Felix 'FX' Lindner

Licht aus!

Sicherheit kritischer Infrastruktur im Test

Dass Nationalstaaten auch in der digitalen Welt aufrüsten, ist spätestens seit der Entdeckung der Stuxnet-Schadsoftware allgemein bekannt. Doch wie würde sich so ein Angriff auf unser tägliches Leben auswirken und wie würde er genau vonstattengehen? Im Rahmen des Projekts „netwars“ hat Felix Lindner mit einem Team seiner Recurity Labs einen simulierten Angriff durchgeführt.

Die bis zum heutigen Tag bekannt gewordenen Operationen nationalstaatlicher oder von Staaten unterstützter Angreifer hatten meist spezifische Ziele. Zum Beispiel sollten die Operationen der USA namens „Olympic Games“ die Forschungen des iranischen Atomprogramms sabotieren, sodass der Iran am Erreichen seines vermuteten Zieles einer eigenen Atombombe gehindert wird. Andere bekannte oder zumindest vermutete Angriffe hatten militärische Aufgaben.

Ein beträchtlicher Teil der Operationen richtet sich lediglich gegen Informations- und Repräsentationsseiten im Internet, ob nun zur Streuung falscher Nachrichtenmeldungen oder um die Webseite einer Regierungsorganisation eines anderen Landes zu verunstalten. Aber auch die industrielle Produktion wurde schon Opfer digitaler Angriffe, deren Initiierung durch staatliche Akteure zumindest nicht ausgeschlossen ist.

Die digitale Zerstörung von rund 55 000 Computern des saudi-arabischen Ölproduzenten Aramco ist ein Beispiel für solche Ereignisse. Dieser Angriff mit einer primitiven und offensichtlich auch nicht wunschgemäß funktionierenden Schadsoftware zeigt deutlich, dass es weder eines ausgefeilten Produktes wie Stuxnet bedarf noch des Erreichens von Zugängen zu den großtechnischen Einrichtungen, um einen erheblichen Schaden für Produktion und Unternehmen zu verursachen.

Obwohl sich also solche digitalen Angriffe in unserer heutigen Welt noch in Grenzen halten, sind die Möglichkeiten durchaus vorhanden und können auch von weniger hoch entwickelten Akteuren genutzt werden. Man

© Copyright by Heise Zeitschriften Verlag
Persönliches PDF für alle Leser der c't aus 30625 Hannover

kann sich also nicht mehr darauf verlassen, dass Staaten oder andere Interessensgruppen sich auf rein militärische Ziele beschränken, und muss sich mit der Frage auseinandersetzen, wie man mit einem solchen Angriff umgehen würde.

Kritische Infrastruktur

Ein offensichtliches Ziel von digitalen Angriffen ist die kritische Infrastruktur für die Versorgung der Bevölkerung mit Strom, Gas, Wasser, Transport und Kommunikation. Ein solcher Angriff ist auch bei rein militärischer Motivation eine wahrscheinliche Komponente, da die Streitkräfte eines Landes und deren Kasernen von der Versorgung genauso abhängen wie die Wirtschaft oder private Haushalte.

Um einzuschätzen, wie schwierig es wäre, die Kontrolle über einen Teil der Versorgungsinfrastruktur zu erlangen, erklärten sich die Stadtwerke Ettlingen sowie die Vertreter der Stadt zu einem außergewöhnlichen Experiment bereit. Mit einem Penetrationstest sollte überprüft werden, ob und auf welchem Wege ein organisierter Angreifer sich einen Zugang verschaffen kann, der ihm die Kontrolle über die gesamte Versorgung ermöglicht. Dieser Test ging von einem Angreifer-Team aus, wie es nationalstaatliche oder vergleichbare Organisationen zur Verfügung haben.

Der erste Schritt eines organisierten Teams ist die Beschaffung von Basisinformationen über das Zielobjekt. Der einfachste Weg ist hier Erpressung oder Bestechung von Mitarbeitern des Betriebs. Aber auch Trickbetrug und andere Formen von sogenanntem „Social Engineering“ bis hin zu Einbrüchen in die Geschäftsräume kommen zur Anwendung. Benötigt wird vorerst nur eine minimale Informationstiefe für die Planung, ein einziger Übersichtsplan der Netzwerksegmente kann schon vollkommen ausreichen.

