IT-Grundschutz-Kompendium des BSI

iX KOMPAKT
Herbst 2020
Ein Sonderheft des Magazins für professionelle Informationstechnik

IT-SICHERHEIT

14,90 €
Österreich 16,40 €
Schweiz 27.90 CHF
Luxemburg 17,10 €
www.ix.de

Ende des Privacy Shield: Konsequenzen für Unternehmen

DSGVO-Fallstricke im IT-Alltag

Cyberrisiken im Griff

Den Krisenfall meistern

Pentests vs. Datenschutz

Notfallmanagement

Produkte für Endpoint Security

KI als Angriffsziel und Tatwerkzeug

Zwei-Faktor-Authentifizierung bedroht

Pentesting in der Cloud

Sicherheitsmanagement: **ISMS-Tutorial**

Awareness: Es mangelt an Gefahrenbewusstsein

Risikofaktor Mensch

TECHNISCHE HOCHSCHULE DEGGENDORF

Akademische Weiterbildung

MASTER CYBER SECURITY

MEHR CYBER-SICHERHEIT IN IHREM UNTERNEHMEN

Für Ingenieure und Informatiker

5 Semester berufsbegleitend

2-3 Blockvorlesungen pro Semester

Themen aus den Bereichen Industrial & Automotive

Berufsbegleitend weiterbilden | www.th-deg.de/weiterbildung | peter.apfelbeck@th-deg.de | Tel. 0991 36 15 - 425

Aktivposten Sicherheit

Wer Hacking, Phishing und Ransomware bisher nur für recht theoretische Bedrohungen von IT-Firmen hielt, wurde spätestens durch die zahlreichen Schlagzeilen zu Emotet, Shitrix & Co. eines Besseren belehrt. Große Unternehmen aus allen möglichen Branchen mussten bereits vorübergehend ihren Betrieb einstellen oder – wie der Heise-Verlag selbst – ihre Netzwerk-Infrastruktur neu einrichten. Und es geht nicht nur um monetäre Schäden: Die Uniklinik Düsseldorf konnte keine Notfälle mehr aufnehmen und eine Patientin starb möglicherweise, weil sie in ein weiter entferntes Krankenhaus gebracht werden musste.

In solchen Fällen stellt sich im Nachhinein meist heraus, dass es zum Schutz der Organisationen, Kunden und Patienten nicht nur einer guten und aktuellen IT-Sicherheitstechnik bedarf, sondern auch einer besseren Aufklärung aller IT-Anwender. Die teuersten und besten Sicherheitsprodukte nützen nichts, wenn das bloße Öffnen eines E-Mail-Anhangs dazu führt, dass Kriminelle Zugriff aufs gesamte Unternehmensnetz und die gespeicherten Daten erhalten, diese verschlüsseln und dann viel Geld für die Herausgabe des Schlüssels erpressen. Und wer Kriminelle bezahlt, weiß nicht nur nicht, ob er die Daten dadurch wiedersieht, sondern kann sich sogar selbst strafbar machen.

Besser ist es, vorbeugend aktiv zu werden, die Schwachpunkte in der eigenen IT ausfindig zu machen und sich nicht zu scheuen, professionelle Unterstützung ins Haus zu holen – sogar im Wortsinne: Das Einschätzen und Minimieren von Risiken und Bedrohungen geht bis hin zum Red Teaming, dem Einbruch auf Bestellung.

Apropos strafbar und teuer: Die Sicherheit der Daten ist eng verknüpft mit rechtlichen Fragestellungen rund um den Datenschutz. Die konkrete Umsetzung der Datenschutz-Grundverordnung (DSGVO) seit anderthalb Jahren einerseits und der lasche Umgang mit Kundendaten andererseits haben bereits zu schmerzhaften Bußgeldbescheiden geführt. Auch dieses Thema müssen die Verantwortlichen aktiv angehen, bevor es teuer wird. Es erhält daher im vorliegenden iX-Sonderheft seinen Platz.

BERT UNGERER

Sichere Symbole

Seit Jahrtausenden wenden Menschen allerlei Kreativität und technische Errungenschaften dafür auf, wertvolle Dinge und Informationen vor dem Zugriff durch andere Menschen zu schützen. Ausgeklügelte mechanische Schlösser und Schlüssel verlieren im Zeitalter der Digitalisierung zwar allmählich an praktischer Bedeutung, ihre Symbolkraft aber bleibt. Sie sind daher in zahllosen Berichten über die sonst schwer darstellbare IT-Sicherheit zu bewundern – so auch im vorliegenden Heft. Das Titelbild und sämtliche Aufmacherfotos hat uns dankenswerterweise die Schell Collection aus Graz zur Verfügung gestellt, das österreichische Museum für Schlösser, Schlüssel, Kästchen und Eisenkunstguss.

Awareness

Sind Sie sicher? Damit kein echter Einbruch mit weitreichenden Folgen stattfindet, müssen Anwender und ITler über die Gefahren und Bedrohungen durch Schwachstellen und Hacker aufgeklärt sein – und darüber, wie sie mit ihrem eigenen Verhalten dazu beitragen können, dass es gar nicht erst zum Schlimmsten kommt. Zu den besonders aufwendigen, aber auch besonders nachhaltigen Testmethoden gehören Red und Blue Teaming: Einbrüche „auf Bestellung“ und deren Abwehr.

ab Seite 6

Awareness

Sicherheitstests

Herausforderungen im Rahmen von Red Team Assessments 6

Blue Teaming: Wie man die Verteidigung gegen Internetangriffe übt 12

Phishing

Awareness-Projekt der Landeshauptstadt Kiel 16

Internetkriminalität

CEO-Fraud: Wenn der „Chef“ zur Geldüberweisung auffordert 22

Datenschutz & Recht

Nach dem Privacy Shield

Rechtliche und technische Maßnahmen 24

Nach EuGH-Urteil: Unternehmen müssen Software und Dienste überprüfen 30

IT-Recht

Cyberrisiken: Wer für die Schäden einstehen muss 36

Datenschutzfallstricke im IT- und Entwickleralltag 40

Bußgeldverfahren im Datenschutz: ein Überblick 44

Compliance

Notfallmanagement

Brenzlige Situationen in der IT überstehen 48

BSI-Standardwerk

Update des IT-Grundschutz-Kompendiums 52

Informationssicherheit

Risikomanagement nach ISO/IEC 27005 58

Tutorial, Teil 1: Aufbau eines ISMS – Erste Schritte 64

Tutorial, Teil 2: Aufbau eines ISMS – Risikomanagement 70

Tutorial, Teil 3: Aufbau eines ISMS – prüfen und verbessern 74

Rechtssicherheit

Datenschutz bei Einbruchtests 80

Markt & Produkte

Risiken managen

Marktübersicht: Cyberversicherungen 84

Gerätesicherheit

Marktübersicht: Neue Techniken der Endpoint-Security 96

Cloud-Security

Mobile Nutzer und Cloud-Strukturen schützen mit Cisco Umbrella 110

Know-how & Praxis

Sicherheit

Gefahren durch Angriffe auf und mit KI 114

Muraena und NecroBrowser hacken Zwei-Faktor-Authentifizierung 118

Wie KI bei der Absicherung des IoT helfen kann 124

SAP-Basiswissen – ein kleines Kompendium 130

Angriffssimulation

Die Post-Exploitation Frameworks Koadic und Merlin 134

Penetration-Tests in der Cloud 143

Sonstiges

Editorial 3

Impressum 127

Inserentenverzeichnis 127

Datenschutz & Recht

2019 und 2020 waren nicht nur von Angriffen auf IT-Systeme geprägt, sondern auch von der Umsetzung der Datenschutz-Grundverordnung (DSGVO) – und nicht zuletzt vom gerichtlich erzwungenen Ende des Privacy-Shield-Abkommens zwischen der EU und den USA. Wie sich hohe Bußgelder vermeiden lassen und was nach dem Privacy Shield kommt,

ab Seite 24

Compliance

Zur Umsetzung geltenden Rechts oder für das Krisenmanagement muss kein ITler dicke Gesetzestexte und abstrakte Kommentare in juristischen Fachzeitschriften lesen, denn es existieren konkrete Normen und Best-Practice-Anleitungen etwa vom Bundesamt für Sicherheit in der Informationstechnik. In einem ISMS-Tutorial zeigt die iX, wie sich Risiko- und Sicherheitsmanagement im Unternehmen implementieren lassen.

