UNIVERSITÄT ZU LÜBECK
INSTITUT FÜR IT-SICHERHEIT

Übungsblatt 4

Network and E-Mail Security

Abgabe bis 16. Mai 2023 um 12:00 Uhr im Moodle

Cybersecurity im Sommersemester 2023

Thomas Eisenbarth, Jan Wichelmann, Anja Köhl

Einführung

Während die Implementierung des Rechtemanagements und des innovativen neuen Abrechnungssystems andauert, wendet sich *Immature Technical Solutions* bereits der nächsten Baustelle zu: Den Kunden wird auf der Firmenwebsite ein Bereich angeboten, in dem nach Login mit Kundennummer und Passwort Auftragsdaten eingesehen und die jeweilige Hosting-Konfiguration bearbeitet werden kann.

In der Vergangenheit gab es hier wiederholt Beschwerden, dass ungewollt Einstellungen verändert und Server mit bösartiger Software gestartet worden sind, was nur durch einen unberechtigten Zugang auf die Kundenkonten passiert sein kann. Sie werden gebeten, einen Blick auf das Kundenportal zu werfen und mögliche Sicherheitslücken zu identifizieren.

Was Ihnen sofort auffällt: Die ganze Seite wird komplett unverschlüsselt übertragen! Eine kurze Nachforschung ergibt, dass eine TLS-Verschlüsselung des Kundenbereichs bisher nach den Worten des Managements „unverhältnismäßig teuer“ gewesen sei, und außerdem auch gar nicht klar sei, „was das überhaupt bringt, man muss doch ein Passwort eingeben“, weswegen der Bereich bis jetzt unverschlüsselt geblieben ist. Beschwerden einiger Kunden hierzu („Wo kommt denn die ganze Malware her?“) wurden offenbar freundlich entgegengenommen und im Bugtracker mit Priorität *Feature Request / Low* zum Verschwinden gebracht.

Inzwischen hat sich jedoch mit *Let's Encrypt* [1] eine Möglichkeit etabliert, kostenlos und automatisiert TLS-Zertifikate generieren und installieren zu können. Sie tragen dies sogleich an das Management heran. Allerdings möchte das Management nicht einfach unnötige Software von irgendwelchen obskuren Organisationen installieren, und bittet Sie daher zuerst um ein paar weiterführende Erklärungen.

Aufgabe 1 Zertifikate (5 Punkte)

Zuallererst geht es wieder mal darum, einige Grundbegriffe verständlich zu machen. Beantworten Sie hierzu die folgenden Fragen:

1. Was hat ein Zertifikat für einen Nutzen, wenn bereits ein Schlüsselpaar aus privatem und öffentlichem Schlüssel vorliegt? Warum wird das Schlüsselpaar nicht direkt eingesetzt?
2. Was ist die Aufgabe einer CA?
3. Warum wird das Schlüsselpaar lokal auf dem eigenen Rechner erzeugt, und nicht zusammen mit dem signierten Zertifikat von der CA zur Verfügung gestellt?

[1] `https://letsencrypt.org/`

Aufgabe 2 Public Key Infrastructure (5 Punkte)

Nun geht es um die konkrete Umsetzung in Let's Encrypt. Öffnen Sie hierzu die Seite `https://helloworld.letsencrypt.org/` und schauen Sie sich das Zertifikat an.

1. Welche Zertifikate sind an der Signatur des Ihnen angezeigten beteiligt? Welche(s) davon sind/ist in Ihrem Browser vorinstalliert?
2. Warum wird das Zertifikat der Website nicht direkt mit einem Root-Zertifikat signiert, sondern mit einem untergeordneten? Begründen Sie Ihre Antwort.
3. Zertifikate werden neben der Verschlüsselung auch dafür genutzt, Server zu authentifizieren. Welchen Rückschluss lässt das Ihnen angezeigte Zertifikat auf den Inhaber der Website zu? Begründen Sie Ihre Antwort.
4. Kann der Inhaber das Ihnen angezeigte Zertifikat nutzen, um die Kette um ein Glied zu erweitern und z.B. ein Zertifikat für `https://uni-luebeck.de/` zu signieren, dem entsprechend alle Browser vertrauen? Begründen Sie Ihre Antwort.

Aufgabe 3 WPA 2 vs. WPA 3 (5 Punkte) *[optional bei bestandener Praktikumsaufgabe 4]*

Diese Aufgabe muss nicht bearbeitet werden, wenn Sie stattdessen die freiwillige Aufgabe "In WPA2-Netzwerk einbrechen" des "Netzwerksicherheit"-Praktikums bestehen. Bitte geben Sie Ihren Gruppennamen aus dem Praktikum an, um die Korrektur zu erleichtern.

