعد خلال قناة الاتصالات الآمنة.

ب) حل التحكم في النفاذ إلى الشبكة (NAC) أو إدارة الجهاز المتنقل (MDM): يقدم التحكم في النفاذ إلى الشبكة القدرات اللازمة للتحقق من حالة الحاسوب أو الحاسوب المحمول، في حين تدعم إدارة الجهاز المتنقل القدرات اللازمة للتحقق من الأجهزة المتنقلة والتحكم فيها. ويساعد التحكم في النفاذ إلى الشبكة المنظمات في تحفيز المشغلين/المهندسين عن بُعد على تشكيل حاسوب يدير عميل أدوات النفاذ عن بُعد وذلك بالتحقق من تشكيلات الجهاز قبل إقامة التوصيل. وإذا كان الجهاز مشكَّلاً بشكل خاطئ، يحظر التحكم في النفاذ إلى الشبكة حركة الشبكة من الجهاز إلى أن يقوم المشغلون/المهندسون عن بُعد بإصلاح التشكيل الخاطئ. إذا استعمل المشغلون عن بُعد أجهزة متنقلة للنفاذ إلى مخدم أدوات النفاذ عن بُعد (RAT)، تحل إدارة الجهاز المتنقل محل التحكم في النفاذ إلى الشبكة.

ج) صورة الآلة الافتراضية (VM): يمكن للمنظمة التي تملك نظام تحكم أن توزع صورة الآلة الافتراضية على المشغلين/المهندسين عن بُعد. وعندما تنشئ المنظمة الصورة، ينبغي تشكيل جميع التشكيلات المتعلقة بجهاز العميل وعميل الشبكة الافتراضية الخاصة وعميل أدوات النفاذ عن بُعد على أساس السياسة الأمنية للمنظمة. وعلاوةً على ذلك، ولحماية صورة الآلة الافتراضية نفسها، ينبغي تجفيرها وتخزينها في أجهزة المشغلين/المهندسين عن بُعد عندما لا تكون قيد الاستعمال.

4.1.8 التحكم في نفاذ المستعمل إلى جهاز العميل

التحكم الأمني

ينبغي ألا يسمح إلا للمستعملين المخولين بالنفاذ إلى برمجيات عملاء أدوات النفاذ عن بُعد (RAT).

الغرض

إذا اقتصر النفاذ إلى برمجيات عملاء أدوات النفاذ عن بُعد على المشغلين/المهندسين عن بُعد المخولين، يمكن تقليل إمكانية إساءة استعمال عميل أدوات النفاذ عن بُعد.

ومع ذلك، يمكن للمشغلين/المهندسين عن بُعد الشرعيين مغادرة المكان مؤقتاً أثناء استعمالهم برمجيات أدوات النفاذ عن بُعد (RAT)، وعندئذٍ تلوح إمكانية إساءة استعمال الدورة الموصولة. وبالتالي، عندما يتوقف المشغلون/المهندسون عن بُعد أو يوقفون عملهم مؤقتاً، ينبغي قفل الجهاز. وعندما يعود المشغلون/المهندسون عن بُعد للحضور أمام جهاز عميل أدوات النفاذ عن بُعد (RAT)، يمكن للمشغلين/المهندسين استئناف عملهم باستعمال إجراءات تعرف الهوية والاستيقان المعمول بها.

المبادئ التوجيهية للتنفيذ

يمكن تنفيذ هذا التحكم بحمل المشغلين/المهندسين عن بُعد على استعمال حساب مختلف عن الحساب المستعمل لأداء مهام منتظمة عند تنفيذ برمجيات عميل أدوات النفاذ عن بُعد (RAT). وبعبارة أخرى، ينبغي أن يكون لدى المشغل/المهندس البعيد حساب آخر لاستعمال عميل أدوات النفاذ عن بُعد (RAT). وبالإضافة إلى ذلك، ينبغي أن تكون كلمة مرور الحساب قوية.

ويعتبر قفل الدورة طريقة فعالة لحل هذا الإشكال الأخير. وهناك نوعان من قفل الدورة؛ 1) قفل الدورة على مستوى نظام التشغيل و2) قفل الدورة على مستوى التطبيق. ولدى معظم أنظمة التشغيل القدرة على قفل الدورات، ولذلك ينبغي بدء تشغيلها بعد فترة من الخمول. ويعتمد ذلك على برمجيات أدوات النفاذ عن بُعد (RAT)، ويختلف اعتماداً على إمكانية قفل الدورة على مستوى التطبيق من عدمه. وبالتالي، ينبغي أن يكون وجود قدرة قفل الدورة معياراً رئيسياً عندما تختار المنظمة المشغِّلة لنظام التحكم برمجيات RAT.

5.1.8 الأمن المادي

متطلبات الأمن

ينبغي عدم السماح إلا للمشغلين/المهندسين عن بُعد المخولين بالنفاذ إلى برمجيات عميل أدوات النفاذ عن بُعد المشغلة مادياً، وتنبغي حماية المكان الذي يستعمل فيه المشغلون/المهندسون الأجهزة من النفاذ غير المخوَّل.

الغرض

على الرغم من تشكيل الجهاز وبرمجيات عميل أدوات النفاذ عن بُعد على نحو آمن لاستعمال خاصيتها الأمنية على الوجه الصحيح، تنبغي حماية الجهاز والمكان الذي يوجد فيه الجهاز من النفاذ غير المخوَّل من جانب أي خصم من الخصوم.

