



FÜR EINSTEIGER

PETE HERZOG
NICOLAS MAYENCOURT
PHILIPP EGLI

Schwierigkeitsgrad:



OSSTMM 3.0

Das Open Source Security Testing Methodology Manual (OSSTMM) ist in den letzten Jahren zum de facto Standard zur Überprüfung der operativen Sicherheit avanciert. Vor dem Release der neuen Version 3 haben sich Pete Herzog, Nicolas Mayencourt und Philipp Egli an einen Tisch gesetzt, um mit Stift und Papier (haben wir vergessen) und einer guten Geschichte zu erklären, was das neue OSSTMM bringt. Der Entscheid wurde zu Gunsten des perfekten Hacks gefällt – dem grössten Diamantenraub aller Zeiten¹.

An einem Wintertag im Februar 2002 erlebte ein Wächter im Antwerpener Diamantenviertel einen herben Schock, als er in den Vorraum des vermeintlich sichersten Safes der Welt trat. Die tonnenschwere Stahltür stand sperrangel weit offen. Innen Chaos, aufgebrochene Koffer, in Eile liegende Wertsachen. Doch kein Alarm. Ein Telefon mit der Zentrale brachte die unangenehme Gewissheit: „Die Systeme arbeiten normal, keine nennenswerten Vorkommnisse heute Nacht“, hiess es. Es hat

also kein Einbruch stattgefunden, dennoch fehlen Diamanten im Wert eines zweistelligen Millionenbetrags.

Sowohl das drei Tonnen schwere Stahltor als auch sämtliche Kameras, Bewegungsmelder, Wärme- und Lichtsensoren wurden umgangen (Abbildung 1: Der Vorraum zum Tresor mit Sicht auf die Sicherheitsmechanismen). Wie konnte das passieren? Eines steht bereits fest, wäre die aktuelle Sicherheitssituation besser analysiert worden, wären die Schwachstellen, die zum Einbruch geführt haben, ersichtlich gewesen. Wir wollen uns in den nächsten Minuten in die Position der Angreifer versetzen, um verstehen zu können wie der Angriff zu Stande gekommen ist. Die Rolle des Analysten ist identisch mit der des Angreifers, denn nur, wer den Feind kennt und versteht kann sich angemessen verteidigen.

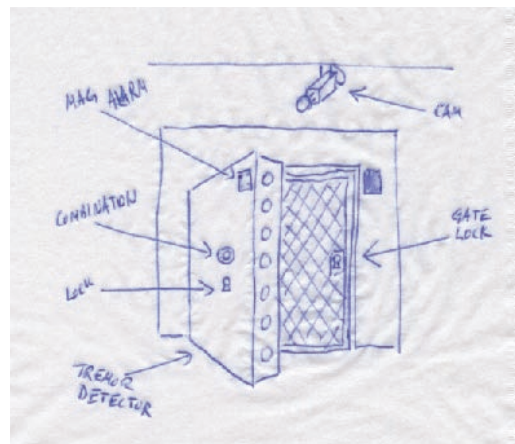


Abbildung 1. Der Vorraum zum Tresor mit Sicht auf die Sicherheitsmechanismen

Ocean's Eleven Explained

Spektakuläre Überfälle auf Safes aller Bauarten gehören zum Standardinventar von Hollywood. Es handelt sich hierbei sicherlich nicht um reine Fiktion. George Clooney als Archetyp des sympathischen Bankräubers hat sein Vorbild in der Realität.

Ein knappes Jahr vor dem Jahrhundertraub. Leonardo Notarbartolo schlürft seinen Espresso in der

IN DIESEM ARTIKEL
ERFAHREN SIE...

was OSSTMM ist.

WAS SIE VORHER
WISSEN/ KÖNNEN
SOLLTEN...

kein spezielles Vorwissen.

