Co-funded by the
Erasmus+ Programme
of the European Union

InCyT-Trainingsmodule

Informationssicherheit für Mitarbeiter **Einheit Nr.: (3) Woche 5** **Name der Einheit (Moduls): (Sicherheit bei Geschäftsreisen)**	
Lernaktivitäten	❑ **Webinar** ❑ **Übungen** ❑ **Workshop** ❑ **Präsentation** ❑ **Sonstiges**
Lehrverantwortliche	• Mirosław Mazurek • Paweł Dymora
Ziele der Lernaktivitäten	1. Drahtlose Netzwerke 2. VPN 3. E-Mail-Verschlüsselung
Zu erwerbende Fertigkeiten	• **TS3** • **SS2**
Dauer der Lernaktivität	2 Wochen
Lernenanforderungen	***Was wird benötigt?***
	• Zugang zum Internet • Internet-Browser • MS Office365

Co-funded by the
Erasmus+ Programme
of the European Union

Kurze Informationen über das Modul

Beschreibung
Der allgemeine Rahmen dieses Moduls besteht darin, einige theoretische und praktische Themen im Zusammenhang mit dem Wissen und den praktischen Fähigkeiten zur Sicherheit auf Geschäftsreisen zu vermitteln. Sie werden die Möglichkeit haben, Ihr drahtloses Netzwerk zu schützen und geschützte drahtlose Netzwerke mit der Idee von VPN zu nutzen. Das Modul behandelt auch den sicheren Versand von E-Mails mit dem kostenlosen PGP-Protokoll für verschlüsselte Nachrichten, die niemand ohne Ihre Zustimmung entziffern kann.

Inhalt des Lernmaterials

1. Einführung in drahtlose Netze. Theoretische Grundlagen: Funktionsprinzip, Verschlüsselungsprotokolle.

Früher wurden WEP- und WPA-Protokolle zur Sicherung drahtloser Netze verwendet, aber sie waren nicht resistent gegen Hackerangriffe. Die Einführung des WPA2-Protokolls ermöglichte es, ein ausreichendes Sicherheitsniveau zu gewährleisten, aber es bietet dennoch keine vollständige Sicherheit. Es gibt viele Netzwerktopologien, drahtlose Zugangsprotokolle und Netzzugangserfassungstechniken, und bei der Netzschlüsselerfassung werden sowohl CPU- (Central Processing Unit) als auch GPU- (Graphics Processing Unit) Rechnerarchitekturen verwendet [1,2].

WEP (Wired Equivalent Privacy) ist einer der ältesten IEEE 802.11-Standards für die drahtlose Verschlüsselung. Er bietet einen Informationsschutz, der auf der Verwendung des RC4-Algorithmus beruht. Er weist viele bekannte Sicherheitslücken auf und wurde daher bereits mehrfach geknackt. Es ist einer der ältesten Standards zur Sicherung von WLAN-Netzen (seit 1997). Er erfordert keine hohe Rechenleistung der installierten Geräte. Es verwendet zwei Methoden zur Benutzerauthentifizierung: Offene Authentifizierung und Shared-Key-Authentifizierung. Darüber hinaus ermöglicht es eine Benutzerüberprüfung auf der Grundlage physischer MAC-Adressen unter Verwendung der ACL (Access Control List). Es gibt eine 64-Bit-WEP-Variante (basierend auf einem 40-Bit-Schlüssel und einem 24-Bit-Initialisierungsvektor) und eine 128-Bit-WEP-Variante (basierend auf einem 104-Bit-Schlüssel). Einige Hersteller haben auch einen 256-Bit-WEP-Standard eingeführt [1,2].

WPA (Wi-Fi Protected Access) ist ein weiterer Standard für die Verschlüsselung von drahtlosen IEEE 802.11-Netzwerken. Er wurde eingeführt, um das Sicherheitsniveau von WLAN-Netzwerken zu verbessern und bekannte Schwachstellen des WEP-Standards zu ersetzen. Er basiert auf der Verwendung von Protokollen: TKIP (Temporal Key Integrity Protocol) und EAP (Extensible

Authentication Protocol), 802.1x Standard und MIC (Message Integrity Check) Mechanismus. Der Standard basiert auf dem RC4-Algorithmus. Er wurde als Zwischenlösung zwischen dem WEP-Standard und dem derzeit sichersten drahtlosen Verschlüsselungsstandard 802.11i eingeführt. Er arbeitet in zwei Modi, die Folgendes umfassen: Enterprise (unter Verwendung eines RADIUS-Servers, der die Zuweisung der Schlüssel an die Benutzer verwaltet) und Personal (unter Verwendung eines gemeinsamen PSK-Schlüssels) [1,2].

WPA2 (Wi-Fi Protected Access 2) ist der derzeit leistungsfähigste Verschlüsselungsstandard für drahtlose Netzwerke (auch bekannt als 802.11i). Er bietet einen Informationsschutz, der auf der Verwendung des AES (Advanced Encryption Standard) basiert. Er wurde eingeführt, um das Sicherheitsniveau von WLAN-Netzwerken zu verbessern und bekannte Schwachstellen des WEP-Standards und des vorläufigen WPA-Standards zu ersetzen. Es implementiert das 802.1x-Protokoll zur Verbesserung der Kontrolle des Benutzerzugangs zum Netz. Es bietet die Arbeit in zwei Modi, die umfassen: Enterprise (unter Verwendung eines RADIUS-Servers, der die Zuweisung der Schlüssel an die Benutzer verwaltet) und Personal (unter Verwendung eines gemeinsamen PSK-Schlüssels) - heute häufig in Heimlösungen verwendet [1,2].

Der WEP-Algorithmus ist der am wenigsten sichere Verschlüsselungsstandard für drahtlose IEEE 802.11-Netze. Aufgrund der vielen derzeit bekannten Schwachstellen in den Sicherheitsaspekten des Algorithmus wurde er bereits mehrfach mit verschiedenen Methoden geknackt. Zu den wichtigsten Nachteilen des Standards gehören[3]:

- Fehlen eines definierten Schlüsselverwaltungssystems (häufig wird ein Netzschlüssel von allen Knoten eines drahtlosen Netzes verwendet);
- Unzureichende Bitgröße des Netzwerkschlüssels (die erste Version des WEP-Standards sieht 40-Bit-Schlüssel vor);
- Unzureichende Bitgröße des IV-Initialisierungsvektors (der WEP-Standard führt einen 24-Bit-Initialisierungsvektor ein, der sich als unzureichend erweist, und aufgrund der relativ hohen Wahrscheinlichkeit von Kollisionen bei einer geringen Anzahl von empfangenen Paketen besteht die Möglichkeit eines kryptografischen Angriffs, um den Wert des WEP-Schlüssels zu erhalten);
- Schwache ICV-Prüfsumme auf der Grundlage der linearen Funktion CRC-32 (es besteht die Möglichkeit einer unbemerkten Veränderung der im Netz übermittelten Informationen);
- Schwacher RC4-Algorithmus zur Informationsverschlüsselung (es bestehen zu viele Abhängigkeiten zwischen dem Netzwerkschlüssel und dem Ergebnis der Informationsverschlüsselung);
- Unzureichendes System zur Benutzerauthentifizierung (es besteht die Möglichkeit, Authentifizierungsnachrichten zu fälschen).
- Auf der Grundlage der vorgestellten Schwachstellen des WEP-Algorithmus wurden viele Tools entwickelt, um Angriffe durchzuführen, die das Sicherheitsniveau von WLAN-Netzwerken testen. Zu den beliebtesten Angriffen gegen WEP gehören:

- FMS-Angriff - ein statistischer Angriff (entwickelt von Fluhrer, Mantin und Shamir) auf den im WEP-Verschlüsselungsstandard verwendeten RC4-Algorithmus;
- KoreK-Angriff - ein statistischer Angriff (entwickelt von einer Person mit dem Spitznamen KoreK), der (im Vergleich zum FMS-Angriff) mehrere weitere Abhängigkeiten des Verschlüsselungsprozesses des RC4-Algorithmus nutzt;
- Chopchop-Angriff - ein interaktiver Angriff, der darauf abzielt, sich Zugang zum Netz zu verschaffen, indem eines der empfangenen Pakete schrittweise entschlüsselt wird;
- PTW-Angriff - ist ein statistischer Angriff (entwickelt von Pyshkin, Tews und Weinmann) auf den RC4-Algorithmus, der dank der sukzessiven Abhängigkeiten des Datenverschlüsselungsprozesses die Wahrscheinlichkeit, den Schlüsselwert mit einer relativ kleinen Anzahl empfangener Pakete zu erhalten, erheblich erhöht.

Eine weitere häufig verwendete Angriffsart ist der Wörterbuchangriff. Es handelt sich dabei um eine der Brute-Force-Methoden zur Erlangung von z. B. kryptografischen Schlüsselwerten in drahtlosen Computernetzen. Um WPA/WPA2-Schlüsselwerte zu erhalten, basiert die Methode auf einer Einwegverschlüsselung und dem Vergleich von Einträgen im Wörterbuch mit Informationen in der aufgezeichneten 4-Wege-Handshake-Sequenz. Wörterbuchangriffe werden mit der Absicht durchgeführt, die Zeit zur Erlangung von Schlüsselwerten im Vergleich zur Brute-Force-Methode zu reduzieren. Der Prozess der Abfrage des Schlüsselwerts wird so lange fortgesetzt, bis ein positives Ergebnis erzielt wird (d. h., wenn sich der Eintrag im Wörterbuch als gültiger Schlüsselwert erweist) oder bis alle Einträge im Wörterbuch mit dem negativen Ergebnis verglichen wurden. Ein negatives Ergebnis kann darauf hindeuten, dass der Schlüsselwert sehr komplex ist und die Brute-Force-Methode angewendet werden muss[3].

Entscheidend für den Erfolg dieses Angriffs ist die Auswahl eines geeigneten Wörterbuchs. Ein Wörterbuch ist eine Textdatei, die bei Wörterbuchangriffen verwendet wird, um z. B. kryptografische Schlüsselwerte zu erhalten. Sie enthält eine Liste von entsprechend vorbereiteten Elementen, die den gesuchten Schlüsselwert darstellen können. Die Verwendung von Wörterbüchern im Falle von Gewaltangriffen ermöglicht es, die Menge der untersuchten Werte erheblich zu reduzieren, was zu einer Beschleunigung des Prozesses zur Erlangung des kryptografischen Schlüsselwerts führen kann. Der Inhalt von Wörterbüchern wird z. B. auf der Grundlage der vorgelegten Elemente erstellt[3]:

- eine Liste von Wörtern, die in nationalen und ausländischen Wörterbüchern enthalten sind;
- Kombinationen von Wörtern mit Groß- und Kleinbuchstaben, rückwärts geschriebene Wörter (z. B. Palindrome);
- Kombinationen von Wörterbucheinträgen mit ausgeschnittenen Vokalen oder Konsonanten;
- Kombinationen von Mehrfachwiederholungen ausgewählter Namen, Nachnamen, Wörterbucheinträge;
- Kombinationen von Wörtern mit numerischen Werten, Sonderzeichen usw.;
- eine Liste der von den Benutzern am häufigsten verwendeten Kennwörter und Logins;

- eine Liste mit bekannten Unternehmen, Organisationen, Fachbegriffen, Eigennamen usw.;
- Informationslecks (d.h. Logins, Nicknames, Passwörter) von verschiedenen Internetportalen;
- Kombinationen von benachbarten Tastaturzeichen für ausgewählte Muster (Abb. 1).

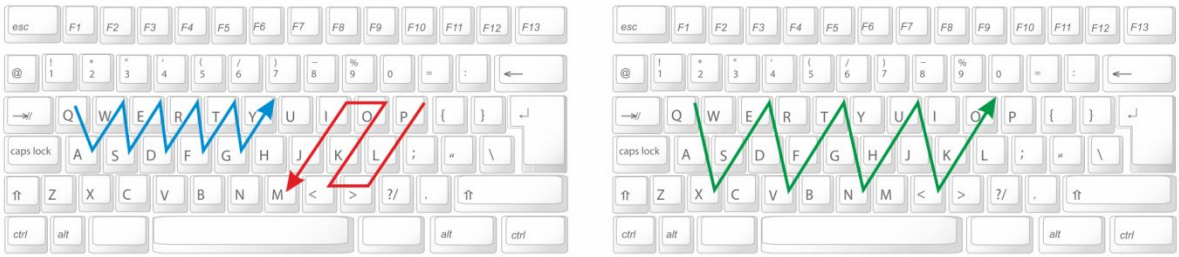

Abb. 1 . Schema mit Beispielen für die Erstellung von Netzwerkschlüsseln

Der Netzschlüssel spielt eine Schlüsselrolle bei der Untersuchung der Netzbelastbarkeit. Es handelt sich dabei um eine Zeichenfolge, die von den Netzbenutzern im Authentifizierungsverfahren verwendet wird. Der Authentifizierungsprozess ist ein wichtiger Schritt, um den Zugang zu gemeinsamen Diensten und Netzressourcen vor unbefugten Benutzern zu schützen. Netzwerkschlüssel werden oft von Netzwerkadministratoren erstellt und verwaltet und können das schwächste Glied in der Sicherheit eines Computernetzwerks darstellen. Schlüsselwerte, die sich als relativ zeitaufwendig oder als unmöglich erweisen, mit Brute-Force-Methoden in realistischer Zeit geknackt zu werden, sollten z. B. auf der Grundlage der vorgestellten Regeln generiert werden[3]:

- Jedes vom Administrator verwaltete drahtlose Netzwerk sollte mit einem anderen Netzwerkschlüssel gesichert werden;
- Jeder Netzwerkbenutzer sollte einen eigenen Netzwerkschlüssel verwenden;
- Netzwerkschlüssel sollten aus einer ausreichenden Anzahl von Zeichen bestehen;
- Die Erzeugung von Schlüsseln sollte auf der Grundlage des maximal verfügbaren Zeichenraums erfolgen;
- Schlüssel sollten nicht unter Verwendung von Unternehmens- und persönlichen Daten erstellt werden;
- Die Erstellung von Schlüsseln sollte nicht auf einer Liste von Einträgen in öffentlich zugänglichen Wörterbüchern basieren;
- Netzwerkschlüssel sollten auf der Grundlage von zufälligen Zeichenfolgen erstellt werden;
- Die Netzwerkschlüssel sollten regelmäßig aktualisiert werden;
- Derzeit verwendete Schlüsselwerte sollten nicht mit Schlüsselwerten verknüpft werden, die nicht mehr verwendet werden.