المبادئ التوجيهية للتنفيذ

لضمان الأمن المادي للأجهزة والبرمجيات والبيئة التي تستعملها، تنبغي مراعاة ما يلي:

أ) تنبغي حماية المكتب الذي يعمل فيه المشغلون/المهندسون عن بُعد بواسطة نظام مناسب للتحكم في النفاذ عبر الأبواب باستعمال تكنولوجيا الاتصال القريب (NFC) أو التعرف بواسطة التردد الراديوي (RFID). وللحصول على أمن أقوى، يمكن النظر في نظام بيومتري للتحكم في النفاذ (مثل بصمات الأصابع وقزحية العين والتعرف على الوجوه).

ب) ينبغي تركيب كاميرا تعمل بالدارة التليفزيونية المغلقة أمام باب المكتب.

ج) تنبغي حماية أي جهاز يُشغّل برمجيات عميل أدوات النفاذ عن بُعد من السرقة باستعمال قفل كبل أو رادع آخر.

2.8 المبادئ التوجيهية للأمن في مخدمات أدوات النفاذ عن بُعد

1.2.8 استيقان المستعمل

التحكم الأمني

ينبغي لخدمة أدوات النفاذ عن بُعد ألا تسمح للمستعملين بالنفاذ إلى موارد النفاذ عن بُعد إلا عند استعمال استيقان بعاملين.

الغرض

يمكن اختراق استيقان الهوية التقليدية وكلمة المرور، ولن تضمن عوامل المعرفة، مثل كلمة المرور أو رقم التعرف الشخصي (PIN)، بمفردها أن المستعمل الذي يهم بالنفاذ هو الشخص الذي لديه الأذونات المناسبة.

وبالنسبة للنفاذ المحلي، تحدد أساليب التحكم بالنفاذ المادي هوية المستعملين الشرعيين وتتيح لهم النفاذ إلى موارد النظام. وتبعاً لذلك، حتى إذا عرف المهاجم هوية المستعمل الشرعي وكلمة المرور الخاصة به، لا يسهل النفاذ مباشرة إلى موارد النظام. أما في مجال النفاذ عن بُعد، فلا يسهل تطبيق أساليب الأمن المادية وأساليب تعرف هوية المستعمل. ولذلك، بدلاً من أساليب الأمن المادي، يمكن للاستيقان بعاملين أن يقلل من إمكانية انتحال الهوية حتى في حال سرقة المعرف وكلمة المرور.

المبادئ التوجيهية للتنفيذ

يمكن أن تشمل عوامل الاستيقان شيئاً تعرفه (عامل المعرفة)، وشيئاً تملكه (عامل الحيازة)، وشيئاً يصفك (عاملاً متأصلاً)، ومكاناً توجد فيه (عاملاً قائماً على الموقع). ويميل الاستيقان بعاملين حالياً إلى أن ينفَّذ من خلال عامل حيازة وعامل معرفة أو عامل متأصل وعامل معرفة.

وفي الآونة الأخيرة، تعتمد معظم الأجهزة المتنقلة (مثل الحواسيب المحمولة والحواسيب اللوحية والهواتف الذكية) أساليب بيومترية، ومن ثم فإن العوامل المتأصلة، بما فيها بصمات الأصابع أو قزحية العين أو الوجه، يرجح أن تكون أفضل خيار للاستيقان بعاملين.

ولكن يتعذر استعمال الأساليب البيومترية في بعض الظروف. فعلى سبيل المثال، إذا اضطر المستعملون البعيدون إلى ارتداء القفازات أثناء ساعات عملهم، ينبغي تجنب البصمة. وفي هذه الحالات، يمكن تطبيق عوامل حيازة من قبيل تأشيرات تجفيرية.

وتقدم معظم برمجيات أدوات النفاذ عن بُعد القدرة على الحد من وقت الانتظار للاستيقان. وفي هذه الحالة يستبعد مخدم أدوات النفاذ عن بُعد طلب الاستيقان إذا لم يتلق رداً من المستعمل خلال فترة زمنية معينة. وبالتالي، يستفاد من ذلك في تقليل احتمال هجمات الحرمان من الخدمة.

2.2.8 تخويل المستعمل

التحكم الأمني

ينبغي ألا يكون لحسابات المستعملين عن بُعد إلا الامتيازات الدنيا اللازمة لأداء وظيفتها.

الغرض

للحد من تأثير الهجوم، ينبغي أن تقتصر امتيازات المستعمل عن بُعد على الحد الأدنى من الامتيازات اللازمة لأداء وظيفته.

المبادئ التوجيهية للتنفيذ

لا تقدم برمجيات أدوات النفاذ عن بُعد (RAT) عادةً أسلوب تخويل دقيق التفاصيل. ولا تقدم معظم برمجيات أدوات النفاذ عن بُعد إلا نوعين من الأساليب مثل أسلوب القراءة فقط وأسلوب التحكم الكامل. وبالتالي، إذا تمكن المهاجمون من النفاذ إلى مخدم أدوات النفاذ عن بُعد، يمكنهم اختراق الجهاز بالكامل. ولتجنب التهديد، يجب أن تقتصر الامتيازات الممنوحة لحسابات المستعمل عن بُعد على الحد الأدنى من الامتيازات اللازمة لأداء وظائفها.

ولذلك، ينبغي، أولاً وقبل كل شيء، ألا يكون حساب المستعمل عن بُعد حساب مسؤول، وينبغي عدم منح حساب المستعمل البعيد أي امتياز قادر على تغيير مخدم أدوات النفاذ عن بُعد. ويمكن أن يكون تثبيت برمجيات، وتشكيل نظام التشغيل، وتشكيل النظام أحد الامتيازات المحدودة.