¹ Quelle: Wired Magazin: http://www.wired.com/politics/law/magazine/17-04/ff_diamonds

Antwerpener Innenstadt. Vor kurzem hat er sich ein Büro im Diamantenviertel gemietet, um in Italien gestohlene Diamanten in Umlauf zu bringen. Er genießt die ersten Sonnenstrahlen. Der Mann hat eine angenehme Erscheinung. Mit ruhiger, sonorer Stimme und einem unverkennbaren italienischen Akzent ruft er dem Kellner zu „zahlen, bitte“. Eine junge Frau lächelt ihm zu, er lächelt kurz zurück, klemmt seine „Gazzetta dello Sport“ unter den

Safety vs. Security

Das ist ein grundlegendes begriffliches Problem. Zentral für die Durchführung von Sicherheitstests ist die Definition des Begriffs „Sicherheit“. Das OSSTMM nimmt eine Nuance auf, die in der Deutschen Sprache nicht exakt wiedergegeben werden kann. Es wird unterschieden zwischen „Safety“ und „Security“. Die beiden Begriffe erhalten ihre Bedeutung im Kontext des bedrohten Wertes.

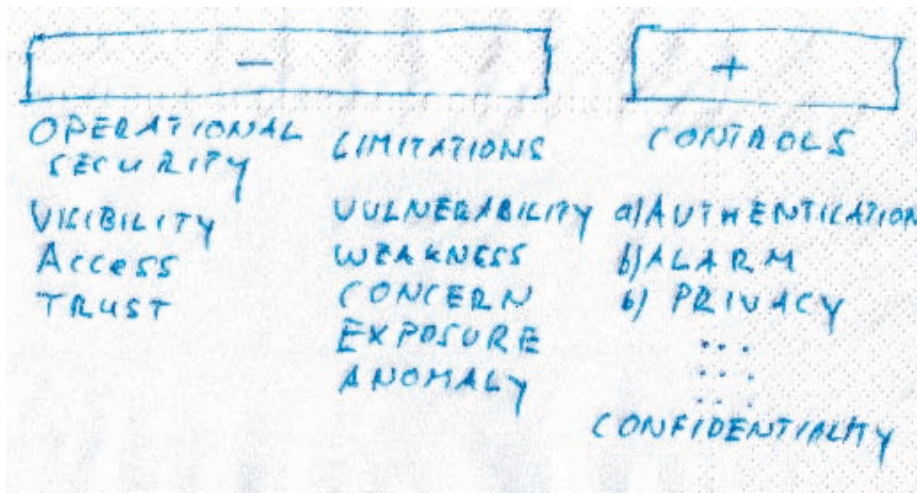


Abbildung 1. Die Kategorien nach OSSTMM

Arm und schlendert die belebte Strasse hinunter. Dieser Mann ist einer der genialsten und tragischsten Diebe der Neuzeit. Doch dazu später mehr: Mit einer Miniaturkamera ausgestattet begibt er sich in den schwer gesicherten Safe zwei Stockwerke unterhalb des Antwerpener Diamantenzenters. Die Bilder, die er dort aufnimmt, dienen seinem Auftraggeber dazu, einen perfekten Nachbau des Safes zu erstellen. Pikantes Detail: Notarbartolo hält mit seiner Kamera auch fest, wie der Wächter den Zugangscode eingibt (nur einer der Sicherheitsmechanismen, um in den Saferaum zu gelangen).

Was muss ich wissen?

Stoppen wir an dieser Stelle die Geschichte. Das, was Leonardo tut ist einer der ersten Schritte eines Angreifers: Er identifiziert mögliche Angriffspunkte. In langer Vorarbeit sammelt er Details und Bilder, um sich auf den Angriff vorzubereiten. Warum hat dieser Mann Zutritt zu diesem sicheren Safe? Weil er ein sympathischer Geschäftsmann ist, den jeder im Viertel kennt, und weil er ein Kunde ist und ein eigenes Schliessfach im Safe besitzt. Und weil ein Safe nur den Nutzen hat, dass Menschen Wertsachen dort deponieren.