Wo Sie gerade schonmal da sind, bittet die Chefin der Infrastrukturabteilung Sie um eine Einschätzung zur Sicherheit von WLAN-Standards, da ITS das alte unverschlüsselte Netzwerk gern durch ein verschlüsseltes ersetzen würde.

1. Erklären Sie, wie sich WPA2-Verbindungen bei Nutzung einer schwachen Passphrase entschlüsseln lassen. Was ist der Vorteil dieses Angriffs gegenüber einem, bei dem mögliche Passphrasen nach und nach direkt beim Access Point ausprobiert werden? Begründen Sie Ihre Antwort.
2. Welche Verbesserungen werden in diesem Kontext durch WPA3 eingeführt?

Aufgabe 4 E-Mail-Sicherheit (8 Punkte)

Während ITS die alten Tickets aus dem Bugtracker abarbeitet, fällt eine weitere Kategorie von Kundenbeschwerden auf: Einige beklagten sich darüber, dass ITS unüblich oft Rechnungen verschicke, teilweise mehrere Male pro Woche. Hierdurch fielen die Kosten für deren Dienstleistungen sehr hoch aus, und es würde daher langsam über einen Umzug zu einem anderen Anbieter nachgedacht. Die Buchhaltung kann das jedoch nicht nachvollziehen, denn diese erstellt immer nur monatliche Rechnungen. Außerdem wurden von allen Kunden wie erwartet monatliche Geldeingänge verzeichnet, weswegen deren Beschwerden bisher nicht nachvollziehbar waren.

Eine tiefere Nachforschung ergibt nun, dass das Problem nur bei Kunden auftritt, die ihre Rechnungen per E-Mail erhalten – von Kunden, die noch auf Postzustellung setzen, gab es bis jetzt noch keine Beschwerden. Sie werden daher gebeten, sich mit einigen der Kunden in Verbindung zu setzen und sich die besagten E-Mails einmal zuschicken zu lassen, um der Sache auf den Grund zu gehen.

1. Während Sie auf die Informationen von den Kunden warten, nutzen Sie die Gelegenheit einmal Ihr Wissen über E-Mail-Kommunikation und das SMTP-Protokoll zu erneuern.

   Informieren Sie sich über das `dig`-Programm[2], und nutzen Sie es um DNS-Einträge der Domain `uni-luebeck.de` auszulesen.

   Welche SMTP-Server sind für das Annehmen von E-Mails an `@uni-luebeck.de` zuständig? Geben Sie den/die Hostname(n) an.

2. Die Kunden haben Ihnen nun endlich einige der E-Mails mit den fragwürdigen Rechnungen zukommen lassen. Auf den ersten Blick sehen diese E-Mails genauso aus wie die nachweislich von ITS verschickten: Aussehen und Inhalt sind originalgetreu nachempfunden, und der Absender ist immer `rechnung@its-hosting.com`. Unterschiede gibt es nur bei der in den Rechnungen angegebenen Kontonummer, und bei der IP-Adresse des versendenden SMTP-Servers.

   Erklären Sie, wie die Betrüger hier vorgegangen sind, und wie sich dies verhindern lässt. Informieren Sie sich über die Architektur von SMTP und das *Sender Policy Framework* (SPF).

[2] `dig` ist ein Standardprogramm, das auf den meisten Linux-Systemen verfügbar sein sollte, inklusive den Uni-Poolrechnern und WSL.

Analysieren Sie als Beispiel den entsprechenden DNS-Eintrag von `uni-luebeck.de`. Welche Server dürfen E-Mails mit der Absenderdomain `uni-luebeck.de` versenden?

3. Nachdem Sie den Grund für die merkwürdigen Rechnungen gefunden haben, legt Techniker Tim einen entsprechenden SPF-Record in der DNS-Konfiguration von `its-hosting.com` an, der die IP des von Kunden und Buchhaltung genutzten SMTP-Servers enthält. Dies scheint auch erfolgreich zu sein, denn eine Woche lang tauchen keine E-Mails mit merkwürdigen Rechnungen mehr auf. Danach geht es allerdings wieder los – erneut haben die (nun vorgewarnten) Kunden zahlreiche E-Mails mit gefälschten, aber sehr echt aussehenden Rechnungen im Postfach.

   Nun scheinen die E-Mails jedoch von ITS' eigenem SMTP-Server zu stammen, die Buchhaltung beteuert aber, diese nicht verschickt zu haben. Was könnte hier passiert sein?