2. Virtuelle VPN-Tunnel. Theoretische Grundlagen: Typen, Architektur, Funktionsprinzip, Verschlüsselungsprotokolle. Installation des Programms Open VPN (Konfiguration, Adressierung, Parameterauswahl, Schlüsselerzeugung).

Ein virtuelles privates Netzwerk ist ein Tunnel, durch den privater Netzwerkverkehr zwischen dem Absender und dem Empfänger über ein öffentliches Netzwerk fließt. VPN steht für "Virtuelles Privates Netzwerk". Ein VPN-Netzwerk verschlüsselt alle Aktivitäten im Internet, verbirgt die IP-Adresse und schützt so die Identität des Netzwerkbenutzers. Eine VPN-Verbindung bietet sicheren Zugang zu Anwendungen, Websites und Unterhaltungsplattformen von jedem Ort der Welt aus. Es ist möglich, die übertragenen Daten optional zu komprimieren oder zu verschlüsseln, um eine bessere Qualität oder ein höheres Maß an Sicherheit zu erreichen und so die Privatsphäre innerhalb des Netzes zu schützen [4].

Ein sicherer Tunnel wird aufgebaut, indem zunächst der Client beim VPN-Server authentifiziert wird. Der Server wendet dann ein Verschlüsselungsprotokoll auf alle Daten an, die gesendet und empfangen werden. Um die Sicherheit jedes Datenpakets zu gewährleisten, legt das VPN es in ein externes Paket, das dann durch Verkapselung verschlüsselt wird. Sie gewährleistet die Sicherheit der Daten während der Übertragung und ist ein wesentlicher Bestandteil des VPN-Tunnels. Nachdem die Daten den Server erreicht haben, werden die externen Pakete im Entschlüsselungsprozess entfernt [4].

VPNs können in zwei Hauptkategorien unterteilt werden [5]:

- Ein Fernzugriffs-VPN, das es Benutzern ermöglicht, sich mit einem entfernten Netzwerk zu verbinden, in der Regel über eine spezielle Software.
- Site-to-Site-VPNs werden von Unternehmen, insbesondere von Großunternehmen, genutzt. Sie ermöglichen es Nutzern an ausgewählten Standorten, sicher auf die Netzwerke anderer Nutzer zuzugreifen.

Ein Beispiel für eine spezielle VPN-Entwicklungssoftware ist *RadminVPN*. In den meisten Fällen ist es nicht notwendig, eine statische IP-Adresse in Ihrem lokalen Netzwerk zu haben, um einen VPN-Tunnel einzurichten. Nachdem Sie die entsprechende Software heruntergeladen haben, wird ein entsprechendes Netzwerk mit einer statischen Adresse Ihres Computers erstellt [6].

Mit Radmin VPN können Sie eine Verbindung zu zwei Computern in zwei verschiedenen Netzwerken herstellen. Ein Konfigurationsbeispiel wird unten gezeigt. Zum besseren Verständnis der Funktionsweise des VPN-Kanals zeigen Abb. 2 und 3 die Anfangskonfiguration der Computer, zwischen denen ein sicherer Kanal aufgebaut werden soll.