„Security“ bezeichnet die physikalische Trennung von Wert und Bedrohung: Ein Safe kommt diesem Bild eigentlich sehr nahe, aber es bestehen dennoch Interaktionsmöglichkeiten. Leonardo, der Diamantenräuber steht in einem Saferaum, der bis oben hin gefüllt ist mit Diamanten. Das ist die Realität, denn in der Praxis lässt sich die Bedrohung nie vollständig vom Wert trennen. Im operativen Umfeld haben wir es mit Sicherheit im Sinne von „Safety“ zu tun. Dieser Zustand wird im OSSTMM als „Operational Security“ bezeichnet. Damit ist die Tatsache gemeint, dass immer ein Mangel an Sicherheit gegeben sein muss, damit etwas interaktiv, nützlich, oder zugänglich ist. Der Grad des Mangels an Sicherheit wird als Durchlässigkeit „Porosity“ bezeichnet. Die Durchlässigkeit wird definiert durch Sichtbar-

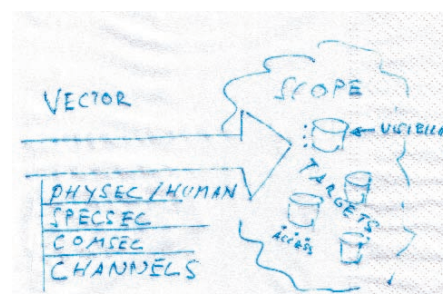


Abbildung 2. Überblick über die Elemente eines Sicherheitstest

keit (Visibility), Zugang (Access) und Vertrauensstellung (Trust). Hundertprozentige Sicherheit besteht also darin, Sichtbarkeit, Zugang und Vertrauensstellungen zu eliminieren. Mit dem kleinen Makel, dass keine Interaktion mehr möglich ist.

Die Qualität von Sicherheitsmechanismen

Wochenlang wird für den bisher grössten Diamantenraub geübt. Das Team besteht aus einem Experten für Schlösser, einem Fahrer, und einem Mann, den sie „Monster“ nennen. Ein Hüne von ungeheurer körperlicher Kraft und gleichzeitig genialer Handwerker und Elektriker. Das Team analysiert die verschiedenen Interaktionsmöglichkeiten. Jeder der Experten kennt die „Tasks“, die zur Erledigung seiner Aufgaben notwendig sind und hat eine eigene Form von Kreativität entwickelt, um die gestellten Aufgaben zu lösen. Einen Tag vor dem Überfall begibt sich Leonardo in den Saferaum, um an sein Fach zu gelangen, besprüht den Bewegungs- und Wärmesensor (10) mit einem handelsüblichen Haarspray. Und richtet der Frau und den Kindern des Wächters im Vorbeigehen Grüsse aus.

Controls vs. Limitations

Das OSSTMM geht davon aus, dass Interaktionsmöglichkeiten durch Sicherheitsmassnahmen beschränkt oder nur für bestimmte Personengruppen zugänglich gemacht werden. Sicherheitsmechanismen werden als „Controls“ bezeichnet. Hierbei sind die Mechanismen in zwei Klassen unterteilt: Einerseits in interaktive Sicherheitsmechanismen (Class A), welche direkt auf die Interaktionsmöglichkeiten einwirken. Bei der anderen Gruppe (Class B) handelt es sich um generelle Defensiv-Massnahmen (Abbildung 1: Die Kategorien nach OSSTMM). Der Bewegungs- und Wärmesensor überwacht den Zutritt zu Tresorraum, und sollte Alarm schlagen, wenn unerlaubter Zutritt erfolgt. Es handelt sich also um ein „Control“ der Klasse B, konkret um das „Alarm Control“. Das „Control“ kann aber umgangen werden, indem es mit Haarspray eingesprüht wird und indem – wie wir später sehen werden – der Sensor überbrückt wird.

Wenn die Funktionalität eines „Controls“ eingeschränkt oder komplett neutralisiert wird, spricht das OSSTMM von „Limitations“. Das Vorhandensein von „Limitations“ wirkt sich negativ, das Vorhandensein von „Controls“ posi-

OSSTMM in drei Schritten

Open Source **Security Testing** Methodology Manual

Die grundlegenden Anforderungen an einen Sicherheitstest werden erfüllt. Ein Wert wird geschützt. Eine Funktionalität wird sichergestellt.

