ITUPublications
Recommandations

Union internationale des télécommunications
Secteur de la normalisation

Recommandation

UIT-T X.1333 (2022) Cor. 1 (09/2023)

SÉRIE X: Réseaux de données, communication entre systèmes ouverts et sécurité

Applications et services sécurisés (2) – Sécurité des réseaux électriques intelligents

---

Lignes directrices sur la sécurité pour l'utilisation d'outils d'accès à distance dans les systèmes de contrôle connectés à l'Internet

Corrigendum 1

RECOMMANDATIONS UIT-T DE LA SÉRIE X

Réseaux de données, communication entre systèmes ouverts et sécurité

RÉSEAUX PUBLICS DE DONNÉES	X.1-X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200-X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300-X.399
SYSTÈMES DE MESSAGERIE	X.400-X.499
ANNUAIRE	X.500-X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600-X.699
GESTION OSI	X.700-X.799
SÉCURITÉ	X.800-X.849
APPLICATIONS OSI	X.850-X.899
TRAITEMENT RÉPARTI OUVERT	X.900-X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	X.1000-X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	X.1100-X.1199
SÉCURITÉ DU CYBERESPACE	X.1200-X.1299
APPLICATIONS ET SERVICES SÉCURISÉS (2)	X.1300-X.1499
Communications d'urgence	X.1300-X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310-X.1319
Sécurité des réseaux électriques intelligents	**X.1330-X.1339**
Courrier certifié	X.1340-X.1349
Sécurité de l'Internet des objets (IoT)	X.1350-X.1369
Sécurité des systèmes de transport intelligents	X.1370-X.1399
Sécurité de la technologie des registres distribués (DLT)	X.1400-X.1429
Sécurité des applications (2)	X.1450-X.1459
Sécurité de la toile (2)	X.1470-X.1489
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	X.1500-X.1599
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	X.1600-X.1699
COMMUNICATIONS QUANTIQUES	X.1700-X.1729
SÉCURITÉ DES DONNÉES	X.1750-X.1799
SÉCURITÉ DES IMT-2020	X.1800-X.1819

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1333

Lignes directrices sur la sécurité pour l'utilisation d'outils d'accès à distance dans les systèmes de contrôle connectés à l'Internet

Corrigendum 1

Résumé

Les outils d'accès à distance (RAT) sont largement utilisés sur les systèmes de contrôle pour les activités de surveillance, de contrôle et de maintenance afin de réduire les coûts de maintenance et de limiter le plus possible le délai d'intervention en cas de dysfonctionnement. Les outils RAT offrent la capacité de manipuler les systèmes de contrôle à distance mais, dans le même temps, une configuration non sécurisée des outils RAT et des vulnérabilités dans ces outils pourraient sensiblement accroître la surface d'exposition aux attaques des systèmes de contrôle. Le problème le plus grave se pose dans le cas d'une interface d'accès au système de contrôle via les réseaux extérieurs, qui pourrait permettre aux auteurs d'une attaque d'accéder au système de contrôle par le biais de l'Internet.

La Recommandation UIT-T X.1333 décrit un ensemble de mesures visant à promouvoir l'utilisation des outils RAT en toute sécurité pour les activités de surveillance, de contrôle et de maintenance. Elle identifie les menaces qui pèsent sur la configuration du réseau en raison de l'utilisation des outils RAT et fournit des lignes directrices sur la sécurité pour adapter une configuration sécurisée et des mesures de sécurité en vue de l'utilisation des outils RAT dans des systèmes de contrôle connectés à l'Internet.

Il serait souhaitable que les fournisseurs de services numériques qui exploitent des systèmes de contrôle mettent en place des contrôles de sécurité correctement organisés pour l'utilisation des outils RAT, ceci afin de réduire la surface d'exposition aux attaques et de contenir les menaces provenant des réseaux extérieurs. Il semblerait également judicieux d'harmoniser les niveaux de sécurité entre les pays développés et les pays en développement, dans la mesure où il ne s'agit pas d'un problème local mais d'un problème mondial.

Le Corrigendum 1 vise à corriger des erreurs aux paragraphes 4, 8.1.4 et 8.3.1.

Historique [*]

Édition	Recommandation	Approbation	Commission d'études	ID unique
1.0	UIT-T X.1333	07-01-2022	17	11.1002/1000/14798
1.1	UIT-T X.1333 (2022) Cor. 1	08-09-2023	17	11.1002/1000/15523

Mots clés

Système de contrôle, ligne directrice, outil d'accès à distance, sécurité.

[*] Pour accéder à la Recommandation, reporter cet URL https://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1333

Lignes directrices sur la sécurité pour l'utilisation d'outils d'accès à distance dans les systèmes de contrôle connectés à l'Internet

Corrigendum 1

Note rédactionnelle: La présente publication contient le texte intégral de la Recommandation. Les modifications apportées dans le présent Corrigendum sont présentées en marques de révision par rapport à la Recommandation UIT-T X.1333 (2022).

1 Domaine d'application

La présente Recommandation fournit des lignes directrices sur la sécurité pour l'utilisation d'outils d'accès à distance (RAT) dans les systèmes de contrôle connectés à l'Internet sur les réseaux de télécommunication. Elle couvre les sujets suivants:

- l'identification des menaces contre la configuration non sécurisée des outils RAT et de leur impact sur les systèmes de contrôle connectés à l'Internet;
- les contrôles de sécurité et leur raison d'être en faveur de la configuration sécurisée des outils RAT;
- la mise en place des lignes directrices pour chaque contrôle de sécurité; et
- un exemple de configuration sécurisée des outils RAT dans l'Appendice I.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une recommandation.

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise le terme suivant défini ailleurs:

3.1.1 interface homme-machine (HMI) [b-IEC 61924-2]: partie d'un système avec laquelle un opérateur interagit. L'interface est l'ensemble des moyens par lesquels les utilisateurs interagissent avec une machine, un appareil et un système. Elle fournit des moyens d'entrée, permettant aux utilisateurs de contrôler le système, et de sortie, permettant au système d'informer les utilisateurs.

3.2 Termes définis dans la présente Recommandation

Aucun.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

API automate programmable industriel (*programmable logic controller*)

DDoS déni de service réparti (*distributed denial of service*)

DMZ zone démilitarisée (*demilitarized zone*)

DNS service de noms de domaine (*domain name service*)

DoS déni de service (*denial of service*)

EWS poste de travail d'ingénierie (*engineering workstation*)

HMI interface homme-machine (*human machine interface*)

ICMP protocole de messagerie de commande Internet (*Internet control message protocol*)

IDS système de détection des intrusions (*intrusion detection system*)

IPsec sécurité du protocole Internet (*Internet protocol security*)

LAN réseau local (*local area network*)

MAC commande d'accès au support (*media access control*)

MDM gestion des dispositifs mobiles (*mobile device management*)

~~MDMS système de gestion des données de comptage (*meter data management system*)~~

NAC contrôle d'accès au réseau (*network access control*)

NFC communication en champ proche (*near field communication*)

PIN numéro personnel d'identification (*personal identification number*)

RAT outil d'accès à distance (*remote access tool*)

RFID identification par radiofréquence (*radio frequency identification*)

SIEM gestion des informations et des événements de sécurité (*security information and event management*)

SSH connecteur sécurisé (*secure shell*)

SSL couche de connexion sécurisée (*secure socket layer*)

TLS sécurité dans la couche transport (*transport layer security*)

URL localisateur uniforme de ressources (*uniform resource locator*)

VM machine virtuelle (*virtual machine*)

VPN réseau privé virtuel (*virtual private network*)

5 Conventions

La présente Recommandation utilise les conventions suivantes:

Le terme "**devrait**" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire.