ثانياً، ينبغي أيضاً تطبيق التحكم في النفاذ إلى التطبيق. فلا يمكن لحساب المستعمل عن بُعد تشغيل أي برمجية باستثناء نظام التحكم في تشغيل البرمجية ومراقبتها. وإذا استطاع مستعمل بعيد فتح برنامج مطراف في آلة مخدم أدوات النفاذ عن بُعد، يمكن للمستعمل النفاذ إلى نظام آخر عن طريق ذلك المخدم. ومن شأن ذلك أن يعود بفوائد ممتازة على المهاجمين.

3.2.8 معاودة الاستيقان الدورية

التحكم الأمني

ينبغي لمخدّم أدوات النفاذ عن بُعد أن يعاود استيقان المستعملين وأجهزة العملاء بعد فترة من الزمن.

الغرض

لضمان أن يقتصر استعمال النفاذ عن بُعد على المشغلين/المهندسين المخولين، ينبغي لمخدّم أدوات النفاذ عن بُعد أن يطلب منهم معاودة الاستيقان دورياً خلال دورات النفاذ الطويلة عن بُعد. ويساعد ذلك على ضمان عدم تمكن الأشخاص غير المخولين من استعمال النفاذ عن بُعد حتى إذا سُرق الجهاز في أثناء إنشاء اتصال بين مخدم أدوات النفاذ عن بُعد والعميل.

وبالإضافة إلى ذلك، تساعد معاودة الاستيقان على مستوى الشبكة على الحد من احتمال التعرض لهجمات اختطاف الدورة.

المبادئ التوجيهية للتنفيذ

ولا تقدم برمجيات مخدم أدوات النفاذ عن بُعد في حد ذاتها القدرة على معاودة الاستيقان بعد فترة من الزمن، في حين أن معظم مسيِّرات الشبكة الافتراضية الخاصة تقدم ميزة الأمن. وبالتالي، لتنفيذ هذا التحكم بشكل صحيح، ينبغي استعمال الشبكة الافتراضية الخاصة بين عميل أدوات النفاذ عن بُعد (RAT) والمخدم.

وبالإضافة إلى ذلك، تقدم معظم مسيِّرات الشبكة الافتراضية الخاصة القدرة على معاودة الاستيقان من العميل. ولذلك، ينبغي للمنظمة أن تتيح قدرة مسيِّر الشبكة الافتراضية الخاصة على استيقان مستعمل أو جهاز بعد فترة من الوقت. فعلى سبيل المثال، عند حمل اتصالات أدوات النفاذ عن بُعد (RAT) عبر الإصدار 1.3 من أمن طبقة النقل (TLS)، ينبغي تفعيل توسع استيقان عميل ما بعد التعارف. فإذا كان التوسع مفعلاً، يطلب مخدم أمن طبقة النقل استيقان العميل بعد إنشاء توصيل أمن طبقة النقل.

4.2.8 تحديث البرمجيات

التحكم الأمني

ينبغي تحديث برمجيات مخدم أدوات النفاذ عن بُعد ونظام التشغيل وأي برمجيات أخرى في جهاز المخدِّم.

الغرض

الأغراض المقابلة للتحكم الواردة في الفقرة 4.2.8 هي نفس الأغراض الموصَّفة في الفقرة 1.1.8.

المبادئ التوجيهية للتنفيذ

المبادئ التوجيهية المقابلة للتحكم الواردة في الفقرة 4.2.8 هي نفس تلك الموصَّفة في الفقرة 1.1.8.

3.8 المبادئ التوجيهية لأمن الشبكات

1.3.8 التحكم في النفاذ إلى الشبكة

التحكم الأمني

ينبغي عدم السماح إلا للمستعملين الشرعيين بالنفاذ إلى اتصالات الشبكة بين مخدم أدوات النفاذ عن بُعد (RAT) وعملاء أدوات النفاذ عن بُعد.

الغرض

يعتبر النفاذ إلى اتصالات الشبكة إحدى الخطوات الأولى لانتهاك الخدمة أو النظام. ويمكن للمهاجمين جمع المعلومات والبيانات بين مخدِّم أدوات النفاذ عن بُعد والعميل وحقن البيانات المزيفة إلى قناة الاتصالات، الأمر الذي يمكن أن يؤدي إلى هجوم الاعتراض الوسيط وتوزيع البرمجيات الضارة وهجمات الحرمان من الخدمة. ولحماية خدمة أدوات النفاذ عن بُعد ونظام التحكم فيها، ينبغي تقييد المستعملين الضارين من النفاذ إلى اتصالات الشبكة بين مخدم أدوات النفاذ عن بُعد والعميل.

المبادئ التوجيهية للتنفيذ

هناك عدة طرق للتحكم في النفاذ إلى الاتصالات الشبكية وحماية محتواها. ويمكن اعتبار الأساليب التالية خيارات.

- يمكن استعمال خط مؤجر لمنع المستعملين غير المخوَّلين من للنفاذ إلى الاتصالات بين نظام إدارة بيانات العداد (MDMS) والطرف الثالث من مقدمي الخدمات.
- ينبغي تطبيق أساليب الاتصالات الآمنة مثل أمن بروتوكول الإنترنت (IPsec) وطبقة المقبس الآمن للشبكة الخاصة الافتراضية (SSL VPN) على الاتصال بين عميل أدوات النفاذ عن بُعد (RAT) ومخدم. وينبغي تمرير حركة أدوات النفاذ عن بُعد ضمن نفق في شبكة خاصة افتراضية (VPN).
- في حال عدم تيسر شبكة خاصة افتراضية، ينبغي تنفيذ النفاذ عن بُعد عبر الإصدار 1.3 من أمن طبقة النقل (TLS)، على الأقل.