In einem Penetrationstest ist dieser Schritt meist nicht angebracht, vor allem nicht, wenn offensichtlich wird, dass er erfolgreich sein würde. Nur wenn ein Unternehmen, eine Behörde, oder – besonders häufig – eine militärische Einrichtung die Sicherheit der IT-Anlagen größtenteils auf der physischen Sicherheit – also etwa bewachten Stacheldrahtzaun der Anlage – gründet, ist es an der Zeit, diese Argumentationskette zu überprüfen. Da auch dies ein spezialisiertes Handwerk ist, bringen sowohl die „bösen“ als auch die „guten“ Jungs in so einem Fall ein weiteres Team mit, das seinerseits den „Über-den-Zaun-Teil“ hauptberuflich praktiziert. Die meisten Hacker sind hierfür eher ungeeignet.

Für den Test wurden die Basisinformationen der Stadtwerke ganz zivilisiert, und nach schriftlicher Vereinbarung zur Geheimhaltung, an das Team übergeben. Außerdem ist es bei Penetrationstests von großer Bedeutung, das weitere Vorgehen abzustimmen und eventuelle Risiken genauestens auszuloten, bevor man eine produktive Umgebung von solcher Bedeutung angreift. Obwohl das professionelle Selbstverständnis natürlich eine erfolgreiche Übernahme der Kontrollmechanismen erwartet, wäre ein Ausfall der städtischen Versorgung nicht etwa ein Erfolg, sondern ein Totalversagen.

Die Stadtwerke Ettlingen ließen sich auf einen simulierten Angriff durch Profis ein.

Angriffswege

Die meisten IT-Infrastrukturen, ob in Industrie, Finanzwelt oder staatlichen Einrichtungen, sind von innen heraus entstanden. Daher ist die Vorstellung einer sogenannten Perimeter-Sicherheit verlockend: Innen sind unsere vertrauenswürdigen Netze, draußen ist die böse Welt. Angreifer beschreiben diese Architektur gerne mit dem Werbe-Slogan von M&M-ähnlichen Süßwaren namens Hershey's Kissables: „Crunchy on the outside, soft and chewy on the inside“.

Das Problem mit der Betrachtungsweise von „innen“ und „außen“ ist, dass ein einziger Weg von außen nach innen ausreicht, um das gesamte Modell zum Einsturz zu bringen. Daher versucht jeder Angreifer zuerst einmal, genau so einen Weg zu finden oder zu schaffen. Das Ziel ist, Netzwerkverkehr über einen Brückenkopf leiten zu können, der als „innen“ betrachtet wird. Dabei ist es egal, welche Rolle das Gerät eigentlich hat. Es muss nicht einmal immer ein PC sein; Drucker sind schließlich auch Computer. Auch ein privilegierter Zugang ist hierfür nicht notwendig. Selbst wenn an dem Gerät grade eine Person arbeitet, ist es unwahrscheinlich, dass die Aktivitäten bemerkt werden, denn es werden nur geringe Datenmengen weitergereicht.

Der technisch einfachste Weg zu einem Brückenkopf ist es, eine Person in der Zielorganisation davon zu überzeugen, ein Programm auszuführen. Was im ersten Moment nach einer sehr unbesonnenen Handlung klingt, ist in Wirklichkeit gar nicht so abwegig. Besonders geeignet hierfür sind Umgebungen, in denen viel branchenspezifische oder speziell entwickelte Software eingesetzt wird, die oft auch nach Jahrzehnten noch manuell mit Updates versorgt werden muss. Der Angreifer muss sich nur per E-Mail als Mitarbeiter des Hersteller- oder Wartungsunternehmens ausgeben und ein „wichtiges Update“ an die E-Mail anhängen, damit sein Schadcode von einem gutgläubigen oder schlicht überlasteten Mitarbeiter gestartet

Eine unscheinbare kleine Box wie dieser „Pwn Plug“ gewährt über GSM/3G/4G transparenten Zugang zum Firmen-Netz. Tools wie Metasploit, SSLstrip, dsniff und mehr sind bereits vorinstalliert.

© Copyright by Heise Zeitschriften Verlag
Persönliches PDF für alle Leser der c't aus 30625 Hannover

wird. Dabei hat der Angreifer den Vorteil, dass erkannte und damit misslungene Täuschungen meist nicht in der Organisation bekannt gemacht werden, sodass er es einfach beim nächsten Opfer mit der gleichen Masche noch mal versuchen kann.