Le terme "**pourra**" indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée.

Dans le corps de la présente Recommandation, les mots "**peut**" et "**pourrait**" apparaissent à quelques occasions. Ils doivent alors être interprétés comme "**est en mesure de**" ou "**était en mesure de**".

Lorsque les termes "**doit**" et "**devrait**" et l'expression du futur apparaissent dans l'Appendice I, elles doivent être interprétées comme étant dépourvues d'intention normative.

6 Aperçu – Les outils d'accès à distance dans les systèmes de contrôle connectés à l'Internet

Les systèmes de contrôle sont utilisés pour atteindre un objectif industriel tel que la fabrication et le transport de matière ou d'énergie. Le système de contrôle a pour objet de garantir le résultat souhaité ou la performance de l'objectif industriel. Pour assurer la performance du système de contrôle, les opérateurs recueillent les informations et les données des capteurs dans les réseaux sur le terrain (voir la Figure 1). Sur la base de ces données et informations, les opérateurs pourront contrôler le système si nécessaire. Pour maintenir le système de contrôle ou venir à bout de problèmes techniques, les ingénieurs de maintenance d'un fournisseur de système de contrôle pourront accéder au système de contrôle.

Les outils d'accès à distance (RAT) sont largement utilisés sur les réseaux industriels pour la surveillance, le contrôle et la maintenance des systèmes de contrôle afin de réduire les coûts de maintenance et de minimiser le temps de réponse en cas de dysfonctionnement. Selon un rapport [b-Kruglov et al.], au premier semestre 2018, les outils RAT étaient utilisés sur 31,6% des ordinateurs du système de contrôle, et ce nombre n'incluait pas le nombre de connexions sur des postes de travail distants.

Dans la majorité des cas, les outils RAT sont utilisés pour:

- suivre/contrôler une interface homme-machine (HMI) depuis un poste de travail de l'opérateur;
- suivre/contrôler une interface homme-machine (HMI) depuis un poste de travail d'ingénierie;
- connecter plusieurs opérateurs sur un seul poste de travail de l'opérateur;
- connecter des opérateurs distants sur un poste de travail de l'opérateur via un réseau externe; et
- assurer la maintenance d'un système de contrôle connecté à l'Internet depuis l'ordinateur d'un ingénieur de maintenance d'un fournisseur de système de contrôle via un réseau externe.

Ces cas d'utilisation montrent que le recours aux outils RAT pour la surveillance, le contrôle et la maintenance du système de contrôle pourrait être un critère indispensable au fonctionnement de ces systèmes. Leur utilisation réduirait également les coûts de maintenance. Il pourrait être possible, par exemple, de réduire le nombre de licences pour le logiciel HMI dans les trois premiers cas d'utilisation mentionnés ci-avant. De plus, des appareils intelligents récents pourraient aussi être utilisés comme clients RAT. Les clients finals peuvent ainsi surveiller et contrôler leurs systèmes photovoltaïques (PV) via un outil RAT sur leur smartphone.

La Figure 1 donne un aperçu schématique de la configuration d'utilisation des outils RAT dans les systèmes de contrôle connectés à l'Internet, sur la base des cas d'utilisation.

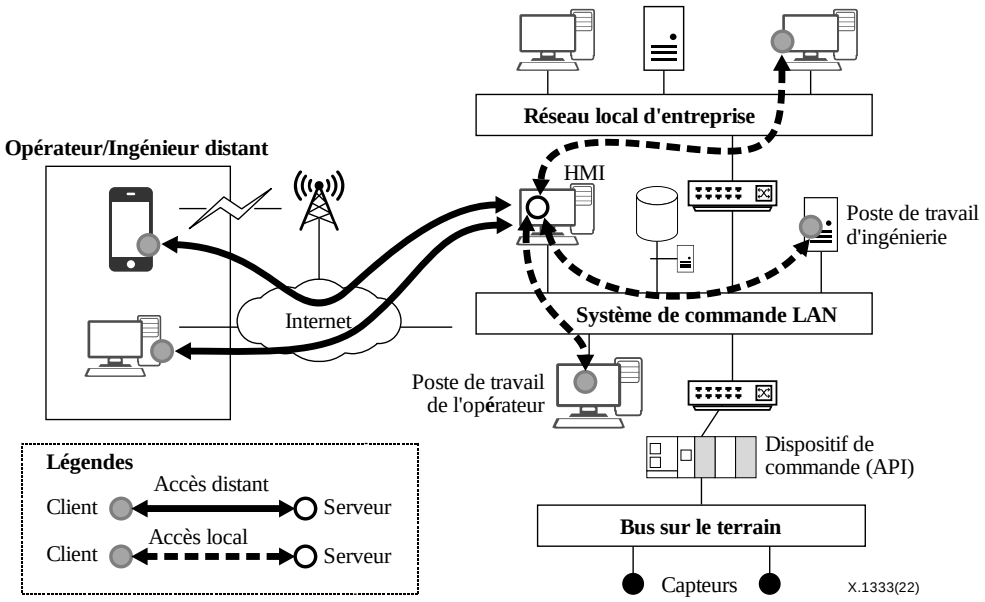

Figure 1 – Configuration du réseau pour l'utilisation des outils RAT dans les systèmes de contrôle connectés à l'Internet

Dans d'autres cas, une organisation exploitant un système de contrôle pourrait associer un système de contrôle de petite taille aux systèmes de contrôle existants. Un site qui possède un groupe électrogène à alimentation générale, par exemple, pourrait utiliser un nouveau système de pile à combustible pour augmenter sa capacité en énergie propre. Ces systèmes de pile à combustible comprennent des ordinateurs HMI, des dispositifs de commande, des capteurs, des batteries et d'autres systèmes. Dans cet exemple, un dispositif HMI et des dispositifs de commande pourraient être connectés au même sous-réseau du système de pile à combustible côté terrain. La Figure 2 présente la configuration d'utilisation des outils RAT pour accéder à un dispositif HMI sur le terrain.

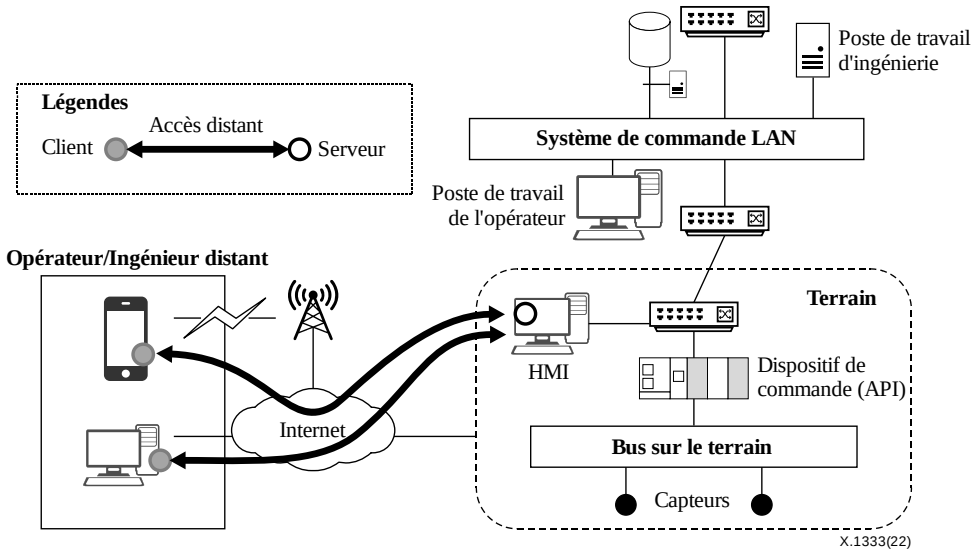

Figure 2 – Configuration du réseau pour l'utilisation des outils RAT dans le réseau sur le terrain des systèmes de contrôle connectés à l'Internet