Open Source Security Testing Methodology Manual

Das OSSTMM ist eine offene Methodologie. Das heisst, es wird von einer internationalen Community getragen und aktiv gepflegt. Dies führt zu mehr Transparenz; sämtliche Inhalte der Methodologie liegen offen und können diskutiert werden. Die Unabhängigkeit der Methode von staatlichen Interessen oder Interessen der Industrie ist gewährleistet.

Dies führt in einem weiteren Schritt zu einer besseren Anwendbarkeit in der Praxis, da unabhängige und transparente Resultate erzielt werden und es wird sichergestellt, dass Wissen und Erfahrung der Anwenderinnen in die aktuellen Versionen des OSSTMM einfließen werden.

Nicht zuletzt ist eine offene Methodologie interessant für jegliche Art von Forschung. Dies reflektiert sich in einem breiten Interesse verschiedener Akademien, Fachhochschulen und Universitäten weltweit. Zertifizierungskurse nach OSSTMM sind universitär akkreditiert und entsprechen einer bestimmten Anzahl ECTS-Punkten (European Credit Transfer System). Das OSSTMM steht in vielen Hochschulen, die eine zeitgemässe Informatikausbildung anbieten, auf den Lehrplänen - Tendenz steigend.

Open Source Security Testing **Methodology Manual**

Das OSSTMM beinhaltet eine Sammlung von Vorgaben bis hin zu den einzelnen „Tasks“, die zur Durchführung von Sicherheitstests notwendig sind. Mit dem Risk Assessment Value steht eine KPI zur Verfügung, mit deren Hilfe sich die operative Sicherheit messen und abbilden lässt. Eine klar definierte Metrik führt in jedem Fall zu einer besseren Vergleichbarkeit von Resultaten sowie zu einer Vereinfachung der Erfolgskontrolle der umgesetzten Sicherheitsmassnahmen.

Ein weiteres zentrales Element bilden die „Rules of Engagement“. Sie beinhalten ethische und legale Richtlinien, die für alle OSSTMM zertifizierten Personen und nach OSSTMM durchgeführten Tests verbindlich sind. Eine positive und konstruktive Grundhaltung gegenüber Sicherheit spiegelt sich in den Rules of Engagement wider. Der Einsatz von FUD (fear, uncertainty and doubt) für Marketingzwecke ist untersagt.

Das Ziel ist „Perfect Security“. Wobei der Begriff „perfect“ auf Deutsch treffend mit dem Wort „angemessen“ übersetzt wird. Das OSSTMM hat zum Ziel, angemessene Sicherheit zu schaffen. Das bedeutet, den Wert der eigenen Assets zu kennen und in jedem Fall angemessen und kosteneffizient zu schützen.