وينبغي النظر في خوارزمية تجفير آمنة عند استعمال طريقة اتصالات آمنة تشمل شبكة خاصة افتراضية (VPN) وأمن طبقة النقل (TLS). ويقدم التعديل [b-ITU-T X.1197] قائمة بأمثلة للخوارزميات الآمنة وأطوال المفاتيح. وعند إعداد قناة الاتصالات، ينبغي لمسيِّر الشبكة الافتراضية الخاصة أو مخدم أدوات النفاذ عن بُعد (RAT) أن يرفضا طلب التوصيل إذا لم يستعمل العميل خوارزمية آمنة وطول مفتاح آمن.

2.3.8 الاستيقان المتبادل على مستوى الشبكة

التحكم الأمني

ينبغي تطبيق الاستيقان المتبادل على قناة الاتصالات بين مخدم أدوات النفاذ عن بُعد وعميل أدوات النفاذ عن بُعد (RAT).

الغرض

ينبغي تنفيذ أسلوب استيقان متبادل لقنوات الاتصالات بحيث يتمكن عميل أدوات النفاذ عن بُعد من التحقق من شرعية مخدم أدوات النفاذ عن بُعد قبل تقديم بيانات اعتماد الاستيقان إليه. وبهذه الوظيفة، يمكن لخدمة أدوات النفاذ عن بُعد أن تتفادى هجمات الاعتراض الوسيط بين عميل أدوات النفاذ عن بُعد والمخدم.

المبادئ التوجيهية للتنفيذ

عند استعمال أمن بروتوكول الإنترنت (IPsec) أو طبقة المقبس الآمن للشبكة الخاصة الافتراضية (SSL VPN) أو الاتصالات عبر أمن طبقة النقل (TLS) في اتصالات أدوات النفاذ عن بُعد (RAT)، ينبغي استعمال شهادة المخدم وشهادة العميل لاستيقان بعضهما الآخر. فالعميل يستيقن المخدم بالتحقق من شهادة المخدم للتأكد من شرعية المخدم.

وتقدم معظم حلول الشبكات الافتراضية الخاصة (VPN) ميزة استيقان المخدم، ولكن هذه الميزة لا تفعَّل في كثير من الحالات. وبالتالي، عندما يستعمل نظام تحكم شبكة افتراضية خاصة لحماية خدمة أدوات النفاذ عن بُعد، ينبغي تفعيل خيار استيقان المخدم.

بالإضافة إلى ذلك، في أمن طبقة النقل، عادة ما يستيقن المخدم وحده العميل بالتحقق من بيانات اعتماد العميل، مثل الشهادة، لأن استيقان المخدم هو خيار. وبالتالي، إذا كان الاتصال بين مخدم وعميل محمياً بواسطة أمن طبقة النقل (TLS) لخدمة أدوات النفاذ عن بُعد (RAT)، ينبغي تطلُّب تبادل شهادات كل منهما بين المخدم والعميل.

وأخيراً، ينبغي تفعيل قدرة انتهاء مهلة الاستيقان والقدرة على الحد من الدورات المتزامنة. والتجاهل الصحيح لطلبات التوصيل التي تنتظر رد استيقان العميل هو مفتاح التخفيف من هجمات الحرمان من الخدمة.

3.3.8 كشف سوء سلوك الشبكة

التحكم الأمني

ينبغي تطبيق كشف سوء سلوك الشبكة على الشبكة التي يوصل بها مخدم أدوات النفاذ عن بُعد (RAT).

الغرض

على الرغم من تطبيق أساليب أمنية مختلفة في جانب عميل أدوات النفاذ عن بُعد، تبقى فرصة اختراق الجهاز المشغِّل لعميل أدوات النفاذ عن بُعد. فعلى سبيل المثال، إذا استطاع المهاجمون النفاذ إلى شبكة نظام تحكم موصول بالإنترنت عبر عميل أدوات النفاذ عن بُعد مخترَق، يمكنهم أيضاً النفاذ إلى أي موارد مسموح بها لمخدم أدوات النفاذ عن بُعد. وفي هذه الحالة، يكون الاختلاف الوحيد بين المشغلين/المهندسين عن بُعد والمهاجمين هو السلوك. ويعرف المشغلون/المهندسون عن بُعد الشبكة والنظام الموصولون بهما، في حين ينبغي للمهاجمين الاستطلاع لمعرفة مكان تحقيق الهدف في الشبكة. وتبعاً لذلك، يمكن أن يساعد نظام كشف سوء السلوك في الشبكة استناداً إلى حركة الشبكة في كشف الهجمات السيبرانية.

المبادئ التوجيهية للتنفيذ

ينبغي لنظام كشف سوء سلوك الشبكة أن يراقب ويفحص جميع الرسائل بين عميل أدوات النفاذ عن بُعد (RAT) ومخدم أدوات النفاذ عن بُعد. بالإضافة إلى ذلك، ينبغي لنظام الكشف أن يراقب ويفحص أيضاً جميع الرسائل الواردة من الجهاز الذي يدير مخدم أدوات النفاذ عن بُعد إلى أي أجهزة أخرى في نظام تحكم موصول بالإنترنت. ومن ثم، ينبغي وضع نظام الكشف في نفس

الشبكة الفرعية التي يوجد فيها مخدم أدوات النفاذ عن بُعد، وينبغي أن يجمع الحركة من جهاز الشبكة الذي يشكل المنفذ المفعَّل المعبِّر عن السياسة المرعية. ففي شبكة كتلك المبينة في الشكل 2 مثلاً، يفعَّل المنفذ المعبِّر عن السياسة المرعية لبدالة الشبكة في الشبكة الميدانية ويجمع نظام الكشف الحركة من السطح البيني الذي يفعَّل فيه المنفذ المعبِّر عن السياسة المرعية.