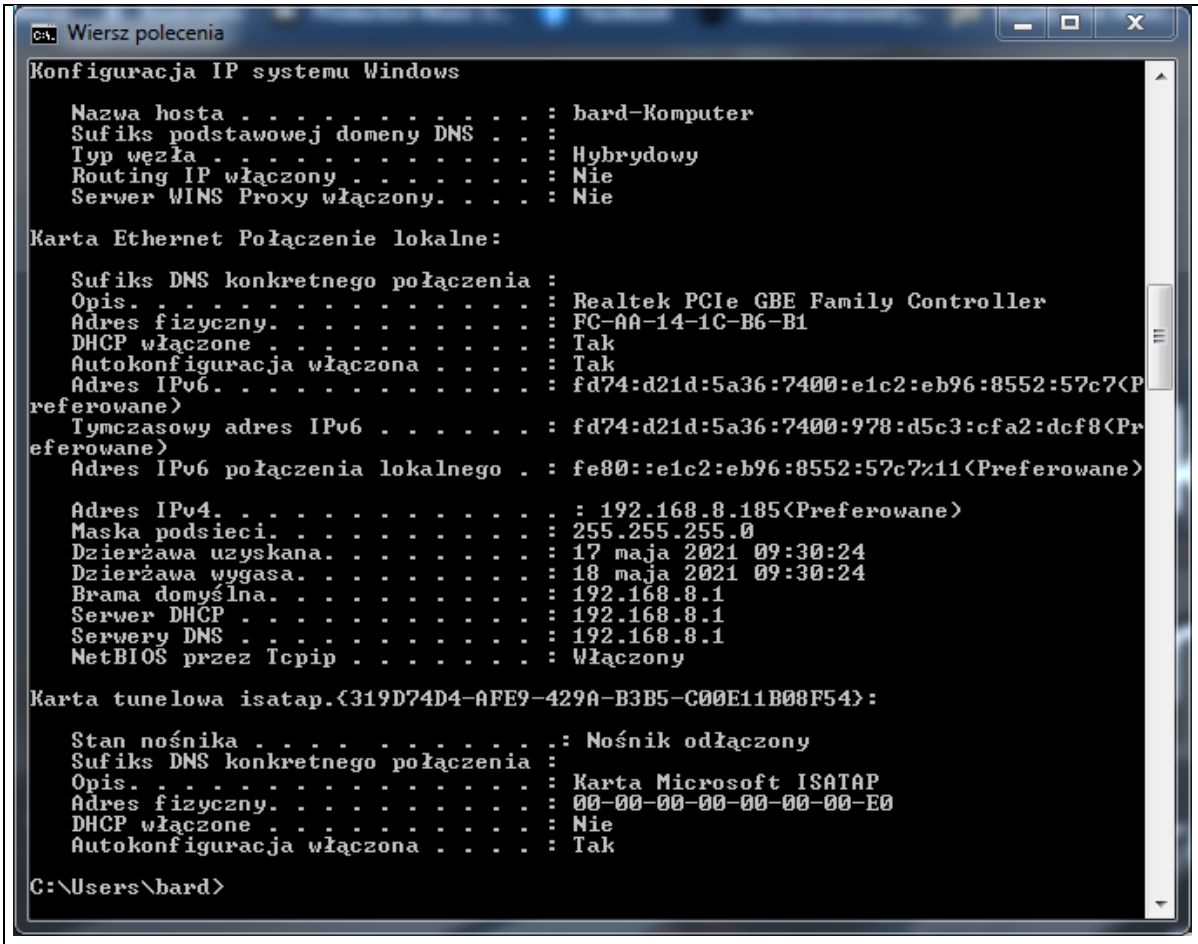

Abb. 2. Ausgangskonfiguration der Computer

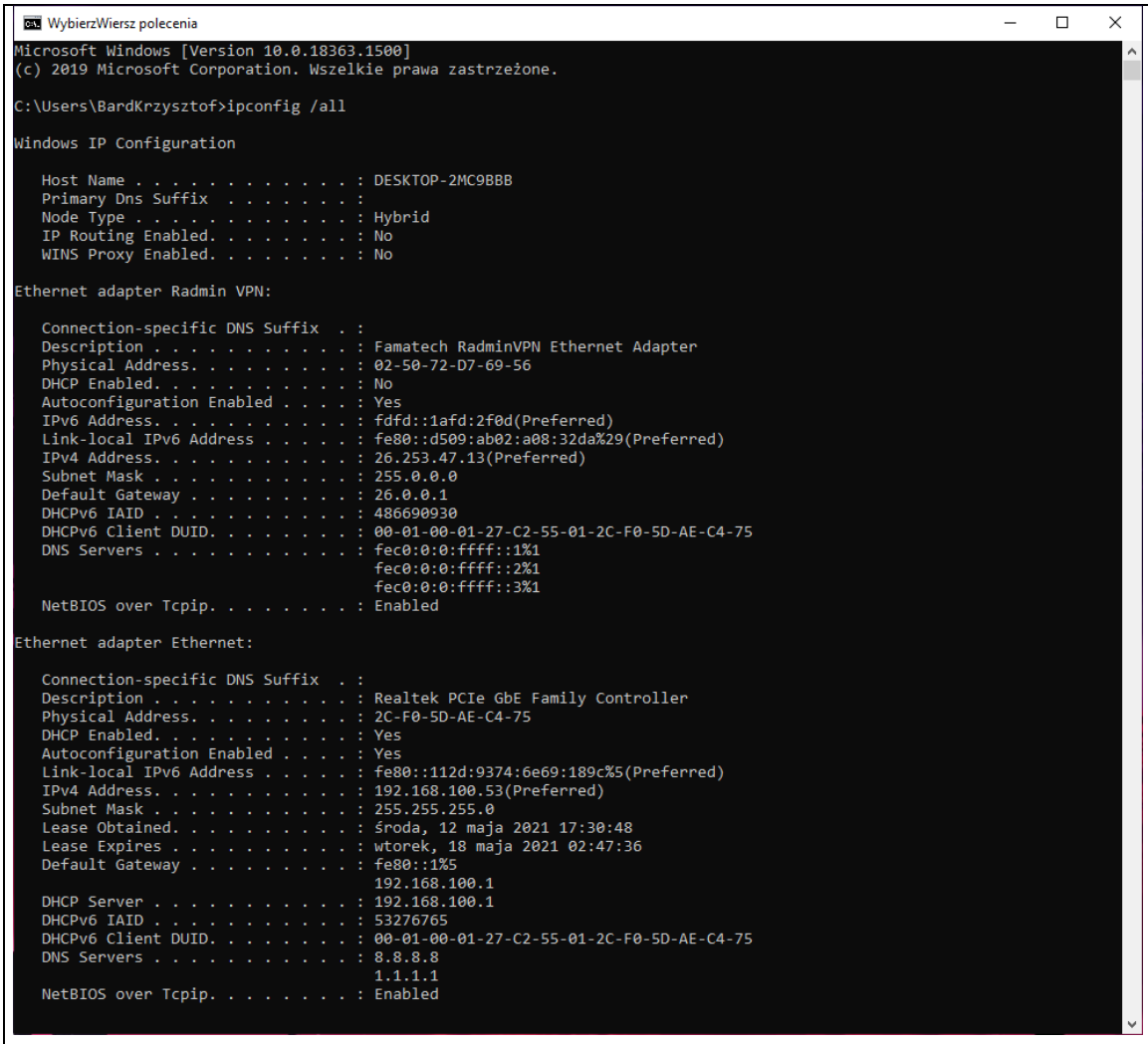

Abb. 3. Ausgangskonfiguration der Computer

Wie Sie sehen können, sind die Gateway-Adressen völlig unterschiedlich, so dass die Computer keine physische oder logische Verbindung zueinander haben. Um einen Kanal zu erstellen, installieren Sie RadminVPN auf beiden Computern. Auf einem von ihnen müssen Sie zunächst Ihr eigenes Netzwerk erstellen.

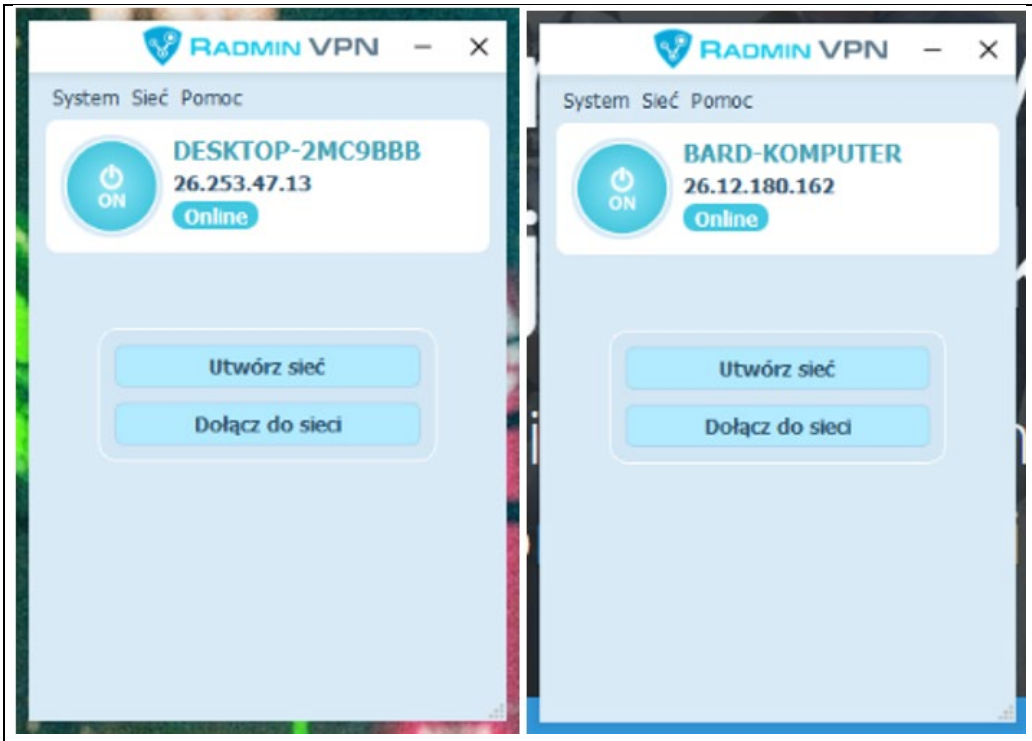

Abb. 4. Ansicht des Hauptbildschirms der Anwendung (linkes Bild - Konfiguration von Computer 1, rechtes Bild - Computer 2).

Um ein Netzwerk zu erstellen, wählen Sie im Anwendungsfenster **Netzwerk erstellen**, geben einen Namen und ein Passwort für das Netzwerk ein und bestätigen mit der Schaltfläche Erstellen. Auf dem zweiten Computer muss das so erstellte Netzwerk hinzugefügt werden, indem Sie auf die Schaltfläche Netzwerk beitreten klicken und den Namen und das Kennwort des soeben erstellten Netzwerks eingeben.