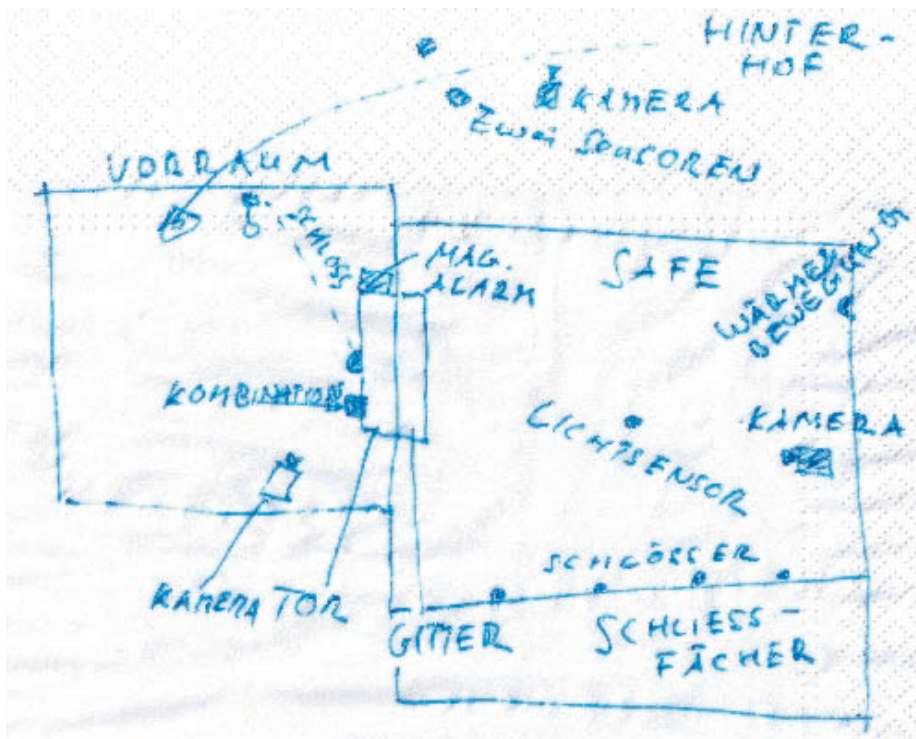


Abbildung 3. Schematische Darstellung des Diamantenraubs

tiv auf die operationelle Sicherheit aus.

Gelingt es einem Angreifer einen Zugang zu erlangen, den Zugang für Dritte zu blockieren oder sich innerhalb des Zieles festzusetzen, spricht das OSSTMM von Verwundbarkeit (Vulnerability). Weitere Kategorien sind die „Weakness“ (Schlecht ausgeführte oder nicht vorhandene „Controls“, die direkt auf die Interaktionsmöglichkeiten einwirken). Oder der „Concern“, der dann eintritt, wenn „Controls“ der Klasse B nicht korrekt umgesetzt oder nicht vorhanden sind. Als „Exposure“ bezeichnet man die unnötige Preisgabe von Informationen. Um eine „Anomaly“ handelt es sich, wenn Elemente ein nicht erklärbares und für die Funktion nicht relevantes Verhalten aufweisen (Abbildung 1: Die Kategorien nach OSSTMM).

Was muss ich tun?

Das Team um Leonardo scheut keinen Aufwand. Ein Nachbau des Tresorraums steht in einem stillgelegten Einkaufszentrum. Die Ex-

perten analysieren die Zugänge, sie studieren die Funktionsweise der einzelnen Sensoren und suchen nach einem Weg, unbemerkt ins Gebäude einzudringen. Das Sicherheitskonzept weist Schwachstellen auf. Aber wie gelangt man unbemerkt in den Tresorraum. Der Analyst muss seinen Scope kennen. Bevor er beginnt, muss er wissen, auf was er sich einlässt. Er muss das Umfeld und die Interaktionsmöglichkeiten kennen. Und er muss sich entscheiden, mit welchen Mitteln (Channel) er das Ziel angreift (Abbildung 2: Überblick über die Elemente eines Sicherheitstest).

Die Vorbereitung nach OSSTMM umfasst alle Punkte, die auch Leonardo berücksichtigt hat. Jedoch muss im Einklang mit ethischen und legalen Grundsätzen gehandelt werden.

1. Zielsysteme: Definiere die Zielsysteme, die untersucht werden müssen
2. Scope: Definiere alle Faktoren, die auf das Zielsystem einwirken. Das heisst. Umwelteinflüsse, oder technische Abhängigkeiten wie die Stromversorgung, verantwortliche Personengruppen, Gesetzgebungen. Diese Überlegungen bilden die Grundlage für die Definition der Angriffsvektoren.
3. Vektor: Ist der Angriffswinkel auf die Zielsysteme. Soll das Zielsystem von aussen oder von Innen angegriffen werden? Soll ein Angriff von Departement A zu Departement B erfolgen. Soll ein Umsystem kompromittiert werden, um die Funktionalität des Zielsystems indirekt einzuschränken?
4. Channel: Mit welcher Methode soll das Ziel angegriffen werden.

Es muss pro Angriffsvektor entschieden werden, welche möglichen Channels zur Verfügung stehen. Gibt es einen Zugriff über Netzwerk oder Wireless oder kann der Angriff mit Hilfe von Social Engineering erfolgen. Macht es Sinn, einen direkten physikalischen Zugriff anzustreben?