ab Seite 48

Markt & Produkte

Mit den IT-Bedrohungen wächst das Bedürfnis nach einer Absicherung für den schlimmsten Fall. Cyberversicherungen tragen dem Rechnung. Um eventuelle Schäden möglichst zu begrenzen, sollte aber auch ein Blick auf den Schutz der unüberschaubaren Zahl an Endgeräten nicht fehlen, den die Marktübersicht zur Endpoint Security erleichtert.

ab Seite 84

Know-how & Praxis

Künstliche Intelligenz, Internet der Dinge, Cloud Computing: Nicht nur die Liste der IT-Themen wächst rasch, sondern auch deren Bedeutung für den Alltag der Menschen – und damit die Risiken im Angriffsfall. An konkreten Beispielen zeigt sich, welche Mittel potenziellen Tätern heute zur Verfügung stehen, aber auch, wie man ihnen zuvorkommen kann.

ab Seite 114

Herausforderungen im Rahmen von Red Team Assessments

Angriffspläne

Joshua Tiago

Bevor die Sicherheitsverantwortlichen in einem Unternehmen eine Angriffssimulation durch ein Red Team veranlassen, gilt es, deren Ziele und Prüftiefe möglichst detailliert festzulegen. Sinnvoll kann es auch sein, das verteidigende Blue Team gleich mitzuschulen.

Um die Wehrhaftigkeit eines Unternehmens gegen Angriffe zu prüfen, haben sich in den letzten Jahren sogenannte Red Team Assessments etabliert – also Angriffssimulationen durch ein externes Expertenteam. Bevor die Verantwortlichen ein solches Red Team Assessment veranlassen, gilt es, einige Aspekte zu berücksichtigen und in die Planung einzubeziehen (siehe Kasten „Fragen vor Beginn ...“). Planungs- und Entscheidungsphase bergen sowohl für den Auftraggeber als auch für den Dienstleister einige Herausforderungen. Am Anfang steht immer die Frage, warum ein Red Team Assessment stattfinden soll. Die Antwort „Wir möchten die Sicherheit unseres Unternehmens erhöhen“ ist in diesem Kontext nicht immer zielführend. Ohne Frage, Red Team Assessments erfreuen sich immer größerer Beliebtheit. Dennoch sind manchen Sicherheitsverantwortlichen die relevanten Unterschiede zwischen einem Red Team Assessment und einem Penetrationstest nicht klar.

Erschwerend kommt hinzu, dass inzwischen viele IT-Sicherheitsfirmen Red Team Assessments anbieten. Ein genauer Blick offenbart oftmals, dass die angebotenen Leistungen nur bedingt als Red Team Assessment bezeichnet werden können. In einigen Fällen werden umfangreiche Penetrationstests, die zum Ziel haben, möglichst viele Schwachstellen in der Breite aufzudecken, fälschlicherweise als Red Team Assessment angeboten. Daher sollte man solche Dienstleistungen stets kritisch hinterfragen und darauf achten, dass der Dienstleister für diese Art der Prüfung Erfahrung und Sachkenntnis vorweisen kann. Doch wann ist es angebracht, ein Red Team Assessment zu beauftragen, und wann reicht ein Penetrationstest aus? Eine Gegenüberstellung beider Prüfungsarten liefert eine erste Antwort.

Zwei verschiedene Verfahren

Penetrationstests sind zielgerichtete Prüfungen zum Feststellen der aktuellen Sicherheit einer Anwendung, eines Systems oder einer Netzwerkumgebung. Der konkrete Prüfgegenstand ist sehr unterschiedlich, angefangen von Webapplikationen (siehe auch iX 7/2019, Seite 46) und mobilen Apps über Netzwerkprotokolle bis hin zu IoT-Geräten. Dabei sucht ein erfahrener Penetrationstester Schwachstellen und nutzt sie aus, um die Verantwortlichen bei der Risikoeinschätzung ihrer Systeme oder Applikationen zu unterstützen. Abschließend empfiehlt er Maßnahmen, mit denen sich die Schwachstellen beheben lassen oder die zumindest ihr Gefährdungspotenzial minimieren.

Ein Beispiel dafür könnte sein, dass eine Bank ihre Onlinebanking-Anwendung überprüfen lassen möchte. Ein Penetrationstest würde sich in diesem Fall ausschließlich auf die Webapplikation beschränken und der Prüfer nach potenziellen Schwachstellen suchen, die ein Angreifer ausnutzen kann. Für die Gesamtsicherheit der Bank ist diese Anwendung sicherlich eine wichtige Komponente, aber eben nicht die einzige. Dennoch sind Penetrationstests sinnvoll. Wenn zum Beispiel eine neue Version der Webapplikation entwickelt wurde oder sich der Aufbau der Architektur des Onlinebankings gravierend verändert hat, lohnt sich eine solche Überprüfung.

Ein Red Team Assessment unterscheidet sich von einem Penetrationstest in mehreren Punkten. Der größte Unterschied besteht darin, dass nicht eine Anwendung oder ein System, sondern alle Entitäten eines Unternehmens gleichermaßen im Visier sind. Dabei spielt es keine Rolle, ob es sich um ein IT-System, einen Mitarbeiter, einen Standort oder auch ein Unternehmen in der Holding-Struktur handelt. Es werden nicht nur die technischen Systeme auf eine Möglichkeit zur Kompromittierung untersucht. Vielmehr handelt es sich um einen ganzheitlichen Ansatz, der alle möglichen Einfallstore eines modernen Unternehmens berücksichtigt.

Dazu zählt unter anderem auch das physische Eindringen in die Räumlichkeiten,

Fragen vor Beginn eines Red-Team-Assessment-Projekts

- Was sind die konkreten Ziele des Red Team Assessments?
- Können die Ziele auch mit einem im Umfang beschränkten Penetrationstest erreicht werden?
- Sollen festgelegte Szenarien im Rahmen des Projekts simuliert werden? Wenn ja, welche?
- Sollen bestimmte Angriffstechniken, Methoden oder Personenkreise aus dem Prüfungsumfang ausgeschlossen werden?
- Falls einige Methoden und Szenarien ausgeschlossen werden sollen, ist die Aussagekraft der Ergebnisse ausreichend relevant?
- Wer soll über die geplante Prüfung unterrichtet werden?
- Wurden bereits Erkennungstechnologien und Prozesse eingeführt, um die zu simulierenden Angriffe zu erkennen und zu unterbinden?
- Welche Angriffe sollten definitiv erkannt werden?
- Falls das Blue Team informiert werden soll, welche Informationen über Art, Umfang und Zeitraum der Angriffe sollen bekannt gegeben werden?
- Soll die Reaktion des Blue Teams auf die Angriffe beobachtet und bewertet werden? Über welchen Zeitraum soll sich die Prüfung erstrecken?

das es einem Angreifer erlaubt, einen besseren Zugriff auf die IT-Systeme zu erhalten. Erfolgreiche Angriffe auf die Mitarbeiter erleichtern ebenfalls den Zugriff auf die Infrastruktur, Systeme oder sensible Daten. Daher gibt es auch nur wenige Einschränkungen, wie weit ein Red Team Assessment gehen darf. Während der Tester bei einem Sicherheitsaudit lediglich auf Schwachstellen hinweist und sie meist nicht ausnutzt, steht gerade Letzteres bei einem Red Team Assessment im Vordergrund.