Der zweite übliche Weg verwendet genau die gleichen sogenannten Client-Side-Exploits, die auch bei Drive-by-Downloads von Schadsoftware zum Einsatz kommen. Hier werden bekannte oder nicht bekannte Schwachstellen im Web-Browser, in Java oder Flash ausgenutzt, um beliebigen Code auf dem Rechner des Opfers auszuführen. Weitere beliebte Angriffsziele sind die installierten Programme zur Darstellung von Dokumentformaten wie PDF sowie Audio- und Video-Dateien. Werden diese per Email von einer angeblichen Absender-Adresse innerhalb der Organisation zugestellt, vermutet fast niemand eine böse Absicht hinter dem Dateianhang. In besonders wichtigen Fällen greifen Angreifer auf Methoden mit so klingenden Namen wie „Wasserloch-Infektion“ zurück, bei der zuerst eine von den Opfern besonders häufig frequentierte Webseite gekapert und mit dem Schadcode ausgerüstet wird, wodurch der morgendliche Nachrichtenüberblick schnell die halbe Organisation infiziert.

Der risikoreichste aber auch verlässlichste Weg zu einem Brückenkopf im Netz des Zieles ist, diesen persönlich dort zu platzieren. Fährt man mittags in leuchtend gelbrotem Overall auf einem Motorroller vor und trägt dann fünf oder mehr frische Pizzen (denn leere Kartons duften nicht) vor sich her, kommt man fast überall hinein. Dabei muss die Einrichtung, zu der man sich auf solche Art Zugang verschafft hat, noch nicht einmal zur angegriffenen Organisation gehören. Gelten die Netze der Einrichtung für das Ziel als „innen“, hat der Angreifer erreicht, was er wollte. Einmal im Gebäude, platziert der Angreifer einen Embedded-PC mit WLAN- und 3G-Modul an einer unbenutzten Netzwerkdose mit Ethernet und kann von nun an vom Auto oder Home Office aus weiterarbeiten.

Nahezu keine Organisation kann sich gegen solches Eindringen effektiv wehren, und genau das macht das Konzept eines Perimeters mit „innen“ und „außen“ so gefährlich. Selbst wenn die üblichen Methoden versagen sollten, es finden sich fast immer Fernwartungszugänge, Telefonanlagen, Systeme für Gebäudeautomatisierung, Zugangskontrolle, Brandschutz oder direkte Zugänge zum Dieselgenerator für den Notstrom, die irgendwann mal irgendwer an das „interne“ Netzwerk angeschlossen hat. Selbst einfachste Fernwirksysteme kann ein Angreifer nutzen, denn sie wurden niemals daraufhin untersucht, wie sie auf ein absichtlich bösartiges Gerät am anderen Ende der Leitung reagieren würden.