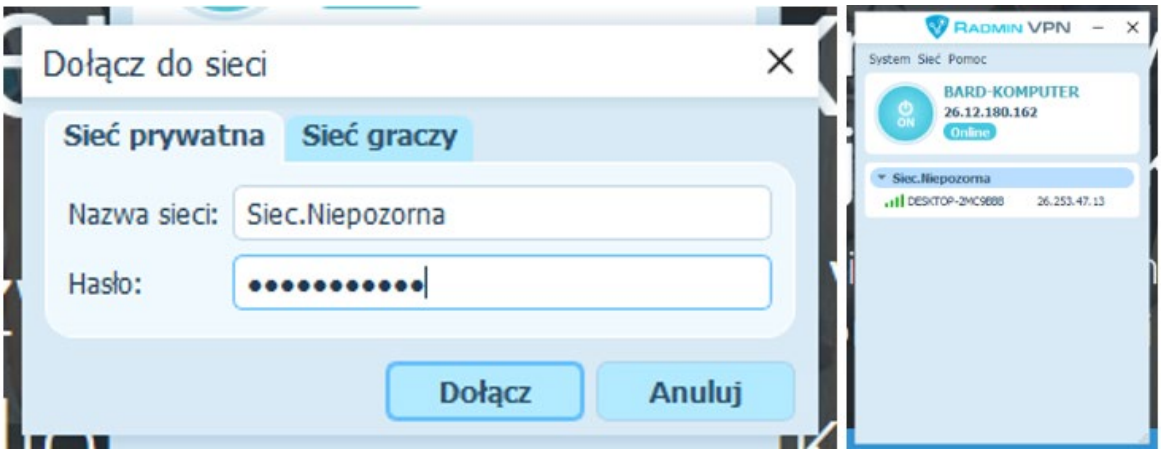

Abb. 5. a) Ansicht des Netzwerkverbindungsfensters; b) Verbindungsstatus.

Nach erfolgreichem Beitritt zum Netzwerk sollten sich beide Computer in einer Netzwerkverbindungsansicht befinden (wie in Abbildung 5b gezeigt). In diesem Fall können Sie den Namen und die Adresse des Computers auf der anderen Seite des Tunnels sehen. Auf dem zweiten Computer sind sie identisch. Der Verbindungsversuch wird in diesem Stadium fehlschlagen, da Radmin Server für den Betrieb des Systems erforderlich ist. Informationen über die Installation werden in der Anwendung angezeigt und müssen auf beiden Computern durchgeführt und neu gestartet werden. Nach Abschluss des gesamten Installationsprozesses können die Computer miteinander kommunizieren, aber es ist nicht möglich, dass einer die Kontrolle über den anderen übernimmt. Um sich gegenseitig steuern zu können, müssen Sie den Remote-Desktop in Windows konfigurieren (Systemsteuerung->System und auf der rechten Seite Erweiterte Systemeinstellungen).

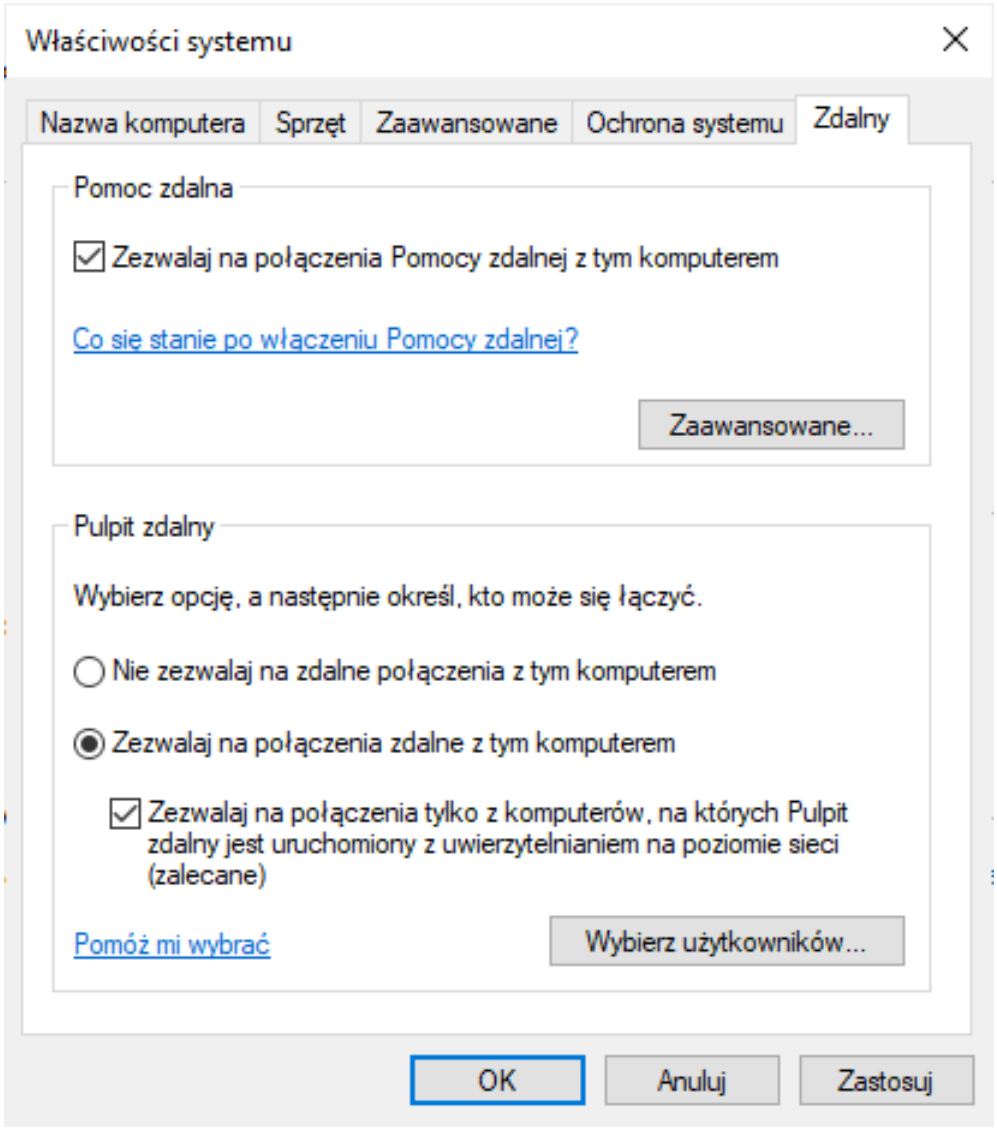

Abb. 6. Einstellungen des Bereichs Remote Desktop

Das Fenster Systemeigenschaften erscheint. Wählen Sie nun die Registerkarte Remote und den Abschnitt Remote Desktop, indem Sie Remoteverbindungen zu diesem Computer zulassen wählen (Abb. 6). Nachdem Sie die Änderungen auf beiden Computern genehmigt haben, erstellen Sie einen Benutzer mit den entsprechenden Zugriffsrechten. Starten Sie dazu RadminServer und wählen Sie in den Feldern auf der rechten Seite Permissions und dann die Option Permissions. Aktivieren Sie im Fenster Berechtigungen die Option Voller Zugriff und erstellen Sie einen Benutzer (Sie müssen ihm einen Namen und ein Passwort geben). Damit ist die Konfiguration des VPN-Kanals abgeschlossen. Der erstellte Tunnel ist bidirektional und kann problemlos zur Steuerung von Computern von beiden Seiten verwendet werden.