Hier werden Schwachstellen geschickt kombiniert und aktiv ausgenutzt, um sich einen Vorteil für einen Angriff zu verschaffen. Diese Art von Prüfung dient nicht dazu, möglichst viele Schwachstellen zu identifizieren. Es reicht in der Regel, nur die eine schwerwiegende Schwachstelle oder die Kombination aus mehreren Schwachstellen zu finden, die es erlaubt, einen Teil der Infrastruktur zu übernehmen. Ein weiterer Unterschied liegt in der Dauer und dem zeitlichen Ablauf des Projekts. Während ein Penetrationstest über einen bestimmten Zeitraum stattfindet, meist ein bis zwei Wochen, läuft ein Red Team Assessment weniger linear ab. In der Regel erstreckt es sich über einen längeren Zeitraum, in dem immer wieder einzelne Angriffssimulationen oder -schritte stattfinden.

Welche Prüfung für wen?

Wenn man diese Unterschiede betrachtet, wird nachvollziehbar, warum ein Red Team Assessment nicht für alle Unternehmen und in allen Situationen die bessere Variante ist. Da dabei alle relevanten Sicherheitsmechanismen und Prozesse abgeklopft werden, um ein Eindringen zu erreichen, ist eine solche Prüfung nur dann sinnvoll, wenn das betreffende Unternehmen bereits die grundlegenden Aufgaben im Bereich IT-Sicherheit erledigt hat und hoher Schutzbedarf besteht.

Um beim Beispiel der fiktiven Bank zu bleiben, folgendes Szenario: Die Bank hat in den vergangenen Jahren viel Zeit, Personal und Geld in das Thema IT-Sicherheit investiert. Es kommen diverse Schutzmechanismen zum Einsatz, Erkennungstechniken wurden eingeführt und Prozesse definiert. Nun möchte die Bank einschätzen, wie es um die Gesamtsicherheit bestellt ist. Gibt es Einfallstore, die nicht berücksichtigt wurden? Sind die Mitarbeiter ausreichend sensibilisiert worden? Gibt es Angriffsketten, die nicht bekannt sind? All diese Fragen lassen sich im Rahmen eines Red Team Assessments beantworten.

Obwohl nur bedingt Einschränkungen für solche Prüfungen bestehen, wird das zu erreichende Ziel im Vorfeld definiert. Konkrete Fragestellungen und Szenarien sind hierbei sehr hilfreich. Am Beispiel der fiktiven Bank wäre eine konkrete Fragestellung, ob ein Angreifer, der in das Gebäude der Bank gelangt, in der Lage ist, unberechtigt eine Zahlung zu veranlassen oder zu manipulieren. Ein weiteres Ziel könnte darin bestehen, die existierenden Erkennungsmechanismen zu überprüfen. Werden Anomalien im Netzwerk entdeckt? Kann sich Malware unbemerkt ausbreiten? Kann sich ein Angreifer dauerhaft im Netzwerk der Bank einnisten?

Schutz der „Kronjuwelen“

Die Ziele sind je nach Unternehmen und Branche sehr unterschiedlich. Ein weltweit führendes Maschinenbauunternehmen muss andere „Kronjuwelen“ schützen als eine Bank oder Versicherung. Doch Red Team Assessments bieten weitere Vorteile. So kann eine solche Prüfung einen hervorragenden Einblick in die Leistungsfähigkeit und Arbeitsweise eines vorhandenen Blue Teams bieten. Blue Teams stellen den Gegenpart zum Red Team dar (siehe Artikel „Rot gegen Blau“, Seite 12). Sie bestehen aus Mitarbeitern der IT-Sicherheitsabteilung und verteidigen das Unternehmen gegen reale Angriffe oder eben die simulierten Angriffe des Red Teams. Große Unternehmen setzen Blue Teams in ihren Security Operations Centern (SOC) ein (siehe Abbildung).

Im Rahmen eines Red Team Assessments können zum Beispiel folgende Aspekte betrachtet werden: Welche Angriffe werden tatsächlich entdeckt? Welche Aktionen des Angreifers bleiben unbemerkt? Wie reagiert das Blue Team auf Stresssituationen, die bei einem Red Team Assessment immer wieder auftreten? Die Erkenntnisse sind für die Verbesserung

iX-TRACT

- Vor einem sogenannten Red Team Assessment gilt es abzuwägen, ob ein solches Projekt überhaupt das Richtige ist oder ein Penetrationstest eventuell sinnvoller wäre.
- Nach Auswahl der geeigneten Testform für das eigene Unternehmen sind das genaue Ziel des Tests, aber auch die Rahmenbedingungen festzulegen.
- Je nach Situation und Umfang des Assessments können Blue Teams, die firmeninternen „Verteidiger“, auf der Gegenseite mitwirken und so gleich mitgeschult werden.

und Weiterentwicklung der Arbeitsweise und Prozesse eines Blue Team beziehungsweise eines SOC-Teams sehr wertvoll.

Frustration bei den Teams vermeiden

Wenn das Training des Blue Teams im Vordergrund steht, ist es empfehlenswert, einen Mitarbeiter des IT-Sicherheitsunternehmens, der das Red Team Assessment durchführt, für den Zeitraum der Prüfung im Blue Team oder im SOC zu platzieren. In diesem Fall spricht man von einer War-Gaming-Übung. Dadurch ist der Mitarbeiter des Dienstleisters in der Lage, in Echtzeit das Reaktionsverhalten des Blue Teams auf die ihm bekannten Angriffe zu beobachten, um das Blue Team später entsprechend zu beraten. Die Herausforderung des Auftraggebers besteht unter anderem darin, Szenarien festzulegen, die im Alltag relevant sind und für die bekanntermaßen Erkennungstechniken und Prozesse vorliegen.

Andernfalls droht dem Blue Team Frustration, wenn Angriffe nicht erkannt werden, weil zum Beispiel keine Metriken oder Erkennungstechniken dafür vorhanden sind oder weil der simulierte Angriff im „Security Playbook" des SOC nicht definiert wurde. Ziel einer solchen Maßnahme ist es nicht, dem Blue Team Versagen vorzuwerfen, sondern konstruktiv an der Optimierung der Arbeitsweise, der Prozesse und der Erkennungstechniken des Teams mitzuwirken. Eine weitere Herausforderung besteht darin, festzulegen, wie viele Informationen man dem Blue Team bekannt geben soll.

Dazu zählen beispielsweise der Zeitraum, in dem die Angriffe zu erwarten sind, die Art der Angriffe sowie die verwendeten Angriffstools. Wie viele Informationen bereitgestellt werden, hängt unter anderem davon ab, wie erfahren das Blue Team ist oder ob es weniger um ein Training des Blue Teams geht, sondern vielmehr darum, ein möglichst realistisches Angriffsszenario nachzustellen. Um den großtmöglichen Lerneffekt zu erreichen, ist es sinnvoll, nach Abschluss des Projekts im Rahmen eines Workshops mit dem Blue oder SOC-Team die daraus gewonnenen Erkenntnisse vorzustellen und gemeinsam Verbesserungen auszuarbeiten. Dabei sollte man auf die vorhandenen Prozesse und Werkzeuge des Blue Teams eingehen.