5. Testtyp: Das OSSTMM unterscheidet mehrere Testtypen. Zum Beispiel Black Box Tests (Double Blind). Oder Double Grey – auch White Box Test genannt. Für jeden Test muss festgelegt werden, nach welchem Paradigma er durchgeführt werden soll.
6. „Rules of Engagement“: Für jeden Security Test muss sichergestellt werden, dass gemäss den Rules of Engagement vorgegangen wird. Die „Rules of Engagement“ beinhalten Regeln zur Kommunikation der Resultate, Regeln zur Planung und Durchführung von Sicherheitstests und einen für Analysten und Tester verbindlichen ethischen und legalen Kodex.

Showtime

In der Nacht des Raubes machen sich der Experte für Schlösser und das Monster mit Leitern in einem Vorhof zwei Blocks vom Diamantencenter entfernt zu schaffen. Mit einem Schild aus Polyester umgehen sie den ersten Wärme- und Bewegungssensor, indem sie sich von hinten an das Device anschleichen und dieses deaktivieren. Kameras wer-

den mit schwarzen Müllbeuteln verdeckt. Die zweite Reihe der Sensoren wird deaktiviert.

Die Polizei rätselt bis heute, wie sie in den Vorraum des Safes gelangen konnten. Tatsache ist, dass sie es geschafft haben. Auch nachts werden Heute in der Überwachungszentrale die Kamerabilder durch Sicherheitspersonal überwacht. Dies war zum Zeitpunkt des Überfalls nicht der Fall.

Der Magnet-Sensor, der ein unerlaubtes Öffnen der Türe verunmöglichen soll, kann von Aussen abgeschraubt werden. Die Männer haben zu diesem Zweck eine Vorrichtung aus Aluminium konstruiert. Der Schlüssel für das Hochsicherheitsschloss wird unglücklicherweise im Vorraum des Safes gelagert. Davon profitieren die Männer. Doch bleibt noch die Eingabe für das Zahlenschloss mit 100 Millionen Kombinationsmöglichkeiten und Sichtschutz. Leonardo hat die Kombination gefilmt - bei seinem Besuch vor fast einem Jahr. Der Code ist immer noch gültig. Die Stahltür öffnet sich. Die ganze Aktion spielt sich bei gedämpftem Licht ab. Zu wenig Licht für die Kamera im Vorraum. Doch jetzt schalten die Männer das Licht vollständig aus. Der lichtempfindliche Sensor im Safeinnenraum darf nicht anschlagen. Doch bevor sich die Männer um diesen Sensor kümmern können, bleibt noch das Stahlgitter. Ein zweites Tor, das tagsüber als Sicherung dient, weil die schwere Safetüre zu träge ist und die Kunden über wenig Zeit verfügen. Dieses Schloss ist schnell geöffnet. Ein leichtes Spiel für den Schloss-Experten.

Der Bewegungs- und Wärme-Sensor im Innern des Safe-raums wurde bereits am Vortag ausser Gefecht gesetzt. Dennoch müssen die Män-

Um in das Gebäude zu gelangen			
Schutzmassnahme	Controls	Limitation	Was es bedeutet
Externer Wärme & Bewegungssensor	Alarm	Concern	Der Sensor kann von hinten umgangen und deaktiviert werden.
Weitere externe Bewegungsmelder	Alarm	Concern	Die Sensoren können demontiert werden.
Externe Überwachungskamera	Authentication	Weakness	Die Kamera dient in erster Linie zur Authentifizierung, da in der Nacht die Kameras nicht überwacht werden, kann das Control umgangen werden.
	Alarm	Concern	Der Alarm kann in der Nacht nicht ausgelöst werden.
		Vulnerability	Der Zugang zum Vorraum ist möglich. Bis heute ist nicht genau bekannt wie der Zugang zu Stande kam.