وعند تطبيق أسلوب اتصالات آمن مثل أمن بروتوكول الإنترنت (IPsec) أو طبقة المقبس الآمن للشبكة الخاصة الافتراضية (SSL VPN) أو الاتصالات عبر أمن طبقة النقل (TLS)، ينبغي وضع جهاز أمني يقدم قناة اتصالات آمنة في محيط الشبكة الفرعية حيث يوجد مخدم أدوات النفاذ عن بُعد (RAT). فعلى سبيل المثال، ينبغي وضع جهاز شبكة افتراضية خاصة قبل جهاز الشبكة بحيث يتمكن نظام كشف سوء سلوك الشبكة من التحقق من جميع الرزم.

ويمكن تصنيف أسلوب الكشف في ثلاثة أنواع مثل الكشف الساكن وكشف سوء الاستعمال وكشف الشذوذ. وبالنسبة للبيئة المشغلة لأدوات النفاذ عن بُعد، ينبغي اعتماد مزيج من كشف سوء الاستعمال وكشف الشذوذ لكشف الهجمات المعروفة والهجمات المجهولة.

4.3.8 تشكيلة الشبكة الآمنة

التحكم الأمني

ينبغي للشبكة التي يركَّب فيها مخدِّم أدوات النفاذ عن بُعد أن تجزَّأ وتُفرز على النحو الصحيح.

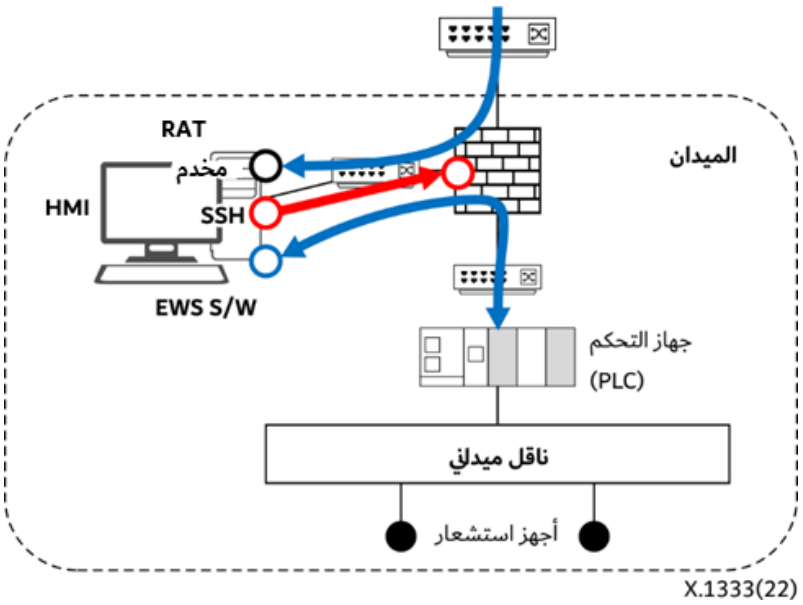
الغرض

تجزئة الشبكة هي تقسيم الشبكة إلى عدة شبكات أصغر، في حين أن فرز الشبكة هو إنفاذ السياسة المرعية للتحكم في الاتصال بين الجهات المضيفة. وبفصل الشبكة التي يركَّب فيها مخدم أدوات النفاذ عن بُعد عن شبكات أخرى، يمكن منع المهاجم من النفاذ إلى موارد نظام التحكم الأخرى حتى لو تعرض مخدم أدوات النفاذ عن بُعد للاختراق.

المبادئ التوجيهية للتنفيذ

ينبغي فصل شبكة يركَّب فيها مخدم أدوات النفاذ عن بُعد عن شبكات أخرى في نظام تحكم، وينبغي التحكم في الاتصال من/إلى مخدم أدوات النفاذ عن بُعد وفقاً لقواعد القائمة البيضاء. ويمكن تنفيذ هذا النوع من تدابير الأمن باستخدام مفهوم المنطقة منزوعة السلاح (DMZ). ويقسم جدار الحماية شبكة فرعية تحتوي على مخدم أدوات النفاذ عن بُعد، والاتصالات المخوَّل بها حصراً، كالاتصالات 1) بين عميل أدوات النفاذ عن بُعد ومخدم أدوات النفاذ عن بُعد؛ 2) مخدم أدوات النفاذ عن بُعد وموارد أخرى في نظام التحكم؛ وذلك بناءً على القواعد المرعية في جدار الحماية. ويمكن تطبيق قائمة التحكم في النفاذ على مستوى الخدمة لقاعدة جدار الحماية. وهذا يعني أن القواعد ينبغي أن تُعرّف على أنها توليفة من عنوان بروتوكول إنترنت (IP) ورقم منفذ.

فعلى سبيل المثال، يمكن فصل السطح البيني للإنسان والآلة (HMI) في الشبكة الميدانية عن الموارد الأخرى في الشبكة الميدانية بواسطة جدار حماية كما هو موضح في الشكل 3. ويتحقق جدار الحماية من جميع الرزم الواردة من/إلى مخدم أدوات النفاذ عن بُعد (RAT) طبقاً لقواعده، وتعرَّف القواعد على أنها الخدمات التي يُسمح لها على مخدم RAT بالاتصال بالخدمات على الأجهزة الأخرى. ويُسمح للاتصال الذي تبدأه خدمة برمجيات محطة العمل الهندسية (EWS) على السطح البيني للإنسان والآلة (HMI) بالوصول إلى جهاز التحكم (أي وحدة التحكم القابلة للبرمجة (PLC) في الشكل 3). وفي المقابل، يقوم جدار الحماية بحظر الاتصال الذي يستهله درع آمن (SSH) على السطح البيني للإنسان والآلة (HMI).