Les outils RAT offrent la possibilité de manipuler les systèmes de contrôle à distance et permettent de réduire les coûts de maintenance. Toutefois, dans le même temps, ils pourraient augmenter considérablement la surface d'exposition aux attaques de ces systèmes s'ils ne sont pas configurés de

manière sécurisée ou présentent des vulnérabilités. Le problème le plus grave est qu'un outil RAT peut être utilisé comme interface pour accéder au système de contrôle connecté à l'Internet depuis les réseaux extérieurs, généralement accessibles depuis l'Internet. Si des adversaires parvenaient à compromettre un client RAT sur un système de contrôle connecté à l'Internet, ils pourraient alors provoquer un dysfonctionnement du système. Il est par ailleurs difficile de détecter leurs activités. C'est pourquoi la présente Recommandation se concentre sur les connexions RAT provenant de l'extérieur des systèmes de contrôle connectés à l'Internet.

7 Menaces pour l'utilisation des outils RAT dans les systèmes de contrôle connectés à l'Internet

7.1 Menaces pour les clients RAT

Un client RAT pourrait être installé sur un ordinateur client dans un endroit distant ou sur un appareil mobile appartenant à un opérateur distant ou à un ingénieur de maintenance à distance. L'emplacement distant pourrait se trouver en dehors de la protection physique de l'organisation et de la protection logique du pare-feu de l'organisation. Les ordinateurs clients ne pourraient être par ailleurs pas bien gérés lorsque les ordinateurs de l'organisation sont étroitement surveillés et solidement verrouillés. Ainsi, un certain nombre de menaces pour l'utilisation des outils RAT pourrait provenir des ordinateurs sur lesquels le client RAT est installé.

Les menaces suivantes pour les ordinateurs client et les clients RAT devraient être prises en compte:

- (M1) L'auteur d'une attaque pourrait exploiter les vulnérabilités des ordinateurs clients ou des clients RAT pour compromettre les ordinateurs clients ou les clients RAT. Une fois que les auteurs d'attaque obtiennent le contrôle total de l'ordinateur client ou du client RAT, ils pourraient se connecter au système de contrôle via le RAT.
- (M2) Un adversaire pourrait exploiter la tunnélisation divisée dans un ordinateur client. Les ordinateurs clients sont généralement connectés non seulement aux serveurs RAT, mais également à tout autre système connecté à l'Internet. Ainsi, un adversaire qui obtient le contrôle total de l'ordinateur client peut transmettre des informations essentielles obtenues depuis le système de contrôle via une connexion Internet non protégée.
- (M3) L'auteur d'une attaque pourrait installer des logiciels malveillants ciblés sur un ordinateur client, identifier les informations sensibles (par ex. identité de connexion et mot de passe) et exfiltrer ces informations. Une fois que les auteurs d'attaque obtiennent ces informations, ils peuvent accéder au serveur RAT en utilisant un client RAT installé sur n'importe quelle autre machine plutôt que l'ordinateur client.
- (M4) L'auteur d'une attaque pourrait conduire une attaque en force brute, une attaque par dictionnaire ou casser les mots de passe au moyen d'outils à code source ouvert pour accéder au serveur RAT.
- (M5) Les adversaires pourraient dissimuler leurs activités sur les ordinateurs client en supprimant les données du journal. L'organisation qui possède un système de contrôle ne pourra donc pas suivre les activités de l'adversaire lorsque l'organisation enquêtera sur l'incident.
- (M6) Un adversaire pourrait exploiter l'accès physique aux ordinateurs client.

7.2 Menaces pour les serveurs RAT

Un serveur RAT pourrait être installé sur une interface HMI dans un système de contrôle connecté à l'Internet. À partir du moment où le serveur ouvre un service connecté à l'Internet, un adversaire pourrait exploiter l'accès à ce service. Si ce service n'est pas correctement protégé, l'adversaire pourrait accéder au système de contrôle par son biais.

Les menaces suivantes pour les ordinateurs client et les clients RAT devraient être prises en compte:

- (M7) L'auteur d'une attaque pourrait exploiter les vulnérabilités d'un serveur RAT ou d'une machine sur laquelle le serveur RAT est installé pour compromettre cette machine ou le serveur RAT. Ce type d'attaque pourrait conduire à une prise de contrôle totale du système de contrôle par l'auteur de l'attaque. Ainsi, à partir du moment où ils accèdent à la machine ou au serveur RAT, les auteurs d'attaque pourraient obtenir davantage de droits sur le dispositif ou le contrôle total du serveur RAT.
- (M8) Un adversaire pourrait mener des attaques par déni de service réparti (DDoS) et par déni de service (DoS) contre le serveur RAT.

7.3 Menaces pour le canal de communication entre le client et les serveurs

Sachant que le serveur et le client RAT sont connectés via l'Internet dans un système de contrôle connecté à l'Internet, le canal de communication peut être accessible à tous. Si les communications ne sont pas cryptées ou sont chiffrées au moyen de méthodes faibles contenant des vulnérabilités connues du public, un adversaire pourrait en tirer parti pour accéder aux canaux et aux informations transférées.

Les menaces suivantes pour les ordinateurs client et les clients RAT devraient être prises en compte:

- (M9) Un adversaire pourrait exploiter les failles de la communication non protégée pour obtenir des informations sensibles (telles qu'identité de connexion et mot de passe) et utiliser ces informations pour accéder au serveur RAT. Il pourrait en être de même lorsque le canal de communication est protégé avec une crytographie faible. S'ils parviennent à accéder au serveur RAT, les adversaires pourraient prendre le contrôle total du système de contrôle.
- (M10) L'auteur d'une attaque pourrait tirer avantage d'un protocole faible contenant des vulnérabilités connues du public et obtenir l'accès au serveur RAT ou provoquer un refus de service pour les utilisateurs des serveurs RAT.

8 Lignes directrices sur la sécurité pour l'utilisation d'outils d'accès à distance dans les systèmes de contrôle connectés à l'Internet

8.1 Lignes directrices sur la sécurité pour les clients RAT

8.1.1 Mise à jour du logiciel

Contrôle de sécurité

Le logiciel RAT, le système d'exploitation et tout autre logiciel côté client devraient être tenus à jour.

Objet

Le logiciel pourrait présenter des vulnérabilités non connues, car les techniques d'attaque évoluent. Lorsqu'une nouvelle vulnérabilité est détectée, c'est une vulnérabilité dite "jour zéro" que les auteurs d'attaque pourraient exploiter pour compromettre le dispositif client RAT. Le nombre de vulnérabilités du logiciel RAT a récemment augmenté. En 2019, on a identifié 31 vulnérabilités pour les logiciels de type informatique virtuelle en réseau (VNC). Les vendeurs du logiciel RAT fournissent une mise à jour de sécurité lorsqu'une nouvelle vulnérabilité est détectée, permettant ainsi aux utilisateurs qui adoptent ces mises à jour d'atténuer la vulnérabilité. L'actualisation des logiciels est l'un des moyens les plus simples de maintenir la sécurité des appareils clients.