FÜR EINSTEIGER

ner höchst vorsichtig agieren. Langsame Bewegungen, damit nicht zu viel Wärme erzeugt wird. Auch der Lichtsensor muss eliminiert werden. Das Monster macht sich an den

Nur kurz blitzt das Licht auf; wenn sie die Wertsachen in Beutel befördern. Kein brauchbares Bild für die Kameras im Saferaum. Nur die Haupttüre verfügt über einen seismischen

Die Analyse

Der Angreifer und der Analyst befinden sich in der selben Situation. Dass der Safeschlüssel im Vorraum aufbewahrt oder die Kombina-

Vorraum			
Schutzmassnahme	Controls	Limitation	Was es bedeutet
Zahlenschloss mit Schutzvorrichtung für Display	Authentication	Weakness	Das Control kann umgangen werden, da der Code nicht häufig genug geändert wird, so ist der gefilmte Code vom Vortag noch gültig.
	Privacy für Sichtschutz	Concern	Das die Möglichkeit des Filmens besteht, ist ein Verstoß gegen das Privacy Control.
Hochsicherheitsschloss	Authentication	Weakness	Der Mechanismus kann umgangen werden, weil der Schlüssel im Vorraum aufbewahrt wird.
		Vulnerability	Die Türe kann auf diese Weise geöffnet werden, was zum Zutritt führt.
Seismischer Sensor in der Safe-Tür	Alarm		Das Control musste nicht kompromittiert werden, um in den Saferaum zu gelangen
Stahlgitter mit Schloss	Authentication	Weakness	Das Schloss kann geknackt werden.
		Vulnerability	Der Zutritt ist möglich.
Magnetischer Sensor (Überwacht die Öffnung der Safetüre)	Alarm	Concern	Der Sensor kann von der Türe entfernt werden, weil die Schrauben zugänglich sind. Dist ist möglich, ohne das Magnetfeld zu unterbrechen (Concern).
Interne Überwachungskamera	Authentication	Weakness	Die Kamera dient in erster Linie zur Authentifizierung, da in der Nacht die Kameras nicht überwacht werden, kann das Control umgangen werden.
	Alarm	Concern	Der Alarm kann in der Nacht nicht ausgelöst werden.

Verbindungskabeln der beiden Sensoren zu schaffen und überbrückt diese. Bei völliger Dunkelheit öffnen sie die einzelnen Schliessfächer mit einem speziell zu diesem Zweck angefertigten Hochleistungsbohrer.

Sensor. Die Schliessfächer sind ungeschützt und geben ihren Inhalt ohne grossen Widerstand preis. Die Männer tragen Handschuhe, es gibt keine Spuren. Einer der Männer telefoniert: „Wir kommen jetzt raus, Leonardo“...

tion monatelang nicht gewechselt worden ist, sind auffällige Versäumnisse, die einem Analysten nicht entgangen wären. Uns bleibt die Bewertung der Situation: Es gibt zwei Zugänge zum Safe. Den Kundeneingang und den

Vorraum			
Schutzmassnahme	Controls	Limitation	Was es bedeutet
Lichtempfindlicher Sensor	Alarm	Concern	Der Sensor kann überbrückt werden, da die Kabel zugänglich sind. Der Sensor schlägt nur auf bestimmte Wellenlängen an.
Interne Überwachungskamera	Authentication	Weakness	Die Kamera dient in erster Linie zur Authentifizierung, da in der Nacht die Kameras nicht überwacht werden, kann das Control umgangen werden.
	Alarm	Concern	Der Alarm kann in der Nacht nicht ausgelöst werden.
Wärme und Bewegungssensor	Alarm	Concern	Der Sensor konnte am Vortag mit handelsüblichen Harspray ausser Gefecht gesetzt und später überbrückt werden.
Schlösser der Einzelsafes	Authentication	Weakness	Das Schloss kann mit einem Hochleistungsbohrer aufgebohrt werden.
		Vulnerability	Der Zugang zu den Wertsachen ist möglich.

Eingang, den die Diebe benutzt haben und der bis zum heutigen Tag unbekannt ist. Das heisst, es gibt zwei Accesses. Auch, dass Leonardo Zugang zum Safeinnenraum hatte, wird als Access gewertet. Das Ziel ist sichtbar, das heisst, wir zählen eine Visibility. Die Controls und die Limitations zählen wir zusammen und übertragen sie ins RAV-Sheet.