الشكل 3 – تجزئة الشبكة وفرزها باستعمال أدوات النفاذ عن بُعد (RAT) في شبكة ميدانية

4.8 المبادئ التوجيهية لأمن سجلات التدقيق

1.4.8 التسجيل

التحكم الأمني

ينبغي تسجيل الأحداث المتعلقة بأمن النظام والشبكة وحماية السجلات.

الغرض

تقع سجلات أحداث أمن النظام والشبكة في صميم إدارة أمن أي نظام. ومن خلال استعراض الأحداث ذات الصلة بالأمن وتحليلها، يمكن كشف الإشكالات الأمنية في الوقت المناسب. وبالتالي، كلما زادت تفاصيل سجلات الأحداث التي يولدها مخدم أدوات النفاذ، زادت سهولة كشف المنظمة للإشكالات الأمنية.

المبادئ التوجيهية للتنفيذ

تقدم بعض برمجيات أدوات النفاذ عن بُعد القدرة على تسجيل أغنى بالتفاصيل مثل استعمال كل تطبيق ومعالجة البيانات في جهاز المخدّم، في حين توزِّد برمجيات أخرى قدرة سجلات بسيطة كالتوصيل بمخدم أدوات النفاذ عن بُعد (RAT) أو فصل التوصيل عنه. وبالتالي، ينبغي لأي منظمة أن تنظر في مستوى تفاصيل سجلات أحداث الأمن المتولدة عن برمجيات RAT عند اختيار برمجيات RAT.

وإذا قدمت برمجيات أدوات النفاذ عن بُعد قدرة تسجيل بسيطة، ينبغي للمنظمة أن تنظر أيضاً في قدرة التسجيل لنظام التشغيل عند تركيب مخدم أدوات النفاذ عن بُعد. ولذلك، ينبغي فصل حسابات المستعملين عن بُعد في جهاز المخدم عن الحسابات الأخرى. وفي هذه الحالة، ينبغي لمسؤول الأمن أن يستعرض الأحداث الأمنية التي يسجلها حساب المستعمل عن بُعد لكشف سوء السلوك.

وبالإضافة إلى سجل أحداث النظام، ينبغي إنشاء سجل أحداث الشبكة أيضاً. وينبغي تسجيل جميع طلبات توصيل أدوات النفاذ عن بُعد (RAT) ونتائجها (أي النجاح أو الفشل). وعلاوة على ذلك، ينبغي أيضاً تسجيل جميع الأحداث المتعلقة ببروتوكولات التوصيل عن بُعد (مثل بروتوكولات المطاريف وبروتوكولات التحكم الصناعي وبروتوكول رسالة التحكم في الإنترنت (ICMP)). وكما ذكر أعلاه، في المرحلة الأولى من الهجوم، يقوم الخصوم عادة باستطلاع النظام. ويمكن استعمال بروتوكولات التوصيل عن

بُعد المختلفة للاستطلاع. لذا، ستساعد سجلات أحداث الشبكة المسؤولين الأمنيين في كشف سوء سلوك مخدم أدوات النفاذ عن بُعد (RAT).

وينبغي تخزين السجلات المتولدة بشكل آمن في مخدم السجل. فإذا خُزنت السجلات في التخزين المحلي للنظام، يمكن أن يتمكن المهاجمون من التلاعب بالسجلات أو الإضرار بها. وبالتالي، ينبغي تخزين سجلات الأحداث في مخدم سجلات منفصل.

وينبغي لمدير الأمن استعراض السجل وتحليله بانتظام.

5.8 العلاقة بين التهديدات الأمنية والضوابط الأمنية

يبين الجدول 1 العلاقة بين التهديدات الأمنية والضوابط الأمنية حيث تشير دائرة مفتوحة في الخلية إلى ضرورة تنفيذ تحكم أمني معين للتخفيف من حدة التهديد المحدد.

الجدول 1 – العلاقة بين التهديدات الأمنية والضوابط الأمنية

		1.7 العملاء						2.7 المخدمات		3.7 الشبكات	
		التهديد 1	التهديد 2	التهديد 3	التهديد 4	التهديد 5	التهديد 6	التهديد 7	التهديد 8	التهديد 9	التهديد 10
العملاء	1.1.8 تحديث البرمجيات	O									
	2.1.8 سلامة البرمجيات	O	O								
	3.1.8 التشكيلة الآمنة	O	O	O							
	4.1.8 التحكم في نفاذ المستعمل				O		O				
	5.1.8 الأمن المادي						O				
المخدمات	1.2.8 استيقان المستعمل								O		
	2.2.8 تخويل المستعمل						O				
	3.2.8 معاودة الاستيقان الدورية						O				
	4.2.8 تحديث البرمجيات							O			
الشبكات	1.3.8 التحكم في النفاذ إلى الشبكة									O	
	2.3.8 معاودة الاستيقان الدورية								O	O	
	3.3.8 كشف سوء السلوك					O				O	O
	4.3.8 تشكيلة الشبكة الآمنة										O
المراجعة	1.4.8 التسجيل					O					