Quelle: Telekom

In den SOCs großer Unternehmen helfen Blue Teams bei der Verteidigung gegen Internetangriffe. Hier das SOC der Telekom, dessen Dienste auch von kleinen Unternehmen beansprucht werden.

Neben dem Auftraggeber muss sich auch der Dienstleister vor Beginn eines solchen Projekts einigen Herausforderungen stellen. Während viele Penetrationstests sehr ähnlich verlaufen, sieht das bei Red-Team-Assessment-Projekten ganz anders aus. Jedes dieser Projekte ist sehr unterschiedlich und spezifisch auf den jeweiligen Auftraggeber zugeschnitten. Bei solchen Prüfungen lässt sich kein Standardvorgehen von Projekt zu Projekt übertragen. Daher muss man viel Zeit für die Vorbereitung und das laufende Projektmanagement einplanen.

Die Hauptakteure auf Dienstleisterseite sind die Mitglieder des Red Teams. Ein solches besteht typischerweise aus erfahrenen Penetrationstestern. Jedes Mitglied ist Experte auf seinem Fachgebiet. Dadurch wird gewährleistet, dass im Team Kompetenz zu Webschwachstellen, Netzwerken, Windows- und Linux-/Unix-Betriebssystemen, Social Engineering, Malware, Lateral Movement, Reversing, Exploiting und vielem mehr vorhanden ist (siehe Tabelle „Anforderungen an das Red Team"). In speziellen Fällen stehen dem Red Team weitere Kollegen im Büro des Dienstleisters zur Verfügung, wenn es die Situation erfordert oder Fachwissen zu sehr speziellen Themengebieten benötigt wird.

Schnelles Anpassen ist gefragt

Somit ist sichergestellt, dass das Red Team stets alle vorhandenen Möglichkeiten und Ressourcen nutzen kann, um sein Ziel zu erreichen. Doch die fachlichen Kenntnisse sind nur eine von vielen Anforderung an die Red-Team-Mitglieder. Sie müssen zudem in der Lage sein, flexibel auf Änderungen – die sich immer wieder im Rahmen solcher Projekte ergeben – zu reagieren und gegebenenfalls ihr Vorgehen anzupassen. Erfolgreiche Red Team Assessments sind nie Ergebnis der Leistung eines Einzelkämpfers. Vielmehr ist eine enge Zusammenarbeit im Team Voraussetzung für den Erfolg.

Wie in jedem Team ist es sinnvoll, einen Leiter für das Red Team zu benennen. Eine seiner Hauptaufgaben besteht darin, das Projektziel im Auge zu behalten und die Red-Team-Mitglieder entsprechend ihren Fähigkeiten einzusetzen. So lässt sich sicherstellen, dass die Mitglieder des Teams nicht die Orientierung verlieren, wenn die Anzahl an entdeckten Schwachstellen sehr hoch ist und der Weg zum Ziel nicht immer klar definiert werden kann. Der Leiter des Teams muss gegebenenfalls

entscheiden, ob das ursprünglich geplante Vorgehen weiterhin Erfolg versprechend ist oder ob eine andere Herangehensweise zum Erreichen des vorgegebenen Ziels lohnender ist. Hierzu sollte eine kontinuierliche Abstimmung mit dem restlichen Team stattfinden.

Vor dem eigentlichen Red Team Assessment ist eine klare Definition der Ziele und des Rahmens notwendig, in dem die Prüfung stattfinden soll. Die Ziele definiert nicht der Dienstleister, sondern der Auftraggeber. Allerdings kann und sollte der Dienstleister seine Erfahrung einbringen und Vorschläge bezüglich sinnvoller Ziele, Szenarien und Vorgehensweisen unterbreiten. Typischerweise beginnt ein solches Projekt daher mit einem Workshop, in dem die grundsätzlichen Rahmenbedienungen für das Red Team Assessment besprochen und die Ziele definiert werden.

Zudem werden ein oder mehrere Ansprechpartner auf Auftraggeberseite benannt, die eingeweiht sind und im Ernstfall eingreifen können sowie für etwaige Rückfragen zur Verfügung stehen. In diesem Kreis wird die in einem früheren Red-Teaming-Artikel genannte „Du kommst aus dem Gefängnis frei"-Karte für den Dienstleister vorbereitet und ausgestellt. Gerade bei Prüfungen für Unternehmen im Bereich kritische Infrastrukturen ist es wichtig, eine solche schriftliche Vereinbarung bei sich zu führen, um die Situation bei Entdeckung mit den Mitarbeitern für den Objektschutz schnell klären zu können.

Der Vorbereitungsworkshop: Rahmen festlegen

Des Weiteren sollte der Auftraggeber der Prüfung im Workshop Bereiche benennen, die vom Assessment ausdrücklich auszuschließen sind: etwa Örtlichkeiten, die nicht betreten werden dürfen, Personen, die im Rahmen von Social Engineering nicht angegriffen werden dürfen, oder bestimmte Tochterunternehmen und Systeme, die unbedingt auszuschließen sind. Darüber hinaus kann während des Workshops festgelegt werden, welches Vorgehen und welche Angriffstechniken nicht infrage kommen. Hierbei gilt es, zusammen mit dem Auftraggeber mit viel Fingerspitzengefühl einen Rahmen zu definieren, der das Ergebnis der Prüfung nicht verwässert – was durch zu viele Einschränkungen der Fall sein könnte.

Solche Workshops erstrecken sich typischerweise über ein bis zwei Tage und werden oftmals in mehreren Terminen durchgeführt, da manche Aspekte erst nach interner Rücksprache auf Seite des Auftraggebers abschließend festgelegt werden können. Am Ende des Workshops hat der Dienstleister in Abstimmung mit dem Auftraggeber einen „Schlachtplan" entworfen, der grob die Szenarien und Angriffspfade benennt.

Ein wichtiger Aspekt, der zu diesem Zeitpunkt berücksichtigt werden sollte, ist der zeitliche Ablauf der Prüfung. Natürlich hat der Auftraggeber ein Interesse daran, das Projekt möglichst schnell abschließen zu können. Allerdings spielt der Zeitraum, über den sich eine solche Prüfung erstreckt, eine wichtige Rolle. In der Vergangenheit hat es sich bewährt, das Assessment über mehrere Monate zu verteilen. Innerhalb dieses vorab abgestimmten Zeitraums werden immer wieder Angriffe vorbereitet und durchgeführt. Der große Zeitraum ist notwendig, da bestimmte Angriffe eine längere Vorlaufzeit benötigen.

Anforderungen an das Red Team	
Hohe Expertise	**Soft Skills**
Webschwachstellen	Teamfähigkeit
Angriffe auf Netzwerkebene	Kommunikationsfähigkeit
Informationsgewinnung	analytische Fähigkeiten
Spear-Phishing	Problemlösungskompetenz
Social Engineering	Flexibilität
Angriffe auf die physische Sicherheit	
Angriffe mit dem Ziel der Rechteerweiterung	
Lateral Movement in komplexen Umgebungen	
Exfiltration der gewonnenen Daten	
Anpassen und Entwickeln von Malware und Backdoors	
Reverse Engineering von Applikationen	

Beispielsweise kann es sein, dass eine Phishingkampagne mittels E-Mails erst nach mehreren Wochen erfolgreich ist oder unter Umständen auch mehrere Anläufe erfordert. Zudem ist es von Vorteil, die dafür verwendeten Internetdomänen mehrere Wochen bis Monate im Voraus zu beantragen, da manche Sicherheitsprodukte auf Eigenschaften wie das Alter einer Internetdomäne prüfen. Darüber hinaus ergeben sich im Laufe eines Jahres immer wieder gute Gelegenheiten für einen Angriff, zum Beispiel bei öffentlichen Ausstellungen an den Standorten des Auftraggebers, die einen besonders einfachen Zugang zu dessen Gebäude ermöglichen. Je länger der Zeitraum bemessen wird, umso höher ist die Chance, dass auch solche Veranstaltungen berücksichtigt werden können.