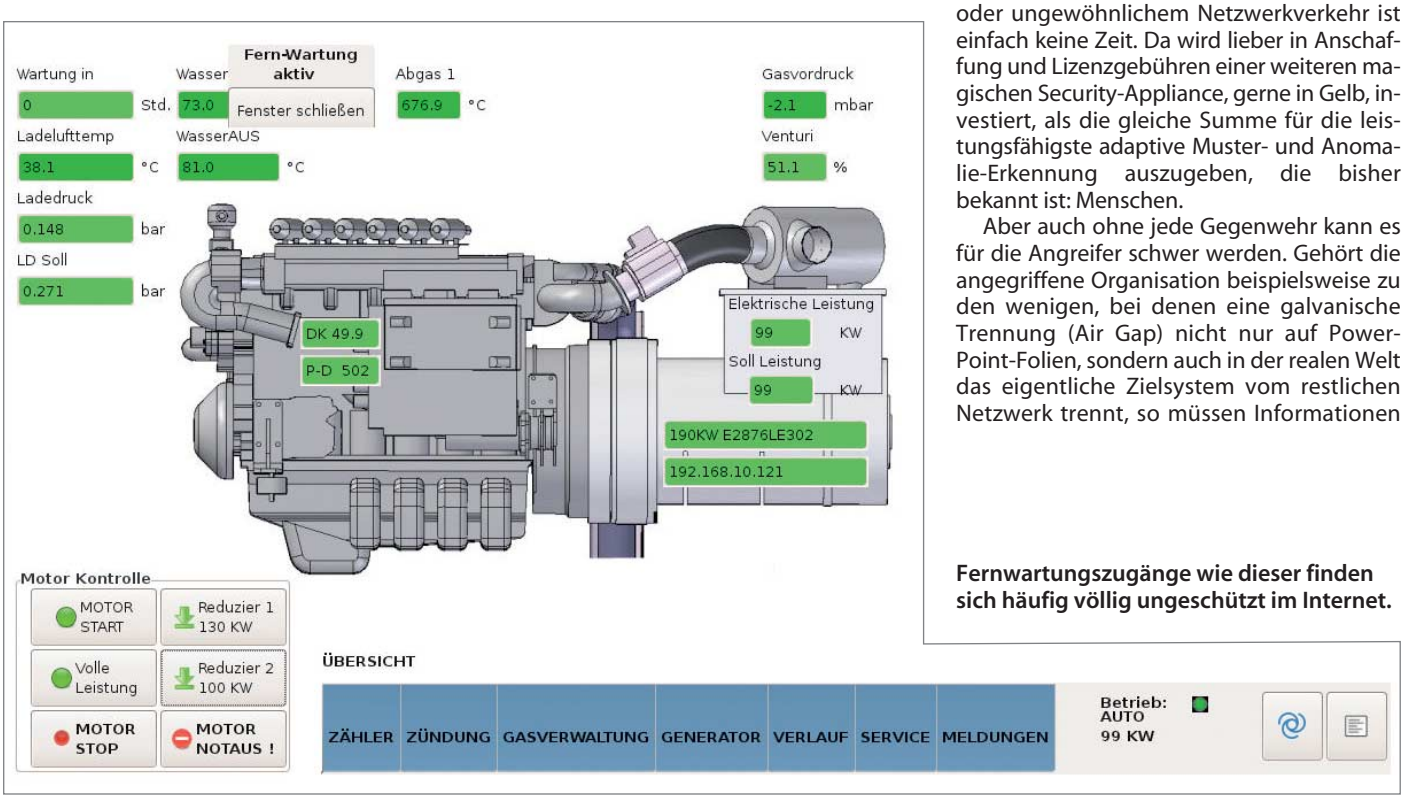
Umsetzung

Mit einem Penetrationstest wird oft die Erwartung verbunden, einen „echten“ Angriff möglichst realistisch abzubilden. Diese naheliegende Vorstellung ist allerdings in den allermeisten Szenarien kontraproduktiv. Effizienter ist es, die einzelnen Schritte eines Angriffs getrennt zu analysieren – eine Option, die böswillige Angreifer nicht haben. So wurden etwa in diesem Fall viele Zugangsmöglichkeiten durchgespielt, damit auch dort die Bedrohungen betrachtet und gegebenenfalls im Nachgang beseitigt werden konnten.

Im Fall der Stadtwerke Ettlingen bot sich für den Einstieg ein Tagungszentrum an, welches nach Informationslage eine Verbindung zum restlichen Unternehmensnetz haben sollte. Nun ist Ettlingen allerdings nicht Schildburg, und so wird das Tagungszentrum von einem vollständig autarken Netzwerk einschließlich eigener Internetzugänge versorgt. Nur ein paar wenige Netzwerkdosen im und um den Empfang waren mit dem Netz der Stadtwerke verbunden, mutmaßlich um interne Systeme sowie die Telefonanlage zu erreichen. So ein Haus mit oft wechselnden Gästen und ohne Bedarf für eine Wachmannschaft ist natürlich ideal, um eigenes Gerät für den Zugang zu platzieren. Gesagt, getan. Ein arbeitsloser Pokini Z1 mit einer frischen Minimalinstallation Linux bekam via Ethernet prompt vom DHCP-Server die notwendigen IPv4-Parameter für den Zugang zum Firmennetz und offerierte uns dann „auf der anderen Seite“ einen WLAN-Hotspot für einen komfortablen Fernzugang.