التذييل I

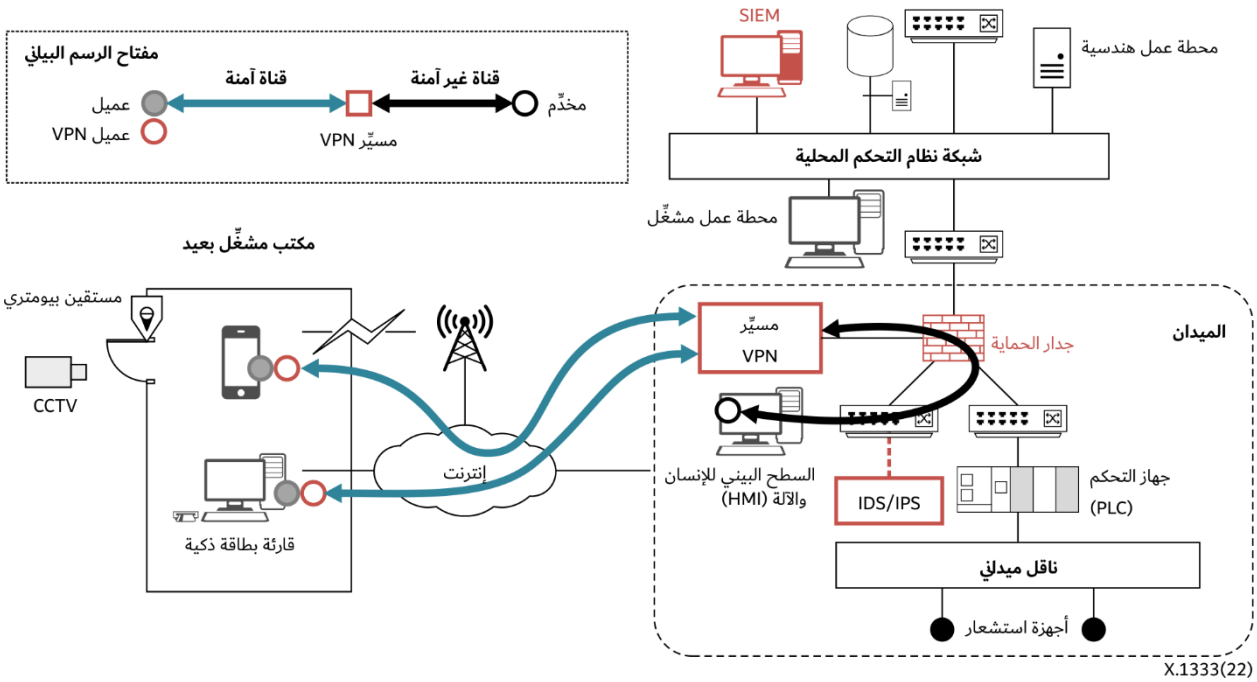
مثال تشكيلة آمنة لأدوات النفاذ عن بُعد في مورد طاقة مستدامة

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

1.I لمحة عامة عن النظام

تركَّب العديد من أجهزة الاستشعار والمفعلات في المولدات. وتقدم أجهزة الاستشعار البيانات المقيسة للتحكم بالأجهزة (مثل PLC في الشكل 1.I)، ويراقب المشغلون حالة المولدات القائمة على البيانات باستعمال السطح البيني للإنسان والآلة (HMI) أو محطة العمل الهندسية. ووفقاً للحالة، يتحكم المشغلون في المفعِّلات عبر السطح البيني للإنسان والآلة (HMI) (أو محطة العمل الهندسية) ووحدة التحكم القابلة للبرمجة (PLC). فعلى سبيل المثال، عندما يهب إعصار، سيوقف المشغلون دوران شفرات عنفات الرياح. وتسمى الشبكة التي توصل أجهزة الاستشعار والمفعلات وأجهزة التحكم *شبكة ميدانية*. وفي الشبكة الميدانية، يركَّب عادة السطح البيني للإنسان والآلة (HMI) من أجل مراقبة المولدات والتحكم فيها.

ويقوم المشغلون عن بُعد في بعض الظروف بتشغيل مولدات تستعمل موارد الطاقة المستدامة، مثل الرياح (عنفات الرياح) و(خلايا وقود) الهيدروجين، و(الخلايا الكهرضوئية) الشمسية. ويراقب المشغلون عن بُعد حالة المولدات ويتحكمون فيها لتوليد الكهرباء بكفاءة.



الشكل 1.I – مثال شبكة آمنة لنظام تحكم في مورد طاقة مستدام

2.I التشكيلة آمنة

يبين الشكل 1.I مثالاً على تشكيلة شبكة آمنة لمورد طاقة مستدام. وفي سائر أجزاء هذه الفقرة، سيرد وصف تدابير الأمن لكل مكون، وهي تشمل عميل أدوات النفاذ عن بُعد ومخدم أدوات النفاذ عن بُعد والشبكة وسجل الأحداث الأمنية.

1.2.I عميل أدوات النفاذ عن بُعد (RAT)

يصار إلى إنشاء حساب منفصل لعميل أدوات النفاذ عن بُعد (RAT)، والنفاذ إلى برمجيات العميل عن طريق الحساب حصراً.

وعندما يقوم مشغل بعيد بتشغيل برمجيات عميل أدوات النفاذ عن بُعد (RAT)، تبدأ عمليات التحقق من التحديث والتحقق من السلامة، ويطبق التحديث قبل بدء برمجيات عميل RAT.

ويتحقق عميل التحكم في النفاذ إلى الشبكة من المستوى الأمني للجهاز ويحظر التوصيل بالإنترنت إذا ما فُقدت أي تشكيلة أمنية. فعلى سبيل المثال، إن لم تعمل برمجيات مكافحة الفيروسات وجدار الحماية الشخصي، لا يسمح التحكم في النفاذ إلى الشبكة (NAC) بأي توصيل لاتصالات.