Nach dem Workshop ist vor dem Assessment

In der Phase nach dem Workshop beginnt die eigentliche Arbeit für das Red Team. Durch gemeinsames Brainstorming arbeitet das Team Ideen und Vorschläge aus, um die mit dem Auftraggeber definierten Ziele und Angriffsszenarien umzusetzen. Hierbei kristallisiert sich oftmals heraus, welche speziellen Fertigkeiten das Red Team benötigt und welche Werkzeuge, Methoden und Verfahren zum Einsatz kommen sollen. Je nach Auftraggeber und Projekt kann der Fokus eher auf der technischen Seite liegen, auf der physischen Sicherheit oder eben sehr stark auf Social Engineering.

Während des Assessments steht das Red Team immer wieder vor ähnlichen Herausforderungen. Oft stellt sich heraus, dass der ausgearbeitete „Schlachtplan“ nicht eingehalten werden kann. Auf technischer Seite kann es viele Gründe dafür geben. Zum Beispiel trifft das Red Team auf robuste Sicherheitsmaßnahmen, die vorher nicht bekannt waren und aufwendig umgangen werden müssen. Oder die Malware, die vor zwei Monaten bei einem anderen Projekt zum Einsatz kam, wird inzwischen von vielen AV-Lösungen erkannt. Das Red Team muss auf diese Änderungen entsprechend reagieren und gegebenenfalls die Methoden und Werkzeuge anpassen oder ersetzen. Im Fall der erkannten Malware kann es notwendig sein, dass das Red Team diese so anpasst, dass das eingesetzte AV-Produkt sie anhand von Signaturen oder Verhaltensanalyse nicht mehr erkennt.

Es kann jedoch auch erforderlich sein, eigene Tools zu programmieren oder sogar spezielle Hacking-Hardware zu entwickeln, um ans Ziel zu gelangen. Zwar gibt es eine Fülle von Angriffswerkzeugen und Hardware für Pentester, allerdings müssen diese teilweise modifiziert werden, um sie im Rahmen eines Red Team Assessments zielgerichtet einsetzen zu können. Dies trifft insbesondere dann zu, wenn die Aktionen des Red Teams so lange wie möglich unentdeckt bleiben sollen.

Des Weiteren kann es sein, dass der geplante Angriffspfad zum Erreichen des Ziels nicht optimal ist. Beispielsweise könnte das Red Team versuchen, mittels Lateral Movement schnell seine Rechte in der Umgebung zu erweitern und so in wenigen Schritten das Zielsystem zu kompromittieren. Dabei könnte sich dann herausstellen, dass das eigentliche Ziel so gar nicht erreicht werden kann, weil andere Schutzmaßnahmen wirken oder sich das Zielsystem isoliert in einem eigenen Segment befindet, zu dem es keine direkte Verbindung gibt. In solchen Fällen ist die langjährige Erfahrung und Kreativität des gesamten Red Teams gefordert, um die Herangehensweise anzupassen und andere Wege und Möglichkeiten zu wählen. Je erfahrener das Red Team ist und je öfter ähnliche Hürden in der Vergangenheit umgangen werden mussten, desto wahrscheinlicher ist es, dass das Team das vorgegebene Ziel erreicht.

Fazit

Neben den technischen Herausforderungen, die im Rahmen eines Red Team Assessments auftreten, ist auch eine Reihe an organisatorischen Aspekten zu berücksichtigen. Beginnend mit der Frage, warum und ob tatsächlich ein Red Team Assessment beauftragt werden soll, bis hin zur Definition von Zielen und Angriffsszenarien eines solches Projekts. Nicht unerheblich sind im Zusammenhang mit vertraulichen Daten und Mitarbeiterrechten auch Compliance- und Datenschutzaspekte, die es ebenfalls im Vorfeld einzuplanen gilt (siehe dazu Artikel „Rahmenwerk“, Seite 80).

Unternehmen mit einem sehr hohen Schutzbedarf, die bereits die grundlegenden Aufgaben im Bereich IT-Sicherheit erledigt haben, profitieren enorm von einem Red Team Assessment. Es vermittelt ein sehr gutes Bild über die Sicherheitslage – insbesondere wenn möglichst realistische Szenarien gewählt werden, bei denen ein potenzieller Angreifer einen erheblichen Schaden herbeiführen könnte. Dadurch ist es möglich, das eigene Unternehmen, die eigenen Mitarbeiter und die Sicherheitsarchitektur aus dem Blickwinkel eines versierten Angreifers zu betrachten und geeignete Maßnahmen zum Beheben der aufgedeckten Schwachstellen zu ergreifen. Die Möglichkeit, das Blue Team dabei zu schulen und seine Arbeitsweise und Prozesse zu optimieren, schlägt als weiterer Vorteil für diese Art von Prüfungen zu Buche.

Wer tiefer in die Praxis des Red Teaming einsteigen möchte, findet in den zwischen Februar 2019 und April 2019 in loser Folge erschienenen *iX*-Artikeln zu „Red Team Assessments“ eine umfangreiche Übersicht über Methoden, Techniken und Werkzeuge der einzelnen Projektphasen.

(ur@ix.de)

Joshua Tiago

ist Leitender Berater bei der cirosec GmbH und verantwortet Red-Team-Assessment-Projekte für große Kunden.

Mehr-Faktor-Authentifizierung im Unternehmen

Mit privacyIDEA zu einem flexiblen MFA-Konzept

Plugins

Anbindung unzähliger zusätzlicher Applikationen über RADIUS, SAML, openID Connect, REST u.a.

Migration

Altes MFA-System im Einsatz? Mit privacyIDEA ist ein sanfter Umstieg möglich oder auch ein zeitlich unbegrenzter Parallelbetrieb.

Setup

Hochverfügbare Mehr-Faktor-Umgebungen on-premises durch redundanten Aufbau realisieren.

Integration

privacyIDEA liest existierende Benutzer aus Benutzerquellen wie Microsoft Active Directory, OpenLDAP oder SQL. Null-invasive Integration in bestehende Organisationen.

Prozesse

Flexibler Token-Rollout, einfaches Onboarding neuer Mitarbeiter, hohe Individualisierbarkeit durch Policies und Event Handler.

NetKnights
securing your identity

NetKnights GmbH, Ludwig-Erhard-Str. 12,
D-34131 Kassel, +49 561 3166 797,
info@netknights.it, www.netknights.it

Blue Teaming: Wie man die Verteidigung gegen Internetangriffe übt

Rot gegen Blau

Frank Neugebauer

Nicht nur das Angreifen von IT-Systemen und Unternehmensnetzwerken will gelernt sein, sondern auch das Abwehren solcher Angriffe. In Übungen spielen sogenannte Blue Teams verschiedene Szenarien durch.

iX-TRACT

- Neben Assessments durch Red Teams, die zumindest in größeren Unternehmen gang und gäbe sind, um die IT-Sicherheit zu testen, gibt es auf verschiedenen Ebenen Übungen für deren Gegenpart, Blue Teams, deren Aufgabe das Abwehren von Angriffen ist.
- Bei den Locked Shields, der weltweit größten Blue-Teams-Übung, treffen sich jährlich IT-Sicherheitsexperten aller Couleur, um gegeneinander anzutreten. Sinn und Zweck der Übung ist nicht das Gewinnen, sondern das Vorbereitetsein auf den Ernstfall.
- Bewährt hat sich insbesondere die Zusammenarbeit von Spezialisten der Regierungsbehörden und privatwirtschaftlichen IT-Sicherheitsexperten.