3. E-Mail-Verschlüsselung. Theoretische Grundlagen: Arten der Verschlüsselung (symmetrisch und asymmetrisch), Sicherheit, Protokolle, Schlüssel. Installation und Konfiguration von OpenPGP. Installation und Konfiguration eines E-Mail-Clients.

Einer der am häufigsten genutzten Kommunikationskanäle ist die elektronische Post (E-Mail), die zunehmend zum Ziel von Hackerangriffen wird. Der Schutz dieses Elements ist ein wichtiger Bestandteil eines Pakets von Cybersicherheitslösungen. Der Schutz von E-Mails und die Verschlüsselung von Anhängen sind zwei sehr wichtige Aspekte der Online-Sicherheit. Die Verschlüsselung von E-Mails minimiert nicht nur das Risiko, dass vertrauliche Daten nach außen dringen, sondern verhindert auch, dass sie von Unbefugten abgefangen werden. E-Mails und ihre Anhänge sind standardmäßig nicht mit SSL- und TLS-Protokollen gesichert, und alle Nachrichten werden im Klartext gesendet [8].

Verschlüsselungsalgorithmen lassen sich wie die Kryptographie in zwei Kategorien einteilen:

- symmetrische Verschlüsselungsalgorithmen;
- asymmetrische Verschlüsselungsalgorithmen;

Der Hauptunterschied zwischen den beiden Verschlüsselungsmethoden besteht in der Anzahl der verwendeten Schlüssel. Bei der symmetrischen Verschlüsselung wird ein einziger Schlüssel verwendet, während bei der asymmetrischen Verschlüsselung zwei verschiedene, aber zusammengehörige Schlüssel verwendet werden. Einer der Schlüssel ist der private Schlüssel, der andere ist der öffentliche Schlüssel. Symmetrische Verschlüsselungsalgorithmen verwenden denselben Schlüssel, um sowohl Ver- als auch Entschlüsselungsfunktionen auszuführen. Der asymmetrische Verschlüsselungsalgorithmus verwendet einen Schlüssel zum Verschlüsseln von Daten und einen anderen Schlüssel zum Entschlüsseln derselben. Das heißt, wenn wir eine verschlüsselte Nachricht an jemanden senden wollen, verschlüsseln wir sie mit dem öffentlichen Schlüssel des Empfängers, und der Empfänger verwendet seinen privaten Schlüssel, um sie zu entschlüsseln.

Ein weiteres Kriterium für die Unterteilung der Verschlüsselung ist die Schlüssellänge. Die Länge des Schlüssels steht in direktem Zusammenhang mit dem Sicherheitsniveau, das die einzelnen kryptografischen Algorithmen bieten. Je länger der Schlüssel ist, desto sicherer sind die Daten. Bei symmetrischen Algorithmen werden die Schlüssel nach dem Zufallsprinzip ausgewählt, und ihre Länge beträgt in der Regel 128 oder 256 Bit, je nach dem erforderlichen Sicherheitsniveau. Bei der asymmetrischen Verschlüsselung muss es eine mathematische Beziehung zwischen dem öffentlichen und dem privaten Schlüssel geben (in Form einer eindeutigen mathematischen Formel), damit die Ver- und Entschlüsselung stattfinden kann.

Aufgrund ihrer größeren Geschwindigkeit wird die symmetrische Verschlüsselung in vielen modernen Computersystemen zum Schutz von Informationen eingesetzt, wie z. B. der Advanced Encryption Standard (AES), der von der US-Regierung zur Verschlüsselung vertraulicher und geheimer Informationen verwendet wird. AES hat den früheren Datenverschlüsselungsstandard (DES) ersetzt.

Die asymmetrische Verschlüsselung wird in Systemen verwendet, in denen mehrere Benutzer Zugriff auf die Ver- und Entschlüsselung einer Nachricht oder eines Datensatzes benötigen. Ein Beispiel wäre die E-Mail-Verschlüsselung, bei der der öffentliche Schlüssel zum Verschlüsseln und der private Schlüssel zum Entschlüsseln der Nachricht verwendet werden kann.

Eine Lösung ist der OpenPGP-Standard. Er definiert kryptographische E-Mail-Erweiterungen - Verschlüsselung und digitale Signaturen. Der Standard basiert auf dem bestehenden PGP-Programm. Derzeit gibt es viele verschiedene Implementierungen. Der Standard ist in RFC 4880 definiert. Häufig verwenden Benutzer den E-Mail-Client Thunderbird, um E-Mails zu versenden. Mit diesem Programm können Sie verschlüsselte und digital signierte E-Mails nach dem OpenPGP-Standard senden und empfangen. Diese Funktion ist allgemein als Ende-zu-Ende-Verschlüsselung (e2ee) bekannt und macht die Kommunikation sicherer und weniger anfällig für das Ausspähen durch Dritte. Thunderbird 78 bietet integrierte Unterstützung für zwei Verschlüsselungsstandards, OpenPGP und S/MIME.

Frühere Versionen von Thunderbird (v68 und früher) hatten eine eingebaute S/MIME-Unterstützung, und Sie konnten OpenPGP-Unterstützung mit dem Enigmail-Add-on und der GnuPG-Software hinzufügen. Das Enigmail-Add-on ist für Thunderbird 78 nicht mehr verfügbar, es sei denn, man möchte seinen ehemaligen Nutzern bei der Migration zu OpenPGP in Thunderbird 78 helfen oder eine Anleitung erhalten, wie sie ihre "Junior Mode"-Regeln von Enigmail wiederherstellen können. Sie können Ihre Thunderbird-Einstellungen von einer älteren Version (z.B. 68.x) auf die Version 78.x aktualisieren. Bevor Sie Thunderbird 78 zum ersten Mal verwenden, sollten Sie jedoch eine Sicherungskopie Ihres Thunderbird-Profils erstellen, da das Profil nach dem Upgrade nicht mehr mit Thunderbird 68 verwendet werden kann.

Enigmail verwendet GnuPG zum Speichern und Verwalten aller Schlüssel und vertrauenswürdigen Einstellungen. Sie können migrieren und Enigmail wird die alten Schlüssel von GnuPG lesen und importieren. Thunderbird 78 verwendet andere Einstellungen als Enigmail. Bei Enigmail war es möglich, OpenPGP für ein E-Mail-Konto zu aktivieren, aber den zu verwendenden

Schlüssel automatisch auswählen zu lassen. Thunderbird 78 kombiniert diese Einstellungen. Um OpenPGP für ein E-Mail-Konto zu aktivieren, müssen Sie explizit angeben, welcher Schlüssel verwendet werden soll.