وتشغَّل جميع الأجهزة التي تشغِّل عملاء أدوات النفاذ عن بُعد في مكتب المشغلين عن بُعد. وينفَّذ التحكم في النفاذ للمكتب باستعمال مستيقن بيومتري (مثل التعرف على بصمات الأصابع أو الوجه) وتُركب كاميرا تعمل بالدارة التليفزيونية المغلقة (CCTV) أمام باب المكتب.

2.2.I مخدم أدوات النفاذ عن بُعد

عندما يحاول المشغلون عن بُعد إقامة توصيل لأدوات النفاذ عن بُعد (RAT) عبر عميل أدوات النفاذ عن بُعد، يُتطلب الاستيقان بعاملين (أي كلمة مرور وبطاقة ذكية). وبالإضافة إلى ذلك، تُستعمل عناوين بروتوكول الإنترنت الساكنة لمسيِّر الشبكة الافتراضية الخاصة ومخدم أدوات النفاذ عن بُعد.

وقبل الاستيقان المتبادل، يصطفى المضيف الذي يطلب التوصيل من خلال عنوان IP وعنوان MAC الخاصين به في مسيِّر الشبكة الافتراضية الخاصة (VPN). وبالإضافة إلى ذلك، يبلغ عمر قناة الاتصال بين عميل VPN ومسيِّر VPN 8 ساعات. وهكذا يتعين على المشغلين عن بُعد تقديم كلمة المرور والبطاقة الذكية الخاصة بهم مرة أخرى لتوصيل الشبكة الافتراضية الخاصة كل 8 ساعات.

وتُفصل حسابات المشغلين عن بُعد في السطح البيني للإنسان والآلة (HMI) عن الحسابات الأخرى للحد من أذونات المشغلين عن بُعد وإنشاء سجلات تفصيلية للحسابات.

3.2.I الشبكة

يحمي أمن بروتوكول الإنترنت للشبكة الافتراضية الخاصة في بروتوكول الإنترنت (IPsec VPN) قناة الاتصالات بين عميل أدوات النفاذ عن بُعد (RAT) ومخدم. وقبل التوصيل بمخدم أدوات النفاذ عن بُعد، ينبغي لعميل الشبكة الافتراضية الخاصة (VPN) المركَّب في جهاز مشغل بعيد أن ينشئ قناة آمنة مع مسيِّر شبكة افتراضية خاصة. ولتقديم الحد الأدنى من مستوى الأمن بطول 128 بتة، يُستعمل طاقم *التجفير B-GCM-256*، من أجل أمن بروتوكول الإنترنت للشبكة الافتراضية الخاصة في بروتوكول الإنترنت على النحو الوارد في المرجع [b-IETF RFC 6379]. وفي استيقان الإصدار الثاني من تبادل مفاتيح الإنترنت (IKEv2)، يُطبَّق توقيع *ECDSA-256* من أجل أمن بروتوكول الإنترنت للشبكة الافتراضية الخاصة في بروتوكول الإنترنت على النحو الوارد في المرجع [b-IETF RFC 6380]. وسعياً إلى تحقيق التوازن بين الأمن والمعلومات الخدمية، يُضبط عمر مفتاح IKE SA لمدة 24 ساعة ويُضبط عمر المفتاح IPsec SA لمدة 8 ساعات.

وتنقسم شبكة هذا المجال إلى جزأين، من قبيل منطقة منزوعة السلاح (DMZ) من أجل السطح البيني للإنسان والآلة (HMI) وشبكة ميدانية من أجل وحدات التحكم القابلة للبرمجة (PLC) وأجهزة الاستشعار والمفعلات. وبالإضافة إلى ذلك، يقع جدار الحماية بين الشبكة المحلية لنظام التحكم والشبكة الميدانية والمنطقة منزوعة السلاح (DMZ) لفصل الشبكات. وهكذا، يُسمح بنقل الاتصالات من محطة العمل الهندسية (EWS) على السطح البيني للإنسان والآلة إلى الشبكة الميدانية، ولكن جدار الحماية يمنع أي حركة أخرى من السطح البيني للإنسان والآلة إلى أي شبكة أخرى.

ويُثبّت نظام كشف الاقتحام (IDS) أو أمن IPS في منطقة منزوعة السلاح (DMZ) ويستقبل حركة الشبكة الواردة والصادرة من منفذ تبديل مشكَّل لاستنساخ الحركة.

4.2.I سجل الأحداث الأمنية

تسجَّل الأحداث الأمنية الناشئة عن حسابات النفاذ عن بُعد ضمن السطح البيني للإنسان والآلة (HMI) وترسَل إلى نظام معلومات الأمن وإدارة الأحداث (SIEM). وسيقوم المدير الأمني للمنظمة التي تشغل مورد الطاقة المستدام باستعراض السجلات دورياً باستعمال نظام SIEM.

بيبليوغرافيا

[b-ITU-T X.1197] Recommendation ITU-T X.1197 (2012), *Guidelines on criteria for selecting cryptographic algorithms for IPTV service and content protection*.

[b-IEC 61924-2] IEC 61924-2:2012, *Maritime navigation and radiocommunication equipment and systems - Integrated navigation systems – Part 2: Modular structure for INS - Operational and performance requirements, methods of testing and required test results.*

[b-IETF RFC 6379] IETF RFC 6379 (2011), *Suite B Cryptographic Suites for IPsec*.

[b-IETF RFC 6380] IETF RFC 6380 (2011), *Suite B Profile for Internet Protocol Security (IPsec).*

[b-Kruglov et al.] Kirill Kruglov, Evgeny Goncharov (2018), *Threats posed by using RATs in ICS*, Technical Report, Kaspersky Lab ICS CERT. https://ics-cert.kaspersky.com/reports/2018/09/20/threats-posed-by-using-rats-in-ics/

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2022