Vielen IT-Sicherheitsspezialisten wird noch unbekannt sein, dass die estnische Hauptstadt Tallinn nicht nur das wirtschaftliche und kulturelle Zentrum des Landes ist, sondern auch einen wesentlichen Beitrag zur Verteidigung im Cyberraum leistet. Die militärischen Führer haben hier das NATO Cooperative Cyber Defence Centre of Excellence (kurz CCDCOE) eingerichtet.

Gemeinsam mit Industrie und Forschung findet hier seit 2010 die mittlerweile weltweit größte Cyberverteidigungsübung statt. Bei den „Locked Shields“ handelt es sich aber nicht um eine der üblichen Kommandostabsübungen, bei denen vorrangig einzelne Befehlsketten trainiert und die Maßnahmen ausschließlich in der Theorie durchgespielt werden. Stattdessen haben das CCDCOE und seine Partner hier über 4000 virtuelle Systeme eingerichtet, auf denen in mehr als 2500 Angriffen ein realer Cyberüberfall auf ein NATO-Mitgliedsland simuliert wird. Es treten rote gegen blaue Teams an, die eine hochkomplexe Infrastruktur angreifen beziehungsweise verteidigen müssen.

Auch wenn die Bilder einer großen LAN-Party ähneln, so haben die Veranstalter im Laufe der Jahre ein sehr hohes Niveau erreicht, das auch auf internationaler Ebene bisher einzigartig ist. Hier müssen die Teilnehmer in Echtzeit und auf realen Systemen beweisen, ob sie den vielschichtigen Cyberangriffen standhalten können und in der Lage sind, erfolgreich Gegenmaßnahmen einzuleiten. Angesichts der realen Cyberbedrohung bieten die „Locked Shields“ den internationalen Teams die Möglichkeit, ihre Infrastruktur (zum Beispiel Stromnetze, Wasserversorgung und öffentliche Einrichtungen) realen Angriffen auszusetzen und entsprechende Konsequenzen abzuschätzen.

Verantwortliche und Teilnehmer

Die im April 2019 durchgeführte Übung „Locked Shields“ wurde in Kooperation mit den estnischen, finnischen und amerikanischen Streitkräften organisiert. Weitere Unterstützung erhielten sie vom National Security Research Institute der Republik Korea und der Technischen Universität in Tallinn. Darüber hinaus beteiligten sich verschiedene Industriepartner wie die Siemens AG, Ericsson, Cisco und viele weitere Helfer aus der ganzen Welt.

Diesmal traten 24 Blue Teams an, die vorrangig von ihren nationalen Standorten aus agierten. Die deutschen Teilnehmer waren von der Luftwaffenkaserne

Köln/Wahn und aus dem Standort Euskirchen mit dem Übungsnetz verbunden (Abbildung 1). Unterstützung erhielten die vorrangig militärischen Übungsteilnehmer aus dem Organisationsbereich Cyber- und Informationsraum (CIR) und der Luftwaffe von zivilen Mitarbeiten des BSI, der BWI GmbH, des Fraunhofer FKIE Bonn und den Firmen Siemens und Symantec.

Sie hatten die Aufgabe, als schnelle Reaktionskräfte einen fiktiven NATO-Staat bei der Abwehr von Cyberangriffen und deren vielfältigen Auswirkungen zu unterstützen (siehe Kasten „Das Szenario der Abwehrübung“). Besonders großer Wert wurde dabei auf die Einsatzbereitschaft der Systeme unter Angriffsbedingungen gelegt. Selbstverständlich war nicht allein der technische Sachverstand gefragt, die Teilnehmer mussten auch strategische Entscheidungen treffen und rechtliche Fragen klären. Um der komplizierten Lage im Einsatzland Herr zu werden, spielte der Umgang mit den Medien und der Bevölkerung eine wichtige Rolle. Dazu betrieb jedes Blue Team eigene Webseiten und beugte durch aktive Informationspolitik Falschmeldungen vor.

Während einer sogenannten Forensik-Challenge wurden die teilnehmenden Blue Teams aufgefordert, ihre Fähigkeiten auf diesem Gebiet unter Beweis zu stellen. Dazu erhielten sie spezielle Beweismittel, die sie auf Spuren der Angreifer auswerteten. Dabei fanden sie heraus, wie die Täter Zugriff auf die IT-Infrastruktur erlangt und wie sie es geschafft hatten, sich auf den Systemen festzusetzen. Besonders wichtig war es auch herauszufinden, welche Daten möglicherweise in unbefugte Hände gelangt waren.

Quelle: Martina Pump / Bundeswehr

Ein Teil des deutschen Blue Teams, das aus einer Luftwaffenkaserne in Köln/Wahn operierte. Die Teilnehmer hatten sich nach ihren Fähigkeiten in Subteams aufgeteilt. Von unten nach oben: Reporting, Radarsysteme, Linux/Webapplikationen, Router und Firewall (Abb. 1).

Scoring: Wie bewertet wurde

Damit am Schluss ein Sieger gekürt werden konnte, hatte das CCDCOE ein ausgeklügeltes Scoringsystem an den Start gebracht, das jeden Fehler bestrafte, gute Leistungen aber auch mit zusätzlichen Punkten bedachte. Als besondere Herausforderung stellte sich heraus, die betriebenen Systeme trotz ständiger Angriffe einsatzbereit zu halten. Jeder erfolgreiche Angriff der Roten führte zu einem empfindlichen Punktverlust. In solchen Situationen mussten die Blue Teams schnell handeln, um nicht weitere Zähler für die Verfügbarkeit der Systeme zu verlieren (Abbildung 2).

In der Hektik des Gefechtes durften die Blue Teams aber auch nicht das Meldewesen aus dem Auge verlieren. Für rechtzeitige und detaillierte Berichte bekamen die Teams Punkte gutgeschrieben. Die Nutzer (gelbes Team, siehe Kasten „Die beteiligten Teams“) standen über ein Ticketsystem mit dem jeweiligen Blue Team in Verbindung. Hier meldeten sie Probleme oder Ausfälle an der genutzten IT-Infrastruktur. Die Blauen waren gut beraten, diesen Hinweisen zeitgerecht nachzugehen, um nicht wertvolle Punkte einzubüßen (Abbildung 3).