Lignes directrices sur la mise en œuvre

Pour maintenir le logiciel à jour, le plus important est de vérifier régulièrement s'il existe une nouvelle mise à jour. Malheureusement, les utilisateurs ne sont pas toujours à même d'effectuer cette vérification de manière régulière, c'est pourquoi l'approche automatique suivante devrait être envisagée pour maintenir le logiciel à jour.

a) Une vérification des mises à jour de sécurité devrait être déclenchée à chaque fois que le logiciel client RAT est exécuté.

b) S'il existe une nouvelle version du logiciel ou une nouvelle mise à jour de sécurité, celle-ci devrait être appliquée au logiciel client avant de lancer l'exécution.

c) La vérification des mises à jour de sécurité pourra aussi être déclenchée à intervalles réguliers lorsque le logiciel client RAT sera en cours d'exécution.

d) S'il existe une nouvelle version du logiciel ou une nouvelle mise à jour de sécurité, celle-ci devrait être appliquée au logiciel client lors de la fermeture.

Dans certains cas, le périphérique client RAT devrait être redémarré après installation d'un correctif de sécurité. Contrairement à un ordinateur client standard, le client RAT pour le système de contrôle n'a pas pu redémarrer à ce moment-là, car il convient que l'opérateur/ingénieur distant surveille le système de contrôle en continu. Dans ces conditions, la vérification des mises à jour de sécurité installe les mises à jour après avoir obtenu la confirmation de l'utilisateur.

De plus, le système d'exploitation et tout autre logiciel de l'appareil exploitant le logiciel client RAT devrait également être mis à jour. La capacité de mise à jour automatique des systèmes d'exploitation devrait être activée. La disponibilité des mises à jour de sécurité pour chaque application devrait être vérifiée régulièrement et les correctifs de sécurité devraient être appliqués rapidement lorsqu'ils sont disponibles.

8.1.2 Intégrité du logiciel

Contrôle de sécurité

Il convient de protéger l'intégrité du logiciel RAT côté client.

Objet

Une version modifiée du logiciel RAT pourrait être installée côté client. L'auteur d'une attaque pourrait compromettre le serveur de mise à jour ou diffuser de fausses mises à jour via un courriel hameçon. Le logiciel RAT infecté par un code malveillant se comporte normalement, mais le code malveillant œuvre pour divulguer des informations ou établir une connexion avec l'auteur d'une attaque le cas échéant. Pour prévenir le comportement anormal d'un logiciel RAT malveillant, il convient par conséquent de protéger l'intégrité du logiciel RAT.

Lignes directrices sur la mise en œuvre

Sachant que, comme mentionné ci-avant, les auteurs d'attaque peuvent diffuser le logiciel RAT malveillant via une chaîne d'approvisionnement officielle, il devient difficile pour l'utilisateur de devoir faire en sorte de savoir si le logiciel a été ou non modifié. La procédure de contrôle d'intégrité automatique devrait donc servir à protéger l'intégrité du logiciel RAT.

La procédure de contrôle d'intégrité automatique présuppose l'approche suivante:

a) La procédure de contrôle d'intégrité devrait être lancée lorsque le logiciel est exécuté ou que la procédure de mise à jour est lancée.

b) Le logiciel ou la procédure de mise à jour devrait être démarré s'il n'y a aucun indice que le logiciel a été modifié.

c) Le statut de la procédure de contrôle d'intégrité devrait être affiché sur l'écran pour que l'utilisateur sache que ce logiciel est normal.

d) La valeur d'intégrité du logiciel devrait être générée par une méthode cryptographique pour garantir que le logiciel n'est pas modifié par quelqu'un d'autre. On utilise pour cette méthode un algorithme cryptographique sécurisé.

8.1.3 Configuration sécurisée du client RAT

Contrôle de sécurité

La configuration du RAT côté client devrait être conforme à la politique de sécurité de l'organisation propriétaire du système de contrôle connecté à l'Internet.

Objet

Quand bien même le logiciel RAT comporte des options de sécurité pour la sécurisation des communications, celui-ci ne peut être utilisé de manière sécuritaire que s'il est correctement configuré. En général, les utilisateurs veulent éviter les désagréments et n'activent pas les fonctions de sécurité. Ils préfèrent utiliser un mot de passe fort. De plus, concernant la sécurité du protocole Internet (IPsec), dont l'utilisateur ne connaît pas les détails corrects de la configuration, des erreurs de configuration augmenteront les risques d'utilisation abusive du logiciel client RAT.

Lignes directrices sur la mise en œuvre

Afin de réduire les possibles erreurs de configuration du client RAT, il est préférable de configurer le client par une organisation qui exploite un système de contrôle. Les approches suivantes devraient être envisagées pour gérer la configuration des clients RAT par l'organisation.

a) Utilisation d'une adresse de protocole Internet (IP) statique pour le serveur RAT: si le localisateur uniforme de ressources (URL) est utilisé pour accéder à la passerelle de réseau privé virtuel (VPN) ou au serveur RAT, les opérateurs/ingénieurs distants risquent d'être exposés à des attaques sévères, telles que hameçonnage, usurpation d'identité du service de noms de domaine (DNS) et empoisonnement du cache DNS. Utiliser une adresse IP statique ou une adresse IP codée physiquement côté serveur permet d'atténuer ces menaces et de fournir une authentification de serveur pour les opérateurs/ingénieurs distants tout le long du canal de communication sécurisé.

b) Solution de contrôle d'accès au réseau (NAC) ou gestion des dispositifs mobiles (MDM): la solution NAC fournit des fonctionnalités pour vérifier l'état d'un ordinateur ou d'un ordinateur portable, tandis que la gestion MDM prend en charge des fonctionnalités pour vérifier et contrôler les appareils mobiles. La solution NAC aide les organisations pour inciter les opérateurs/ingénieurs distants à configurer un ordinateur fonctionnant avec un client RAT en vérifiant les configurations de l'appareil avant d'établir une connexion. Si l'appareil est mal configuré, la solution NAC interdit le trafic réseau sur l'appareil jusqu'à ce que les opérateurs/ingénieurs distants remédient aux erreurs de configuration. La solution MDM remplace la solution NAC lorsque les opérateurs distants utilisent des appareils mobiles pour accéder à un serveur RAT.

c) Image de la machine virtuelle (VM): l'organisation qui possède un système de contrôle pourra distribuer une image de la VM aux opérateurs/ingénieurs distants. Lorsque l'organisation crée l'image, toutes les configurations liées à l'appareil client, au client VPN et au client RAT devraient être configurées en fonction de la politique de sécurité de l'organisation. De plus, pour être elle-même protégée, l'image de la VM devrait être cryptée et stockée sur les appareils des opérateurs/ingénieurs distants lorsqu'elle n'est pas utilisée.

8.1.4 Contrôle de l'accès des utilisateurs à l'appareil client

Contrôle de sécurité

Seuls les utilisateurs autorisés devraient pouvoir accéder au logiciel client RAT.

Objet

Le fait de limiter l'accès du logiciel client RAT aux opérateurs/ingénieurs distants autorisés est un moyen de réduire les risques d'utilisation abusive du client RAT.

Cependant, les opérateurs/ingénieurs distants légitimes peuvent aussi interrompre temporairement l'utilisation du logiciel et donner lieu dans ce cas à des tentatives d'utilisation abusive lors de la session connectée. L'appareil devrait donc être verrouillé lorsque les opérateurs/ingénieurs distants arrêtent ou interrompent leur travail. Lorsqu'ils reviennent devant le périphérique client RAT, ces derniers peuvent reprendre leur travail en utilisant la procédure d'identification et d'authentification établie.

Lignes directrices sur la mise en œuvre

Pour mettre en œuvre ce contrôle, les opérateurs/ingénieurs distants devraient utiliser un compte différent de celui utilisé pour effectuer des tâches régulières lors de l'exécution du logiciel client RAT. En d'autres termes, un opérateur/ingénieur distant devrait avoir un autre compte distinct pour l'utilisation du client RAT, assorti par ailleurs d'un mot de passe fort.