Für die Verschlüsselung wird die Software GPG4win verwendet. Dabei handelt es sich um eine Reihe von fortschrittlichen Datenverschlüsselungswerkzeugen. Es ermöglicht den Schutz vor unbefugtem Zugriff nicht nur auf E-Mails, sondern auch auf Dateien und Ordner. Die Arbeit mit Gpg4win basiert auf asymmetrischer Verschlüsselung, d.h. auf der Grundlage von zwei Schlüsseln - einem privaten und einem öffentlichen. Der erste wird zum Verschlüsseln der Daten verwendet, der zweite soll die Empfänger der Nachricht erreichen, die auf diese zugreifen können. Bewahren Sie den privaten Schlüssel an einem sicheren Ort auf.

Das Paket enthält Elemente wie das Verschlüsselungstool GnuPG, den Zertifikatsmanager Kleopatra (Abb. 7), den alternativen GPA-Zertifikatsmanager, den E-Mail-Client Claws Mail sowie zwei Plugins, die die Integration mit Microsoft Outlook (in den Versionen 2003, 2007, 2010 und 2013) und dem Windows Explorer ermöglichen.

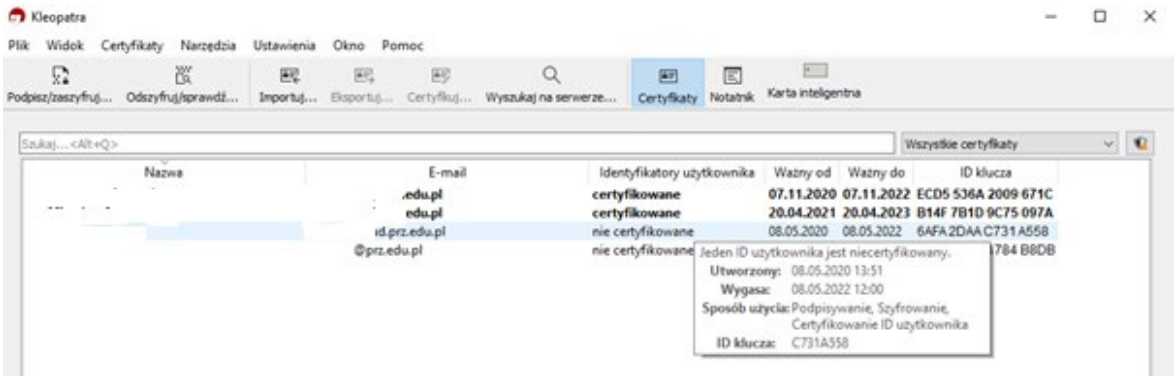

Abb. 7. Zertifikatsverwalter - Kleopatra.

Gpg4win unterstützt die Standards OpenPGP und S/MIME (X.509) und erstellt Zertifikate standardmäßig mit 2048-Bit-Schlüsseln. RSA ist der Standard-Verschlüsselungs- und Signieralgorithmus. Darüber hinaus ermöglicht das Paket auch die Erzeugung und Überprüfung von SHA1-, SHA256- und MD5-Prüfsummen.

Konfiguration der Nachrichtenverschlüsselungsumgebung.

Nachdem Sie dem Programm GPG4WIN E-Mail-Konten zugewiesen haben, sollten Sie ein Schlüsselpaar erzeugen. Ein Schlüsselpaar besteht aus einem privaten Schlüssel und einem öffentlichen Schlüssel. Der private Schlüssel wird einem bestimmten Konto zugewiesen. Wer eine verschlüsselte Nachricht an dieses Konto senden möchte, muss den öffentlichen Schlüssel des Empfängers besitzen.