Die Veranstalter legten besonderen Wert auf einen regen Informationsaustausch der

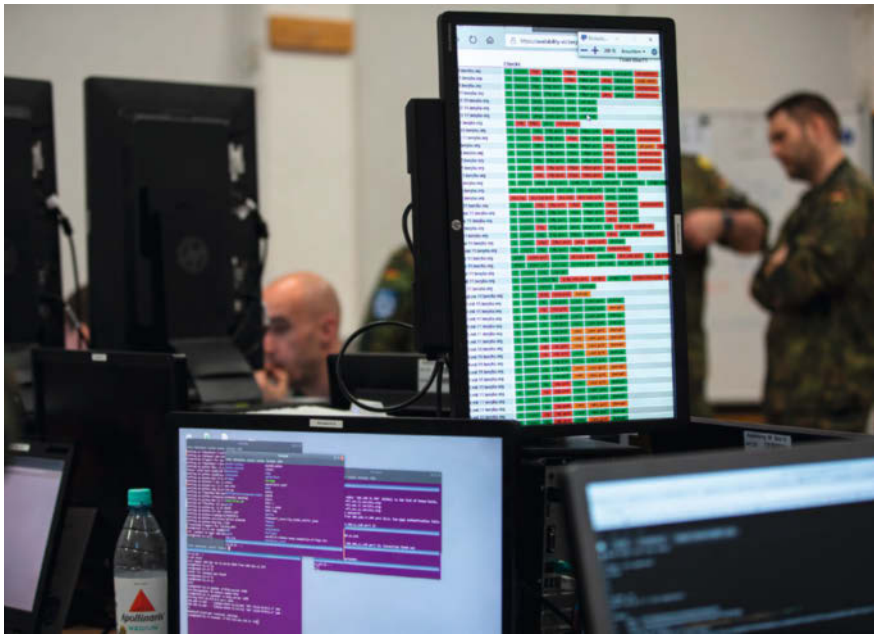
Das Szenario der Abwehrübung

Das NATO-Mitglied Berylia ist seit längerer Zeit Anfeindungen seines Nachbarlandes Crimsonia ausgesetzt, die nach und nach die Infrastruktur des Landes bedrohen. In kurzer Zeit hat sich eine Organisation innerhalb Berylias gebildet, die die Souveränität des Staates untergräbt und einen Regierungswechsel anstrebt. Das Ziel der ethnischen Minderheit des Landes ist eindeutig: Sie haben, unterstützt von Crimsonia, eine Informationskampagne ins Leben gerufen, die Angst und Hass gegenüber Einwanderern schürt und das öffentliche Leben destabilisieren soll.

Heftige Regenstürme setzten große Teile Berylias unter Wasser und beschädigen wichtige Infrastruktur des Landes. Die politische Gegenseite nutzt das Durcheinander, um weitere Proteste gegen die Regierung zu organisieren und das soziale Leben innerhalb der Bevölkerung zu destabilisieren.

Die Regierung Berylias nimmt die Hilfe der internationalen Staatengemeinschaft an und beauftragt ein NATO „Rapid Reaction Team“, die wichtigen Informations- und Kommunikationssysteme wiederherzustellen und die Wasseraufbereitung des Landes wieder in Betrieb zu nehmen.

Das entsandte NATO-Team stellt bereits nach kurzer Zeit fest, dass wichtige Teile der IT-Infrastruktur schon längst vom Gegner infiltriert sind. Sie einfach abzuschalten ist aber keine geeignete Option. Vielmehr müssen die Verantwortlichen weitere Angriffe des Gegners abwehren, ohne dabei die Funktionsfähigkeit der Systeme zu beeinträchtigen.



Quelle: Martina Pump / Bundeswehr

Besonders wichtig war es, den mit Nagios ermittelten Status der einzelnen IT-Systeme im Blick zu haben. Bei den in der Übersicht rot angezeigten Zuständen galt es, schnell zu handeln, um den empfindlichen Punktabzügen zu entgehen (Abb. 2).

internationalen Blue Teams untereinander. Hier sollten die Vorgehensweise der erkannten Angriffe, angewandte Techniken und die von den „Kriminellen" genutzten IP-Adressbereiche ausgetauscht werden. Für diese Hinweise gab es Extrapunkte.

Besondere Herausforderungen

Die Angreifer waren je nach Fähigkeit in verschiedenen Gruppen organisiert und agierten von Tallinn aus. Spezielle Windows-Teams führten vorrangig Client-Side-Angriffe aus, die auf die Verfügbarkeit der PCs, Server und der angeschlossenen Domäne zielten. Dabei erhielten sie unfreiwillig Schützenhilfe vom gelben Team an den einzelnen IT-Systemen, denn diese „Nutzer" wurden Opfer einer ausgeklügelten Phishingkampagne und von E-Mails mit Schadcode im Anhang.

Die Blauen sahen sich schon zu Beginn der Übung infizierten Systemen ausgesetzt, die aufgrund der bereits ausgebrachten Schadsoftware schwierig zu verteidigen waren. In diesem Zusammenhang war es wichtig, die mittels der Software Cobalt Strike (siehe Kasten „Das Angriffs-Framework Cobalt Strike") agierenden Angreifer zu erkennen und ihre Absichten zu vereiteln. Dabei war es nicht immer leicht, den Schadcode mithilfe der eingesetzten Virenschutzsoftware auszumachen.

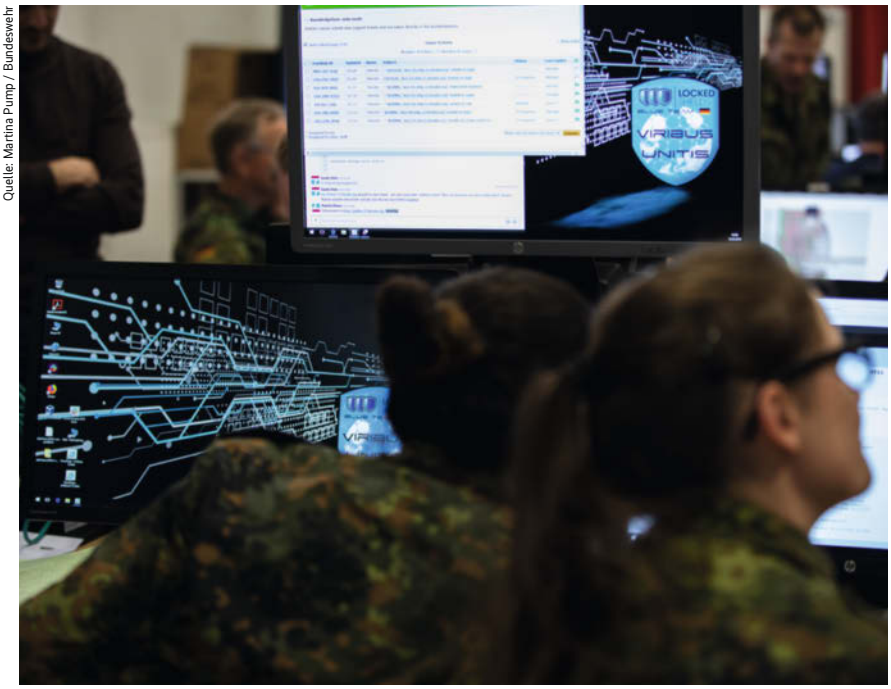
Im Verlauf der Übung gelang es den Angreifern, das Passwort eines Administrators in der Domäne zu ändern und für ihre Zwecke einzusetzen. Außerdem wurden bekannte und unbekannte Exploits eingesetzt. Während der gesamten Übung war es den Angreifern über die Strike Beacons (siehe Kasten zu Cobalt Strike) möglich, Zugriff auf die Windows-Systeme zu erlangen und weitere Schadsoftware nachzuladen. Die kompromittierten Windows-Systeme wurden in der Endphase der Übung eingesetzt, um die Wasseraufbereitung und die Stromversorgung des fiktiven Einsatzlandes anzugreifen.

Alle Webapplikationen und Linux-Systeme waren mit Schwachstellen versehen, die mehr oder weniger schwer zu erkennen waren. Besonders schwierig für das Blue Team war es, die Webseiten zu verteidigen. Eine weitere Herausforderung stellte der Einsatz mehrerer Docker-Container dar, die zu einem Schwarm zusammengefasst waren. Darüber hinaus musste das Team mehrere Programmiersprachen (etwa PHP, Python und Java) beherrschen, um eingebetteten Schadcode zu erkennen.