Sind die Angreifer einmal im „internen“ Netzwerk, müssen sie unbemerkt an die nächste Stufe der notwendigen Informationen gelangen. Hier können durchaus böse Überraschungen auf sie warten, denn die Angreifer befinden sich nun auf dem Terrain der angegriffenen Organisation und die kann sich den Heimvorteil zunutze machen. Leider sind die meisten IT-Abteilungen derart unterbesetzt, dass schon der reguläre Betrieb eine Herausforderung für die dünne Personaldecke ist – ganz zu schweigen davon, dass mal jemand krank wird. Für Nachforschungen zu Ursachen von auffälligem Systemverhalten oder ungewöhnlichem Netzwerkverkehr ist einfach keine Zeit. Da wird lieber in Anschaffung und Lizenzgebühren einer weiteren magischen Security-Appliance, gerne in Gelb, investiert, als die gleiche Summe für die leistungsfähigste adaptive Muster- und Anomalie-Erkennung auszugeben, die bisher bekannt ist: Menschen.

Aber auch ohne jede Gegenwehr kann es für die Angreifer schwer werden. Gehört die angegriffene Organisation beispielsweise zu den wenigen, bei denen eine galvanische Trennung (Air Gap) nicht nur auf PowerPoint-Folien, sondern auch in der realen Welt das eigentliche Zielsystem vom restlichen Netzwerk trennt, so müssen Informationen



Fernwartungszugänge wie dieser finden sich häufig völlig ungeschützt im Internet.

© Copyright by Heise Zeitschriften Verlag
Persönliches PDF für alle Leser der c't aus 30625 Hannover

Anzeige

© Copyright by Heise Zeitschriften Verlag
Persönliches PDF für alle Leser der c't aus 30625 Hannover

über Update-Prozesse, Verantwortlichkeiten, sowie Art und Form der transferierten Daten ausfindig gemacht werden. Auch hier unterscheidet sich ein Penetrationstest deutlich von einem Angriff nationalstaatlicher Akteure, denn Letztere greifen in so einem Fall schnell auf Wege der Informationsbeschaffung durch Gewaltanwendung zurück.

Passwörter

Im Normalfall haben es Angreifer allerdings deutlich leichter. Prekäre Personalausstattung sowie permanente nachdrückliche Wünsche aus Führungsetagen nach mehr Echtzeitdaten und Dashboards führen zu einer immer intensiveren Vernetzung. Allerdings sind selbst die unbedachtesten Konstruktionen nicht für jeden Mitarbeiter zugänglich. Die Angreifer müssen also zuerst das Netz erkunden, genauso als wenn sie in ein unbekanntes Bürogebäude eingebrochen wären: Man muss an jeder Bürotür rütteln (Port-Scan), und sollte die Tür irgendwie aufgehen, muss der Eindringling nach Dingen suchen, die zum Erreichen des eigentlichen Zieles hilfreich sein könnten. Wer LucasArts Adventures gespielt hat, kennt das Muster sicherlich.

Bei einem zielgerichteten Angriff geht es vor allem um Benutzerkonten und deren Passwörter sowie um Informationen über die technische Seite des Arbeitsprozesses, vulgo Workflow. So war im Fall der Stadtwerke Ettlingen bekannt, dass es einen Übergang vom Unternehmensnetzwerk zu dem der Leitstelle geben soll. Geschwätzige Layer-2-Discovery-Protokolle verkündeten regelmäßig die wichtigsten Informationen über aktive Netzwerkkomponenten, sodass für die Erkundung der Topologie nicht einmal Port-Scans nötig waren. Mittels SNMP konnten wir einige Router befragen und die so gewonnenen Routing-Informationen wiesen uns den IP-Weg zur Leitstelle. Parallel hierzu liefen im Hintergrund diverse Port-Scans.

Wir vermuteten allerdings von vornherein, dass der Zugang zur Leitstelle nur über bestimmte Benutzerkonten möglich sein würde. Hier tauchen die Parallelen zu Adventure-Games wieder auf, denn die Sammelleidenschaft ist des Angreifers Freund. Unterwegs waren bereits einige Benutzerverzeichnisse im Säckel gelandet, beispielsweise von anonym abzufragenden Verzeichnisdiensten. Darin konnten wir Personen identifizieren, für die überall ein Konto eingerichtet war. Die nahezu gleiche Gruppe Personen verfügte oft auch noch über hohe Privilegien im jeweiligen System. Dieser Zusammenhang legte nahe, dass wir da bereits eine Liste der Administratoren erstellt hatten.