Le verrouillage de session est un moyen efficace de résoudre le problème susmentionné. Il en existe deux types: 1) le verrouillage de session au niveau du système d'exploitation et 2) le verrouillage de session au niveau de l'application. La majorité des systèmes d'exploitation possèdent une fonction de verrouillage de session qui devrait être lancée après une période d'inactivité. ~~La~~ Toutefois, en fonction du logiciel RAT, l'existence d'une fonction de verrouillage au niveau de l'application~~, en revanche, n'est pas toujours fournie et dépend du logiciel.~~ peut être essentielle. La présence d'une fonction de verrouillage de session au niveau de l'application devrait donc être un critère ~~essentiel à prendre en compte par le système~~important pour les organisations qui exploitent des systèmes de contrôle ~~d'exploitation de l'organisation,~~ lors du choix du logiciel RAT.

8.1.5 Sécurité physique

Exigences de sécurité

Seuls les opérateurs/ingénieurs distants autorisés devraient pouvoir accéder physiquement à l'appareil sur lequel le logiciel client RAT est exécuté, et l'emplacement où les opérateurs/ingénieurs utilisent ces appareils devrait être protégé contre tout accès non autorisé.

Objet

Même si l'appareil et le logiciel client RAT sont configurés de manière sécurisée avec une fonction de sécurité en bonne et due forme, l'appareil et son emplacement devraient aussi être protégés contre tout accès non autorisé par des adversaires.

Lignes directrices sur la mise en œuvre

Afin de garantir la sécurité physique des appareils, des logiciels et de leur environnement, il convient de tenir compte de ce qui suit:

a) Le bureau où travaillent les opérateurs/ingénieurs distants devrait être protégé par un système de contrôle d'accès approprié utilisant la technologie de communication en champ proche (NFC) ou d'identification par radiofréquence (RFID). Pour une sécurité plus forte, un système de contrôle d'accès biométrique (par exemple, reconnaissance des empreintes digitales, de l'iris et du visage) pourra être envisagé.

b) Une caméra de télévision en circuit fermé devrait être installée devant la porte du bureau.

c) L'appareil sur lequel le logiciel client RAT est exécuté devrait être protégé contre le vol à l'aide d'un câble antivol ou d'autres moyens de dissuasion.

8.2 Lignes directrices sur la sécurité pour les serveurs RAT

8.2.1 Authentification de l'utilisateur

Contrôle de sécurité

Un service RAT devrait permettre aux utilisateurs d'accéder à distance aux ressources, mais seulement via une authentification à deux facteurs.

Objet

L'authentification traditionnelle par identifiant et mot de passe pourrait être rompue, et les facteurs liés à la connaissance, tels que le mot de passe ou le numéro d'identification personnel (code PIN), ne permettront pas à eux seuls de garantir que l'utilisateur qui accède dispose des autorisations appropriées.

Au niveau local, les méthodes de contrôle d'accès physique identifient et autorisent les utilisateurs légitimes à accéder aux ressources système. Par conséquent, même si l'auteur d'une attaque connaît l'identifiant et le mot de passe d'un utilisateur légitime, il n'est pas facile d'accéder directement aux ressources du système. À distance, ces méthodes physiques de sécurité et d'identification des utilisateurs sont difficilement applicables. Au lieu et place de ces méthodes de sécurité physiques, une authentification à deux facteurs pourrait réduire la possibilité d'usurpation d'identité même si l'identifiant et le mot de passe ont été volés.

Lignes directrices sur la mise en œuvre

Les facteurs d'authentification pourront inclure une chose que connaît l'entité (facteur lié à la connaissance), une chose que possède l'entité (facteur lié à la possession), une chose qu'est l'entité (facteur intrinsèque) et un endroit où est l'entité (facteur lié à la localisation). L'authentification à deux facteurs est généralement mise en œuvre aujourd'hui par le biais d'un facteur lié à la possession et d'un facteur lié à la connaissance ou d'un facteur intrinsèque et d'un facteur lié à la connaissance.

La plupart des appareils mobiles (tels que ordinateurs portables, tablettes et smartphones) utilisent aujourd'hui des données biométriques. Les facteurs intrinsèques (empreinte digitale, de l'iris ou reconnaissance faciale) pourraient donc être la meilleure option pour l'authentification à deux facteurs.

Cependant, les méthodes biométriques ne peuvent pas toujours être utilisées en toutes circonstances. Par exemple, les utilisateurs distants qui doivent porter des gants pendant les heures de travail devraient éviter d'utiliser l'empreinte digitale. Dans ce cas, ils pourraient utiliser un facteur lié à la possession comme une clé cryptographique.

La plupart des logiciels RAT permettent de limiter le temps d'attente d'authentification. Dans ce cas, le serveur RAT rejette la demande d'authentification s'il ne reçoit pas de réponse de l'utilisateur au bout d'un certain temps. Cela aide ainsi à réduire la probabilité d'attaques par déni de service.

8.2.2 Autorisation de l'utilisateur

Contrôle de sécurité

Les comptes pour les utilisateurs distants ne devraient avoir que les privilèges minimaux nécessaires pour exécuter leur fonction.

Objet

Pour limiter l'impact d'une attaque, les privilèges de l'utilisateur distant devraient être limités aux privilèges minimaux nécessaires à l'exécution de sa fonction.

Lignes directrices sur la mise en œuvre

Les logiciels RAT ne fournissent généralement pas de méthode d'autorisation précise. Ils n'offrent pour la plupart que deux types de modes: le mode lecture seule et le mode contrôle total. Par conséquent, les auteurs d'attaque qui parviendraient à accéder à un serveur RAT pourraient compromettre entièrement l'appareil. Pour éviter cela, les privilèges accordés sur les comptes des utilisateurs distants devraient être limités aux privilèges minimaux nécessaires à l'exécution de leurs fonctions.

Premièrement, un compte d'utilisateur distant ne devrait pas être un compte administrateur et aucun privilège susceptible de modifier le serveur RAT ne devrait être accordé sur ce compte. L'installation du logiciel, la configuration du système d'exploitation ou la configuration du système pourra être l'un des privilèges limités.

Deuxièmement, le contrôle d'accès pour une application devrait également être appliqué. Le compte d'utilisateur distant ne peut exécuter aucun autre logiciel, à l'exception du système de contrôle d'exploitation et de surveillance du logiciel. S'il parvient à ouvrir un programme de terminal sur la machine du serveur RAT, l'utilisateur distant pourra accéder à un autre système via le serveur RAT, ce qui serait une véritable aubaine pour les auteurs d'attaque.

8.2.3 Réauthentification périodique

Contrôle de sécurité

Un serveur RAT devrait réauthentifier les utilisateurs et les appareils client après un certain temps.

Objet

Afin de garantir que seuls les opérateurs/ingénieurs autorisés distants utilisent l'accès à distance, le serveur RAT devrait les obliger à se réauthentifier périodiquement pendant les longues sessions d'accès à distance. Cette procédure permet de garantir que les personnes non autorisées ne pourraient pas utiliser l'accès à distance même si l'appareil est volé alors qu'une connexion entre le serveur et le client RAT a été établie.

De plus, la réauthentification au niveau du réseau aide à réduire la probabilité d'être exposé à des attaques de piratage de session.

Lignes directrices sur la mise en œuvre

Le logiciel serveur RAT n'intègre pas la fonction de réauthentification après un certain temps, mais la plupart des passerelles VPN fournissent cette fonctionnalité. Pour assurer ce contrôle en bonne et due forme, il convient donc d'utiliser une passerelle VPN entre le client et le serveur RAT.