Im Verlauf der Übung startete das Red Team automatisierte Angriffe, die zum gleichzeitigen Defacement mehrerer Webseiten führten. Dabei erzielte eine ausgelagerte Web Application Firewall (WAF) des Blue Teams nicht den beabsichtigten Schutzeffekt.

Ein Vorsprung für Rot

Ziel des für die Firewall und den Router eingesetzten Red Teams war es, die Kommunikation so weit aufrechtzuerhalten, dass die anderen Angreifer ihre Aufgabe erfüllen konnten. Dazu hatte es 24 verschiedene Möglichkeiten implementiert, Zugriff auf die Systeme zu erlangen und zu erhalten. Man konnte also davon ausgehen, dass schon in der Anfangsphase das Red Team Zugriff auf die meisten Systeme



Quelle: Martina Pump / Bundeswehr

Das gelbe Team meldete die Ausfälle an den genutzten IT-Geräten, die dann in einem Ticketsystem erfasst wurden. Wer die Nutzer zu lange warten ließ oder die gemeldeten Probleme zu spät in den Griff bekam, riskierte hohe Punktverluste (Abb. 3).

hatte. Die Herausforderung auf der blauen Seite bestand darin, diese Einfallstore zu finden und den Zugriff zumindest einzuschränken.

Ein spezielles Cisco-Team wurde seitens der Roten eingesetzt, um die Router anzugreifen. Dabei ging es vor allem darum, Passwörter und Nutzernamen zu kompromittieren und die Konfiguration der einzelnen Systeme herauszufinden. Einen ähnlichen Ansatz verfolgte ein spezielles Ericsson-Team, das Angriffe auf die Mobilfunksysteme ausführte.

Die zweitägige aktive Übungsphase stellte sich als Härtetest für alle Übungsteilnehmer heraus, der der Kreativität der Angreifer wie der Verteidiger alles abverlangte. So ging im Minutentakt die Kontrolle einzelner Systeme verloren oder wurde wiedergewonnen. Dabei mussten die Blauen ständig Kompromisse eingehen, um beispielsweise die Nutzbarkeit der einzelnen Systeme nicht durch zu starke Härtungsmaßnahmen einzuschränken. Am Ende blieb aber nichts anderes übrig, als einzelne Teilbereiche aufzugeben, um die wirklich wichtigen Komponenten im komplexen Netzwerk abzusichern.

Ziel der Veranstalter war es, durch ständig erhöhte Angriffsintensität Stresssituationen zu erzeugen. Diese sollten strategische Entscheidungen erzwingen oder auch Fehlentscheidungen provozieren.

Am Ende gelang es dem deutschen Blue Team, die Schlüsselpositionen zu halten und mithilfe des ungarischen Teams die Strom- und Wasserversorgung zu sichern. Unter diesen extremen Bedingungen konnte ein sehr guter achter Platz erreicht werden. Das deutsche Forensik-Team leistete zu diesem Erfolg einen besonderen Beitrag, indem es zum vierten Mal in Folge in dieser Wertung den ersten Platz belegte.

Letztendlich errang das französische Blue Team den ersten Platz, dicht gefolgt von der Tschechischen Republik und Schweden.

Die beteiligten Teams

Blau: Die Verteidiger

30- bis 50-köpfige Teams, die von ihren Standorten aus agieren und per VPN mit dem Übungsnetz verbunden sind.

Rot: Die Angreifer

IT-Sicherheitsexperten, die auf Angriffe auf Computernetzwerke spezialisiert sind. Sie treten in kleineren Gruppen auf und konzentrieren sich auf die Bereiche Clients, Server, Webapplikationen oder Firewall und Router. Sie agieren von Tallinn aus.

Gelb: Die Nutzer

Sie bedienen die Informationstechnik im Einsatzland. Sie simulieren die Beschäftigten in Firmen und Kraftwerken und führen bestimmte Aktionen aus, die in Drehbüchern festgelegt sind – das bedeutet, sie handeln, wie es normale Nutzer auch tun würden. Hier waren vorrangig Studenten der Technischen Universität Tallinn eingesetzt.

Weiß: Die Schiedsrichter

Das Team wertet das automatisierte Punktesystem aus und greift bei strittigen Situationen korrigierend ein. Hier sind auch die simulierten Pressevertreter angesiedelt, die Informationen mit den Blue Teams austauschen dessen Reaktionen bewerten.

Grün: Die Techniker

Sie sind für das Übungsnetzwerk und alle virtuellen Systeme verantwortlich. Dies umfasst auch die VPN-Verbindung zu den Standorten der verschiedenen Blue Teams.

Fazit

Bei den Locked Shields handelt es sich um die weltweit größte Live Fire Cyber Defence Exercise, die im Vergleich zu den Vorjahren noch einmal einen höheren fachlichen Anspruch hatte. Der eigentliche Sinn der Übung besteht sicherlich nicht im Sammeln von Punkten. Sie trainiert aber alle Beteiligten auf einem sehr hohen technischen Niveau auf realen Systemen. Dabei umfasst die Übung alle Facetten einer möglichen Auseinandersetzung im Cyberraum.

Im Vergleich insgesamt lagen die Nationen im vorderen Bereich, die diese Übung als Schwerpunkt ihrer Tätigkeit sehen und über das gesamte Jahr trainieren. In diesem Zusammenhang ist es besonders wichtig, sowohl eine gute Mischung von Systemadministratoren und IT-Sicherheitsfachleuten als auch von jüngerem und erfahrenem Personal zu erreichen. Daher arbeiten einige Blue Teams mit externen Organisationen und Firmen zusammen, die bereits über notwendige Fähigkeiten verfügen.

Insgesamt hat sich gezeigt, dass militärische Organisationen, zivile Behörden und Institutionen zusammenarbeiten können, um bei möglichen Auseinandersetzungen im Cyberraum erfolgreich zu agieren. (ur@ix.de)

Quellen

Hintergrundinformationen zu den Organisatoren und Teilnehmern der Locked Shields, Fotos der Veranstaltung sowie das Handbuch zu Cobalt Strike Beacon sind über ix.de/z5kq zu finden.

Das Angriffs-Framework Cobalt Strike

Cobalt Strike ist ein von Raphael Mudge geschriebenes kommerzielles Framework, das vorrangig von Penetrationstestern und Red Teams eingesetzt wird. Es verfügt über Werkzeuge, die helfen Informationen zu beschaffen, Schwachstellen zu finden, in IT-Systeme einzudringen und sich im Netzwerk festzusetzen. Dabei werden Techniken angewendet, die auch reale Gegner einsetzen, wenn sie keine oder nur geringe Informationen über ein Zielsystem haben.

Mit dieser Java-Applikation lassen sich Phishingangriffe ausführen und Software on the fly mit Malware infizieren. Die Angreifer stehen dabei untereinander in Verbindung und sind in der Lage, relevante Informationen auszutauschen.

Ein sogenannter Beacon ist eine Payload in Cobalt Strike, die die Kommunikation mit einem kompromittierten Host über einen langen Zeitraum gewährleistet. Dabei ist es irrelevant, ob die Payload über einen Clientangriff gesendet oder in eine bereits bestehende Session injiziert wurde. Einmal im Zielsystem integriert, kann sie zeitgesteuerte Aufgaben ausführen oder Informationen weitergeben.

Dipl.-Ing. (FH) Frank Neugebauer

hat als Offizier der Bundeswehr über 25 Jahre auf dem Gebiet der IT-Sicherheit gearbeitet. Seit 2017 ist er im Ruhestand und noch immer als Berater und externer Mitarbeiter tätig. Er ist außerdem Autor des Buches „Penetration Testing mit Metasploit".