Die Systemarchitektur der Leitstelle war aus den Vorbesprechungen nur sehr oberflächlich bekannt. Außerdem stellt sich die Wirklichkeit aus Blick des Angreifers immer etwas anders dar, vor allem bei vorher völlig unbekannten Lösungen. Informationen auf der Webseite des Herstellers ließen erkennen, dass eine übliche Installation einen Windows Fat-Client verwendet. Also begaben wir uns auf die Suche nach einer Kopie dieser Software, die vermutlich auf irgendeiner Freigabe, einem FTP-Server oder Ähnlichem herumliegen würde. Als diese langwierige Suche endlich von Erfolg in Form eines Backups gekrönt war, kamen die Namen der Administratoren zum Einsatz.

Die Leitstellen-Software verfügt natürlich über eine eigene Benutzerverwaltung, welche auf keine bekannte Kontendatenbank zurückzugreifen schien. Allerdings war es sehr wahrscheinlich, dass einer oder mehrere der Administratoren auch hier Konten hatten. Die Suche nach den Nachnamen förderte sogleich mehrere Dateien zutage – aber nur eine enthielt alle Namen. Mit der von Berufswegen antrainierten Fähigkeit, auch in einem unbekannten Binärformat Muster zu erkennen, fiel sofort ins Auge, dass in unmittelbarer Nähe der Namen jeweils eine Zeichenkette aus 32 Zeichen Hexadezimalziffern auftauchte. Unsere erste Hypothese: MD5-Hashwerte. Die CUDA-Variante von Hashcat sah das ähnlich und lieferte in weniger als drei Sekunden die ersten beiden dekodierten Passwörter. Eine erfolgreiche Anmeldung an einem ausschließlich lesend eingebundenen Monitoring-System bestätigte, dass nun gültige Konten zur Verfügung standen.

Erfolg

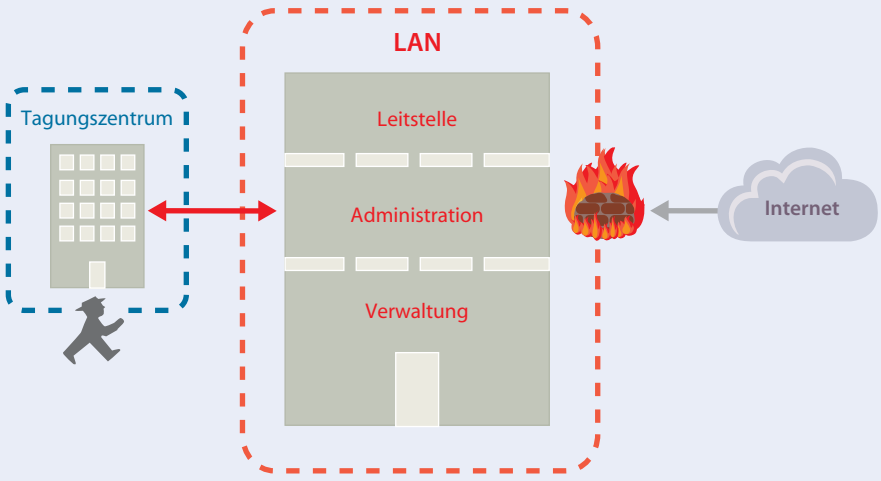
An diesem Punkt bei Penetrationstests von Produktionsumgebungen muss der Angreifer ein paar Gänge runter schalten, denn jetzt ist vorsichtiges und besonnenes Vorgehen gefragt. Die Zielsetzung ist bis zu diesem Punkt auf hochprivilegierte Zugänge fokussiert. Jede Fehlbedienung hat allerdings umso größere Auswirkungen, je mehr Privilegien der Zugang hat. Man spielt ja auch bei einem Krankenhausbesuch nicht einfach mal an den Knöpfen der Geräte rum, nur weil man herankommt. Bösartige Angreifer haben dieses Problem selten, denn sie müssen nur alle Schalter für „Aus“ finden. Richten sie dabei anderen Schaden an, spielt das für sie keine Rolle. Soll allerdings die Beeinflussung durch den Angriff so subtil wie bei Stuxnet sein oder einen bestimmten physischen Schaden zur Folge haben, kostet das Erarbeiten des notwendigen Wissens und die Entwicklung der Wirkfunktion deutlich mehr Zeit und Geld, als alle anderen Aktivitäten zusammen.