Les passerelles VPN sont également nombreuses à proposer une fonctionnalité de réauthentification du client. L'organisation devrait dans ce cas activer l'authentification de l'utilisateur ou de l'appareil après un certain temps sur la passerelle VPN. Par exemple, lorsque la communication RAT est transmise via le protocole de sécurité dans la couche transport (TLS) version 1.3, l'extension d'authentification client post-prise de contact devrait être activée. Dans cette configuration, le serveur TLS demandera l'authentification du client après avoir établi une connexion TLS.

8.2.4 Mise à jour du logiciel

Contrôle de sécurité

Le logiciel serveur RAT, le système d'exploitation et tout autre logiciel exploité par un dispositif serveur devraient être tenus à jour.

Objet

L'objet du contrôle présenté au paragraphe 8.2.4 est le même que celui spécifié au paragraphe 8.1.1.

Lignes directrices sur la mise en œuvre

Les lignes directrices décrites présentées au paragraphe 8.2.4 sont les mêmes que celles spécifiées au paragraphe 8.1.1.

8.3 Lignes directrices sur la sécurité pour les réseaux

8.3.1 Contrôle d'accès au réseau

Contrôle de sécurité

Seuls les utilisateurs autorisés devraient pouvoir accéder aux communications réseau entre le serveur et le client RAT.

Objet

L'une des premières étapes pour compromettre un service ou un système consiste à accéder à une communication réseau. Les auteurs d'attaque pourraient ainsi rassembler des informations et des données entre un client et un serveur RAT et injecter des données falsifiées dans le canal de communication, ce qui pourrait ainsi conduire à une attaque par intercepteur, une distribution de logiciels malveillants ou une attaque par déni de service. La solution pour protéger le service RAT et le système de contrôle consiste à empêcher les utilisateurs non autorisés d'accéder aux communications réseau entre le serveur et le client RAT.

Lignes directrices sur la mise en œuvre

Il existe plusieurs façons de contrôler l'accès aux communications sur le réseau et d'en protéger le contenu. Les méthodes ci-après sont des options à envisager.

- Une ligne louée pourra être utilisée pour empêcher des utilisateurs non autorisés d'accéder à la connexion ~~entre un système de gestion des données de comptage (MDMS) et des fournisseurs de services tiers~~ entre le client et le serveur RAT.
- Des méthodes de communication sécurisées, telles que IPsec et la couche de connexion sécurisée (SSL) VPN, devraient être appliquées aux communications entre le client et le serveur RAT. Le trafic RAT devrait être tunnellisé au sein d'un réseau VPN.
- Si la solution du réseau VPN ne peut être appliquée, l'accès distant devrait être réalisé via le protocole TLS version 1.3 ou supérieure.

Un algorithme cryptographique sécurisé devrait être envisagé lorsqu'une méthode de communication sécurisée, incluant VPN et TLS, est utilisée. [b-UIT-T X.1197] fournit une liste contenant des exemples d'algorithmes et de longueur de clés sécurisés. Lors de la configuration du canal de communication, une passerelle VPN ou un serveur RAT devrait rejeter une demande de connexion si l'algorithme et la longueur de clé fournis par le client ne sont pas sécurisés.

8.3.2 Authentification mutuelle au niveau du réseau

Contrôle de sécurité

La méthode d'authentification mutuelle devrait être appliquée au canal de communication entre le serveur et le client RAT.

Objet

Une méthode d'authentification mutuelle pour les canaux de communication devrait être mise en œuvre de façon à ce qu'un client RAT puisse vérifier la légitimité d'un serveur RAT avant de lui fournir des informations d'authentification. Cette méthode permet au service RAT d'éviter une attaque par intercepteur entre le client et le serveur RAT.

Lignes directrices sur la mise en œuvre

Si la communication RAT intègre les méthodes IPsec, SSL VPN ou la communication sur le protocole TLS, il convient d'utiliser à la fois le certificat du serveur et le certificat du client à des fins d'authentification mutuelle. Un client, pour authentifier un serveur, vérifie le certificat de ce dernier pour s'assurer de sa légitimité.

La plupart des solutions VPN proposent une fonction d'authentification du serveur, mais celle-ci bien souvent n'est pas activée. Ainsi, lorsqu'un système de contrôle utilise un réseau VPN pour protéger un service RAT, l'option d'authentification du serveur devrait être activée.

Par ailleurs, avec le protocole TLS, seul le serveur généralement authentifie le client en vérifiant les informations d'identification du client, comme un certificat, car l'authentification du serveur est une option. Par conséquent, si une communication entre un serveur et un client est protégée par le service TLS pour RAT, l'échange mutuel de certificats entre le serveur et le client devrait être requis.

Enfin, les fonctions d'expiration du délai d'authentification et de limitation des sessions simultanées devraient être activées. Savoir rejeter les demandes de connexion en bonne et due forme est une clé d'atténuation des attaques par déni de service.

8.3.3 Détection de comportements anormaux sur le réseau

Contrôle de sécurité

La fonction de détection des comportements anormaux devrait être appliquée au réseau sur lequel le serveur RAT est connecté.

Objet

Quand bien même plusieurs méthodes de sécurité seraient appliquées côté client RAT, il est toujours possible que l'appareil qui exécute le client RAT soit compromis. Par exemple, si les auteurs d'attaque peuvent accéder au réseau d'un système de contrôle connecté à l'Internet via un client RAT compromis, ils peuvent également accéder à toutes les ressources autorisées sur le serveur RAT. Dans ce cas de figure, seul le comportement différencie les opérateurs/ingénieurs distants et les auteurs d'attaque. Les opérateurs/ingénieurs distants connaissent le réseau et le système auquel ils se sont connectés, tandis que les auteurs d'attaque devraient avoir besoin d'effectuer une reconnaissance pour déterminer où se trouve la cible dans le réseau. Par conséquent, un système de détection des comportements normaux sur le réseau basé sur le trafic réseau pourrait aider à détecter les cyberattaques.

Lignes directrices sur la mise en œuvre

Le système de détection des comportements normaux sur le réseau devrait surveiller et examiner tous les messages entre un client RAT et le serveur RAT. De plus, tous les messages en provenance de l'appareil exécutant le serveur RAT vers tout autre appareil d'un système de contrôle connecté à l'Internet devraient également être surveillés et examinés par le système de détection. De ce fait, le système de détection devrait se situer dans le même sous-réseau qui abrite le serveur RAT et devrait collecter le trafic du dispositif de réseau dans lequel le miroir de port est activé. Par exemple, dans un réseau du type de celui qui est présenté à la Figure 2, la politique de miroir de port du commutateur de réseau sur le réseau de terrain est activée et le système de détection collecte le trafic depuis l'interface sur laquelle la politique de miroir de port est activée.

En présence d'une méthode de communication sécurisée, telle qu'IPsec, SSL VPN ou la communication sur le protocole TLS, il y a lieu de placer le dispositif de sécurité qui fournit le canal de communication sécurisé à l'intérieur du périmètre du sous-réseau où se trouve le serveur RAT. Il devrait par exemple être positionné avant le dispositif réseau de sorte que le système de détection des comportements anormaux sur le réseau puisse contrôler tous les paquets.

Il existe trois types de méthodes de détection: la détection statique, la détection des utilisations abusives et la détection des anomalies. Dans un environnement qui comporte des outils d'accès à distance, on devrait combiner les méthodes de détection des utilisations abusives et de détection des anomalies afin de repérer les attaques connues et inconnues.

8.3.4 Configuration sécurisée du réseau

Contrôle de sécurité

Un réseau sur lequel un serveur RAT est installé devrait être correctement segmenté et subdivisé.