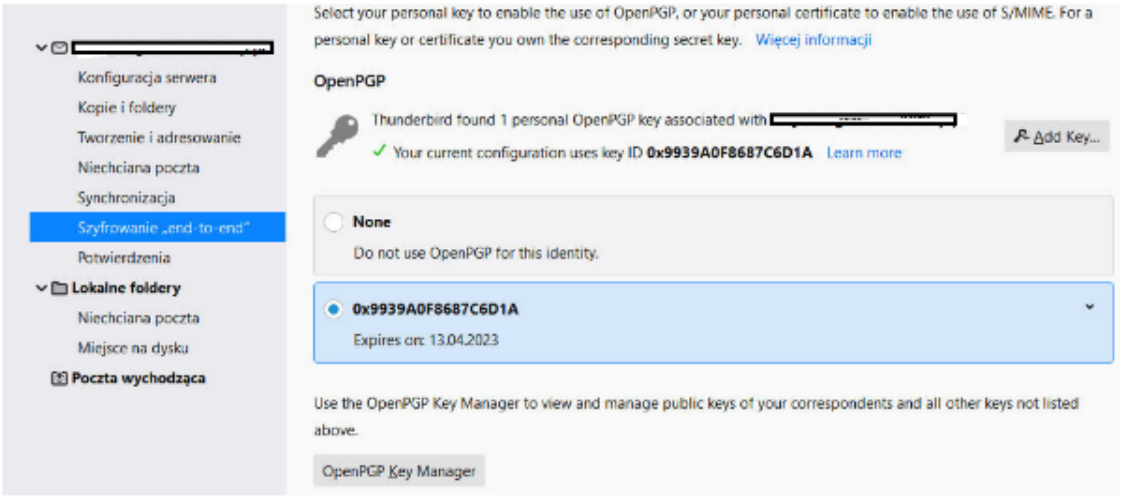

Abb. 8. Einstellungen des Bereichs Remote Desktop

Sobald die Konten in Cleopatra konfiguriert sind, können Sie Thunderbird direkt zum Senden und Empfangen verschlüsselter Nachrichten verwenden, ohne ein externes Programm zu benutzen. Denken Sie daran, Ihren öffentlichen Schlüssel zu senden, wenn Sie Ihre erste Nachricht an einen neuen Empfänger senden (Abb. 8). Ein Beispiel für eine verschlüsselte Nachricht ist in Abb. 9 dargestellt.

```
-----BEGIN PGP MESSAGE-----

wcDMA0r5u59RHK/uAQv/cvK0XliobGKfmQ25IcGe4kxtcXan9oDhQ0HODeAQyLSfpPFYOitt4LpF
Kc2aae3ayqRN+0bhTESVFaxttCw76E5wszkM9cK8UdxYzrX9PuaujtzYj8kSx3m0skfXrdglYnM8
llIYNETSgTnFSZ4jHKQLVIHVw9ZMztoo/ibLVJY3TTd7aKn7+cYyepNasrPPzoxcSGjJ1pQCkJ6t
SGtm8HDBfekKbK6qTKefYdGrCDBS4sAsuszwaX5QtSn50LAE2FkXCiKzTh6DkdFxQQ7yk/rUTs93
MkRwRtjteDqO7KC1yNPBim+KVLVG20EibD1FrdFIsbaEaPI13Y06LhmjBMrUOUaMhPJpYDM1Ki8u
gqGHOQmqISQU1y6/poyGDmOfSPOFchWaTB+9fjzpmEb32mK10D1JOM2llut5AtmZH8W1lKpy4cdC
XygSXMkJ4as+p9/MtICdESyFkDXamESbtI04Ay5Xj+YrBnQ+Wk0lHOeLfSFg+cj7fwUuasRvEIe0
wcDMA3pK1foZRRoWAQv/UVilR5h++k8Tq8uk/IeUchC3Si832Li8Ro++dGxy65Gomjlzg+oxbOoj
0u1kZGs5QbCywv5+vlo7CxpGSeMcBbjlT5jV/cKk1An9bdCjADXFLw4sEWCtqTR47OFqArvqi2gm
2iOW4g6Zcnd2lcfGe5kmeyRKt8OmHL6LDaZXSnJCJkhNRwr3GKHh8gJeT00bn+72M9TbBKXxLe3T
bnGw2ypPIQJ55k2x+ZbgkjDnQQDogsHpB1ip7K5yYArf+rI4uPqbYQgSU3NYYAUsmOtI2yesouvV
gFic/0TE9xq0qhciE2bTWPxH5ikxCMwLQa33E8+hngsSDfoyoRdolSEwjhI8KHthzddXzPNSkdgn
Q4pdGU1jFaDivtLc7cNs3SFKoZBiZcQaHRTABVNDMQgRqgoG6F0Ditu03vXCh5aR8/zUVS6moGT8
2sh/VWvryEAHKLSUPZulgwaZlD5hxosUMuwzGibLzaCApbilNdzm4zaDz2KdGBwmvyGkC7oT41vj
0sMwAbnd2f3Hz+AuXFajZ6uO8m6ibKMtJRM3EXggkNhue0rIU4KLchp9U9jLAt6GMQjPFKmgGqEj
U7/QPiVbJ8DjbmhYH90JwYH8hJCx1rq4AtXOxJgz8w0B+MOe6maKxDaDqS9gQj/n9N/Hvj8btZKz
turb54Y8MxZXXXoNxLAVZr1HHcbQoweHIx0EXanoMsxEwT3ugAiQetwBzXnR9DOzxTkzeOMK1ooS
6jnVTQy454q1+w6fNWAfBbpYY73Lt1NifD7mHoqe1G3oWhgzj/uUs67TJ1DjLfqzhxqw0TnfXyNM
+457fZCj+iYwdV8DhfDb4dyfYmDjA8LLP8Uw7gLtkFxD1dsaLf7/xQ5g98eKhz/4INI0xL+5Znno
x4SnkX++hy4z/nRKBNQcIupW7KuG1SOABTIhQWx3mtxyte0mxBRxiApfC5HfNzQM+vtmhJK8mlHK
Osc3kVw6kTodafSTi/qLghcOh2R7h8hL7qRc56ig7i4nPY5bnsPpfyyPYAuUDJQUz5z4tFrdEX/+
gw/gH3O8hTS17VSfgya0BUwJvMnlbS1+VZ7zomF405ne8hrFsT5j/dnjP7NgGS3CVMDLyEDtQA7k
Vbru0EN4JTsCu3T7rMnRrGtX1kfsTXBLayhcpbaMyHojMKw60p41o2gvTn5fw/+GJHGQdsZ3HJ+g
fr9EWKLQzQX6PSLsJ5OexLRkMtHXV4jBoSRyTzFTwprBkNNKZu2aRYa17BBFuVc5RTf8rSVWq7Eq
rKrXGOP+GgqGGTxoD8zfFtp0YJ+mP28L0DtuPnmG9IzxdbXO/JG6sT6hzPEA6MIlaW6Y++94Jpg2
XEKsGOdW9IHx9613FwjPtj6HKC8GtN5s8dgSAm3tw5KUWfchtKIOZYiynxuRnwIMN0UM0G2QFKYr
pU+50ba8rdui9D2YFzEcbw9a3meaWksO3Zvd8obQfwGFMX9DwV5VPEcmASHEUMULGBUO3KIUtaxU
Sdg9qmehxPMkkH3bB3x+G79WmV0ss0G9r+uVk/XhzxckqUI0w++q2PmWsXAIP2NsyX7W1BHyZ5J0
HhUwUllGtpl3gv/WwOxTyoEz2oeQucK5Eq91vEwaudCnip7STqK2WpboGvAQ54ZIZRFbm/4sOd/W
4kH6xyeYBTsIf3ft7LyvoB6Xq91A1xOFe94CcAqty90FynvF26Da7QRsNQalhfhfB1bnaEQIgf+7
J9fpMYQEcC4tT8RW9vtozQurNpgZnZS9sjWjke6/j3XV7paxOW7OG8nc+1r09LQMMtVjvI5Zd1FV
JyAtr1EsoF/9MzFfofn6eCtU8VvXiS8+cIDjTqrb2EKS68Rpu9Z8LCgz
=MjYk
-----END PGP MESSAGE-----
```

Abb. 9. Ein Beispiel für eine verschlüsselte Nachricht.

Thunderbird entschlüsselt automatisch Nachrichten und Anhänge, die mit ihnen gesendet werden. Denken Sie daran, dass Sie den öffentlichen Schlüssel des Empfängers kennen müssen, bevor Sie verschlüsselte Korrespondenz versenden. Die Verschlüsselung mit dem GPG-Add-on schützt nicht nur den Inhalt, sondern auch die Anhänge. Ohne den Schlüssel des Empfängers zu kennen, ist es nicht möglich, eine verschlüsselte Nachricht zu versenden. Außerdem können Sie mit Thunderbird mehrere E-Mail-Konten synchronisieren.

Fragen:

Fragen Diskussionsforum, die mit einer kurzen Erklärung beantwortet werden müssen. Die Antworten werden mit dem Mentor während der Mentoring-Sitzungen besprochen

1. Was ist ein VPN?
2. Wie können Sie die VPN-Lösung nutzen?
3. Können Sie jemandem Ihren privaten Schlüssel für die PGP-E-Mail-Verschlüsselung schicken?

Fragen zur Selbsteinschätzung. Nach der Beantwortung kann der Lernende die Ergebnisse sehen und sie mit den auf der Plattform gespeicherten Ergebnissen vergleichen

1. Sichere Methode für den Zugriff auf Ihre Daten über Fernzugriff
2. Methoden zur Sicherung Ihrer E-Mail-Konversation

Anhänge:

1. Präsentation
2. Video-Filme

Referenzen:

1. Rana, Muhammad Ehsan & Abdulla, Mohamed & Arun, Kuruvikulam. (2021). Gemeinsame Sicherheitsprotokolle für drahtlose Netzwerke: A Comparative Analysis. 10.2991/ahis.k.210913.080.
2. Habibi Lashkari, Arash & Sendón Varela, Juan & Samadi, Behrang. (2009). Eine Übersicht über drahtlose Sicherheitsprotokolle (WEP, WPA und WPA2/802.11i). 10.1109/ICCSIT.2009.5234856.
3. Kumkar, Vishal & Tiwari, Akhil & Tiwari, Pawan & Gupta, Ashish & Shrawne, Seema. (2012). Vulnerabilities of Wireless Security Protocols (WEP and WPA2). International Journal of Advanced Research in Computer Engineering & Technology. 1.

4. Costa, Luís & Fdida, Serge & M. B. Duarte, Otto Carlos. (2000). Eine Einführung in virtuelle private Netzwerke: Auf dem Weg zu D-VPNs.
5. https://www.vpnmentor.com/blog/different-types-of-vpns-and-when-to-use-them/
6. https://www.radmin-vpn.com
7. https://www.fortinet.com/resources/cyberglossary/pgp-encryption