Bei Stresstests von Sicherheitssystemen, ob nun physischen oder digitalen, sollte unbedingt eine psychologische Grenze ausgelotet werden: Einerseits sollen auch fachfremde Personen ein erfolgreiches Eindringen sowie den damit verbundenen potenziellen Schaden auf Anhieb erkennen. Andererseits darf der Angriff auf keinen Fall Schaden verursachen. Jeder Schaden verwandelt die angestrebte differenzierte Beurteilung der Erkenntnisse in eine allgemeine Suche nach Verantwortlichen und Schuldigen, die bald nichts mehr mit den eigentlichen Ergebnissen zu tun hat.

Gemeinsam mit Mitarbeitern der Stadtwerke Ettlingen wurde diese Grenze gezogen, als die Steuersoftware der Leitstelle innerhalb einer virtuellen Maschine der Tester soweit startete, dass sie die Übernahme der Kontroll- und Steuerfunktionen anbot. Das Risiko, Schaden anzurichten, hatte nun einen Punkt erreicht, dessen Überschreitung absolut inakzeptabel gewesen wäre. Außerdem konnte aufgrund vorheriger Erkenntnisse dargelegt werden, dass die Übernahme mit

Der Weg nach „drinnen“

Das eigentlich getrennte Tagungszentrum hatte eine Verbindung zum internen Netz der Stadtwerke. Somit eignete es sich ideal als Brückenkopf für die weiteren Aktivitäten.

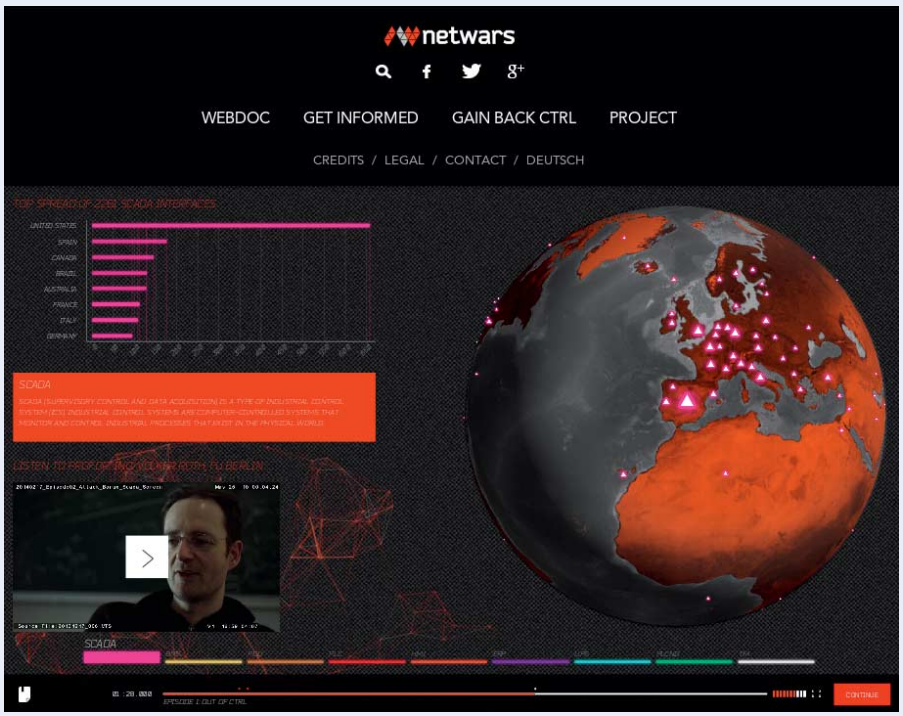


© Copyright by Heise Zeitschriften Verlag
Persönliches PDF für alle Leser der c't aus 30625 Hannover

heise online präsentiert: „netwars / out of ctrl“

Der Fernsehsender ARTE strahlt am 15. 4. um 20:15 die Dokumentation „Netwars – Krieg im Netz“ aus, in deren Rahmen Felix 'FX' Linder diesen Test durchgeführt hat. Darüber hinaus finden Sie ab diesem Dienstag auch die interaktive Webdoc „netwars / out of ctrl“ auf heise online.