Objet

La segmentation du réseau est la répartition d'un réseau en plusieurs réseaux de plus petite taille; la subdivision du réseau est l'application de la politique pour contrôler la communication entre les hôtes. En séparant le réseau sur lequel le serveur RAT est installé des autres réseaux, il est possible d'empêcher l'auteur d'une attaque d'accéder à d'autres ressources du système de contrôle même si le serveur RAT est fragilisé.

Lignes directrices sur la mise en œuvre

Dans un système de contrôle, le réseau sur lequel un serveur RAT est installé devrait être séparé des autres réseaux et les communications depuis/vers le serveur RAT devraient être commandées conformément aux règles de la liste blanche. Il est possible de mettre en œuvre ce type de mesure de sécurité grâce au concept de zone démilitarisée (DMZ). Un pare-feu partitionne un sous-réseau contenant le serveur RAT et seules les communications autorisées, telles que les communications 1) entre le client RAT et le serveur RAT; 2) entre le serveur RAT et d'autres ressources du système de contrôle, sont admises conformément aux règles du pare-feu. Une liste de contrôle d'accès au niveau du service pourra être appliquée pour la réglementation du pare-feu. Les règles doivent donc être définies comme la combinaison de l'adresse IP et du numéro de port.

Ainsi, l'interface HMI du réseau sur le terrain pourrait être séparée des autres ressources du réseau sur le terrain par un pare-feu, comme illustré à la Figure 3. Le pare-feu vérifie tous les paquets depuis/vers le serveur RAT en conformité aux règles établies, et les règles définissent quels sont les services sur le serveur RAT qui sont autorisés à communiquer avec quels autres services sur d'autres appareils. Les communications initiées par un service de logiciel de poste de travail d'ingénierie (EWS) sur l'interface HMI sont admises sur le dispositif de commande (automate programmable industriel, API dans la Figure 3). En revanche, les communications initiées par le connecteur sécurisé (SSH) sur l'interface HMI sont bloquées par le pare-feu.

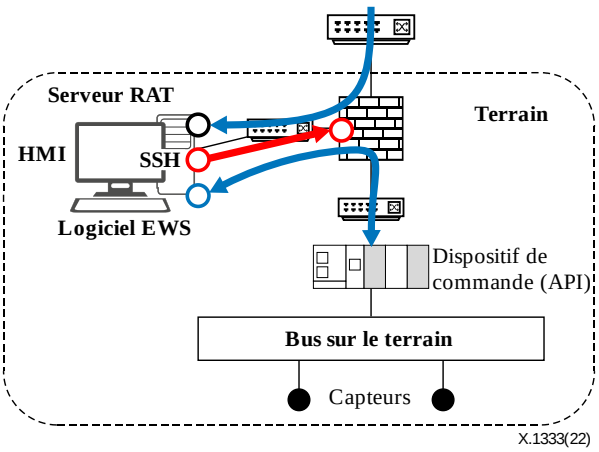

Figure 3 – Segmentation et subdivision du réseau pour utiliser le serveur RAT dans un réseau sur le terrain

8.4 Lignes directrices sur la sécurité pour les pistes de vérification

8.4.1 Journalisation

Contrôle de sécurité

Les événements relatifs à la sécurité du système et du réseau devraient être consignés dans des journaux, lesquels journaux devraient être protégés.

Objet

Les journaux d'événements relatifs à la sécurité du système et du réseau sont au cœur de la gestion de la sécurité de tout système. L'examen et l'analyse des événements liés à la sécurité permettent de détecter à temps les problèmes de sécurité. Ainsi, plus le serveur RAT génère des journaux d'événements détaillés, plus l'organisation détecte facilement les problèmes de sécurité.

Lignes directrices sur la mise en œuvre

Certains logiciels RAT intègrent des fonctions de journalisation plus poussées, par exemple lors de l'utilisation de chaque application et la manipulation des données dans le dispositif serveur, tandis que d'autres logiciels proposent des fonctions de journalisation plus sommaires, par exemple lors de la connexion et déconnexion du serveur RAT. Lorsqu'elle choisit un logiciel RAT, une organisation devrait donc tenir compte du niveau des fonctions de journalisation.

Si le logiciel RAT ne fournit qu'une fonction simple au niveau des rapports, l'organisation devrait également regarder les fonctions offertes en la matière par le système d'exploitation sur lequel le serveur RAT est installé. Pour cela, les comptes des utilisateurs distants sur le dispositif serveur devraient être séparés des autres comptes. Dans ce cas de figure, un administrateur de la sécurité devrait examiner les événements de sécurité enregistrés par le compte de l'utilisateur distant pour détecter un comportement anormal.

En plus du journal d'événements système, un journal d'événements réseau devrait aussi être généré. Toutes les demandes de connexion RAT et les réponses y afférentes (positives et négatives) devraient être consignées. De plus, tous les événements relatifs aux protocoles de connexion à distance (tels que les protocoles de terminaux, les protocoles de contrôle industriels et les protocoles de messagerie de commande Internet (ICMP)) devraient également être consignés. Comme mentionné ci-dessus, au premier stade d'une attaque, les adversaires effectuent généralement une reconnaissance du système. Divers protocoles de connexion à distance pourraient être utilisés pour cette reconnaissance. Les journaux d'événements réseau aident ici les administrateurs de la sécurité à détecter les comportements anormaux sur le serveur RAT.

Les journaux générés devraient être stockés en toute sécurité dans le serveur de journalisation. S'ils sont enregistrés sur le système au niveau local, il est possible que des auteurs d'attaque puissent les manipuler voire les endommager. C'est pourquoi il convient de les stocker sur un serveur de journalisation séparé.

Les journaux devraient être régulièrement examinés et analysés par l'administrateur de la sécurité.

8.5 Relations entre les menaces de sécurité et les contrôles de sécurité

Le Tableau 1 présente les relations entre les menaces de sécurité et les contrôles de sécurité. La présence d'un cercle dans une cellule indique que ce contrôle de sécurité devrait être mis en place pour atténuer la menace considérée.

Tableau 1 – Relations entre les menaces de sécurité et les contrôles de sécurité

		7.1 Clients						7.2 Serveurs		7.3 Réseaux	
		M1	**M2**	**M3**	**M4**	**M5**	**M6**	**M7**	**M8**	**M9**	**M10**
Clients	8.1.1 Mise à jour du logiciel	O									
	8.1.2 Intégrité du logiciel	O	O								
	8.1.3 Configuration sécurisée	O	O	O							
	8.1.4 Contrôle de l'accès des utilisateurs				O		O				
	8.1.5 Sécurité physique						O				
Serveurs	8.2.1 Authentification de l'utilisateur								O		
	8.2.2 Autorisation de l'utilisateur						O				
	8.2.3 Réauthentification périodique						O				
	8.2.4 Mise à jour du logiciel							O			
Réseaux	8.3.1 Contrôle de l'accès au réseau									O	
	8.3.2 Authentification mutuelle								O	O	
	8.3.3 Détection des comportements anormaux					O				O	O
	8.3.4 Configuration sécurisée du réseau										O
Audits	8.4.1 Journalisation					O					

Appendice I

Un exemple de configuration sécurisée des outils d'accès à distance dans un système de contrôle des ressources énergétiques durables

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

I.1 Aperçu du système

De nombreux capteurs et actionneurs sont installés sur les générateurs. Les capteurs fournissent des données mesurées aux dispositifs de contrôle (par exemple, l'API sur la Figure I.1) et les opérateurs surveillent l'état des générateurs en fonction des données à l'aide d'une interface HMI ou d'un poste de travail d'ingénierie. Selon l'état, les opérateurs contrôlent les actionneurs via l'interface HMI (ou le poste de travail d'ingénierie) et l'API. Par exemple, lorsqu'un typhon arrive, les opérateurs arrêtent la rotation des pales de l'éolienne. Le réseau reliant les capteurs, les actionneurs et les dispositifs de commande est appelé réseau de terrain. Dans le réseau de terrain, une interface HMI est généralement installée pour la surveillance et le contrôle des générateurs.