Es folgt die Berechnung des Risk Assessment Values. Hierbei ist anzumerken, dass die Weaknesses, die bei den Kameras vergeben worden sind, nur einmal gezählt werden, da bei allen Kameras das Fehlen einer Wachperson, die das Geschehen an den Monitoren auswertet, die Ursache für die Weakness ist. Die Concerns werden voll gezählt, da jede der Kameras über mangelhafte Nachtsichteseigenschaften verfügt.

Der Risk Assessment Value muss als KPI (Key Performance Index) zur Bemessung der operativen Sicherheit gesehen werden. Als Grundlage dient der für jeden Test bereits definierte Scope und die Angriffsvektoren. Bei einem Sicherheitstest nach OSSTMM wird analysiert (je nach CHANNEL mit unterschiedlichen Mitteln), welche der genannten Kategorien vorhanden sind. Dabei wird lediglich ihr Auftreten „gezählt“. Für Operational Security bedeutet dies, dass alle Visibilities, alle Accesses und alle Trusts pro Vektor gezählt werden. Das selbe gilt für die Controls und deren Limitations. Auf dieser Datengrundlage funktioniert der Risk Assessment Value wie eine Waage: Negativ ins Gewicht fallen die Operational Se-

curity, das heisst die grundsätzliche Durchlässigkeit des Zielsystems und die Limitations, das heisst Mängel auf den umgesetzten Controls. Positiv wirken sich die Controls aus (Abbildung 1: Die Kategorien nach OSSTMM). Um den negativen Effekt einer Durchlässigkeit (Operational Security) eines System vollständig aufzuwiegen sind 10 Controls notwendig.

Was bleibt

Auf der Flucht verlieren die Männer die Nerven und hinterlassen Säcke mit Beute und Dokumenten im Wald. Ein braver Bürger, der sich über die Jugendlichen aufregt, die in diesem Waldstück immer Müll deponieren, verrät Leonardo ohne es zu wissen. Als er erwähnt, dass es sich beim Abfall um Umschläge des Diamantencenters handelt, wird der Polizist am Telefon hellhörig. Die Beamten rekonstruieren aus Papierschnipseln ein Dokument: Die Kaufquittung für die Miniaturkamera der Name Notarbartolo ist darauf klar lesbar. Leonardo ist überführt. Als er in den nächsten Tagen nach Antwerpen zurückkehrt, ist die Polizei bereits alarmiert. Für Leonardo hatte dies naturgemäss Konsequenzen. Er verbüsste eine mehrjährige Haftstrafe. Am 24. März 2009 wurde er entlassen (Autogrammadresse den Autoren nicht bekannt). Bei seinem Auftraggeber handelt es sich wahrscheinlich um einen Versicherungsbetrüger.

Mit Hilfe einer Analyse nach OSSTMM wäre klar ersichtlich gewesen, dass die massiven Schutzmassnahmen nicht den gewünsch-

ten Effekt haben. Die aufgezeigten Limitations führen zu einem Risk Assessment Value der kleiner als 90 % ist. Für eine Umgebung mit höchsten Ansprüchen an die Sicherheit ist dies zu wenig. Durch die klare Vorgehensweise bei der Analyse können auch klare Behebungsmaßnahmen angegeben werden. Nicht zuletzt kann eine solche Analyse dazu verwendet werden, um aufzuzeigen, dass das Risiko einer Kompromittierung der Sicherheit im Falle eines Angriffs sehr hoch ist. Wir hätten die Verantwortlichen gerne beraten...

Über die Autoren:

Pete Herzog: Gründer von ISECOM und Herausgeber des OSSTMM

Nicolas Mayencourt: Schweizer Sicherheitspionier und CEO von Dreamlab Technologies AG

Philipp Egli: Analytischer Philosoph und Sicherheitsexperte bei Dreamlab Technologies AG

Weitere Infos:

www.isecom.org

www.osstmm.org,

www.dreamlab.net