Les générateurs qui utilisent des ressources énergétiques durables, telles que l'éolien (éoliennes), l'hydrogène (piles à combustible) et le solaire (photovoltaïque), sont dans certains cas exploités par des opérateurs distants. Ces opérateurs surveillent à distance l'état des générateurs et les contrôlent pour produire efficacement de l'électricité.

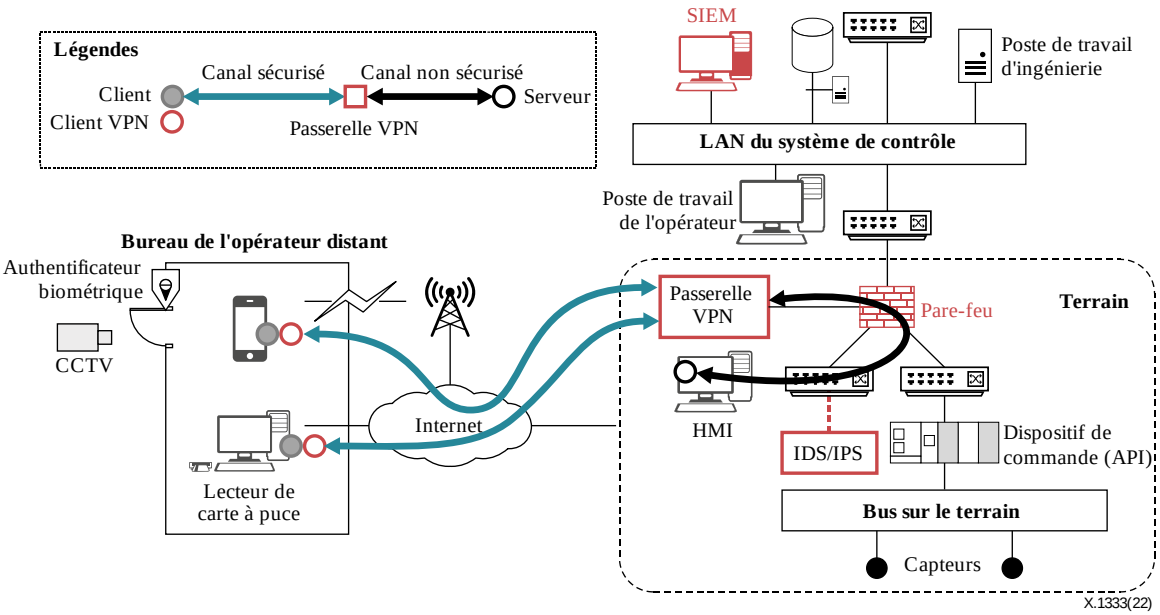

Figure I.1 – Un exemple de réseau sécurisé dans un système de contrôle des ressources énergétiques durables

I.2 Configuration sécurisée

La Figure I.1 montre un exemple de configuration de réseau sécurisé pour une ressource énergétique durable. Les mesures de sécurité pour chaque composant – client RAT, serveur RAT, réseau et journal des événements de sécurité – sont décrites ci-après.

I.2.1 Client RAT

Un compte séparé est créé pour le client RAT et le logiciel client est accessible uniquement par ce compte.

Chaque fois qu'un opérateur distant allume le logiciel client RAT, les processus de vérification de mise à jour et de contrôle d'intégrité sont lancés. La mise à jour, quant à elle, sera appliquée avant de démarrer le logiciel client RAT.

Le client NAC vérifie le niveau de sécurité du dispositif et bloque la connexion Internet si une configuration de sécurité fait défaut. Par exemple, si aucun logiciel anti-virus et aucun pare-feu personnel n'est activé, aucune connexion de communication ne sera autorisée par le client NAC.

Tous les appareils sur lesquels le client RAT est exécuté sont exploités dans le bureau des opérateurs distants. Le contrôle d'accès pour le bureau est mis en œuvre à l'aide d'un authentificateur biométrique (par exemple, empreintes digitales ou reconnaissance faciale) et d'un circuit fermé de télévision installé devant la porte du bureau.

I.2.2 Serveur RAT

Lorsque les opérateurs distants tentent d'établir une connexion RAT via un client RAT, une authentification à deux facteurs (c'est-à-dire un mot de passe et une carte à puce) est requise. Des adresses IP statiques pour une passerelle VPN et un serveur RAT sont par ailleurs utilisées.

Avant l'authentification mutuelle, l'hôte demandant une connexion est filtré par son adresse IP et son adresse de commande d'accès au support (MAC) au niveau de la passerelle VPN. Qui plus est, la durée de vie d'un canal de communication entre un client VPN et la passerelle VPN est de 8 heures. Par conséquent, les opérateurs distants doivent à nouveau fournir leur mot de passe et leur carte à puce pour la connexion VPN toutes les 8 heures.

Les comptes de l'interface HMI pour les opérateurs distants doivent être séparés des autres comptes pour limiter l'autorisation des opérateurs distants et générer des journaux détaillés pour les comptes.

I.2.3 Réseau

Le tunnel VPN IPsec protège un canal de communication entre un client RAT et un serveur RAT. Avant de se connecter au serveur RAT, un client VPN installé sur l'appareil d'un opérateur distant devrait établir un canal sécurisé avec une passerelle VPN. Pour fournir le niveau de sécurité minimum de 128 bits, la suite cryptographique, *Suite-B-GCM-256*, pour IPsec VPN est utilisée comme dans [b-IETF RFC 6379]. Pour l'authentification IKEv2, *ECDSA-256* est appliqué pour le VPN IPsec comme dans [b-IETF RFC 6380]. Pour équilibrer la sécurité et la surcharge, la durée de vie pour IKE SA est fixée à 24 heures et la durée de vie pour IPsec SA est fixée à 8 heures.

Le réseau de terrain est divisé en deux segments, comme une zone démilitarisée (DMZ) pour une interface HMI et un réseau de terrain pour les API, les capteurs et les actionneurs. Un pare-feu est également placé entre le réseau local (LAN) du système de contrôle, le réseau de terrain et la zone démilitarisée pour la subdivision du réseau. De ce fait, une communication d'un poste de travail d'ingénierie sur l'interface HMI peut être transférée vers le réseau de terrain, mais le pare-feu bloque tout autre trafic de l'interface HMI vers tout autre réseau.

Un système de détection des intrusions (IDS) ou IPS est installé dans la zone démilitarisée et reçoit le trafic réseau entrant et sortant depuis un port de commutateur configuré pour la mise en miroir du trafic.

I.2.4 Journal des événements de sécurité

Les événements de sécurité générés par les comptes d'accès à distance sont consignés dans le système HMI et transmis au système de gestion des informations et des événements de sécurité (SIEM). L'administrateur de la sécurité de l'organisation qui exploite la ressource énergétique durable examinera les journaux à intervalles périodiques via le système SIEM.

Bibliographie

[b-UIT-T X.1197] Recommandation UIT-T X.1197 (2012), *Lignes directrices relatives aux critères de sélection d'algorithmes cryptographiques pour la protection de service et de contenu de TVIP*.

[b-CEI 61924-2] CEI 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/

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Publié en Suisse
Genève, 2024