Dort führt Sie ein virtueller Cyber-Dealer in die Welt der digitalen Kriegsführung ein. Er präsentiert auf unterhaltsame und hintergründige Art seine Philosophie („I don’t judge, I’m just a salesman“), gewährt Einblicke in sein Waffen-Arsenal („Why build new weapons, when you can turn anything into a weapon?“) und lässt Experten wie FX oder General Keith Alexander zu Wort kommen. Dabei entscheiden Sie selbst, ob Sie Informationen zu Bot-Netzen oder Würmern interessieren oder eher Statistiken zu SCADA-Systemen im Internet und Details zu Ihrem digitalen Fingerabdruck im Netz. Das von Filmtank realisierte, innovative Multimedia-Projekt ist als fünfteilige Serie angelegt, deren erster Teil Sie ab dem 15. 4. unter http://heise.de/netwars zum Stöbern und Gruseln erwartet.



Die Webdoc kombiniert kurze Videos mit Statistiken und anderen Hintergrundinformationen rund um das Thema Cyberwar.

sehr großer Wahrscheinlichkeit funktionieren würde; quod erat demonstrandum.

So gradlinig der Angriff klingt, beschreibt er doch nur einen kleinen Ausschnitt des Gesamtbildes. Dies ist ein inhärentes Problem von Penetrationstests. Da solche Test-Angriffe strikt zielgerichtet sind, ist der Erfahrungsgewinn primär auf Seiten der Angreifer. Wer das System verteidigen muss, weiß nun von einem einzigen Weg ins Innere, aber nichts über die Gesamtsituation. Es wurden deshalb neben dem zielgerichteten Experiment eine Reihe weiterer Aspekte betrachtet und mit dem Team der Stadtwerke diskutiert. Denn deren Wissen und Erfahrung aus der täglichen Arbeit spielen eine entscheidende Rolle bei der Wahl möglicher Verbesserungen. Anmaßungen seitens der Angreifer sind hier schlicht fehl am Platze.

Die Menschen, die unsere tägliche Versorgung sicherstellen, sind selbst die beste Verteidigung gegen Angriffe auf kritische Infrastrukturen. Was Angreifer mit Laptops ausschalten, können Leute im Blaumann auch wieder anschalten. Das Experiment zeigte nur eine Seite. Vor allem lokale Versorger haben da einen großen operativen Vorteil im Falle von IT-verursachten Ausfällen, ob nun absichtlich herbeigeführt oder nicht: Man kann schnell mal hinfahren, und viel wichtiger: Man kann es auch manuell bedienen. Aber auch große Versorger denken zunehmend über Fragen des Wiederanlaufs nach, die mit zunehmender Größe allerdings auch zunehmend schwieriger sind.

Das Wichtigste zum Schluss

Trotz der engen Zusammenarbeit mit dem Team der Stadtwerke wären alle Erkenntnisse bedeutungslos, würden sie nicht aufbereitet und niedergeschrieben. Ein Selfie von ein paar stolzen Hackern weckt nach einem Jahr vielleicht noch Erinnerungen, arbeiten kann damit keiner. Kontext, Zielsetzung und Vorgehen sind mindestens so wichtig wie die einzelnen Ergebnisse, denn jede IT-Umgebung ändert sich kontinuierlich. Daher ist es immens wichtig, die Ergebnisse auch nach einiger Zeit und in einer veränderten Umgebung einordnen zu können.

Die Dokumentation ist noch aus einem weiteren Grund das einzig entscheidende Arbeitsergebnis, denn natürlich sollen erkannte Schwachstellen in einzelnen Produkten auch dem jeweiligen Hersteller mitgeteilt werden. Die Stadtwerke Ettlingen gingen hier sogar noch einen Schritt weiter und luden Hersteller zu Gesprächen ein, um gemeinsam angemessene Lösungswege zu vereinbaren. Der Austausch der verschiedenen Blickpunkte seitens Angreifer, Betreiber und Hersteller schafft außerdem ein nachhaltiges Verständnis, welches weit über die Bereitstellung eines Patches hinausgeht. Derlei Luxus ist allerdings bei Anbietern, die sich dem Druck täglich aktualisierter Tiefstpreis-Listen stellen müssen, kaum noch möglich.

Und was ist jetzt mit Cyberwar? Aus der Sicht der Angreifer gab es zwei Erkenntnisse: Eindringen und Kontrolle sind realistische Ziele, diese Kontrolle zu behalten eher nicht. Herkömmliche Stromnetze haben so viele elektrotechnisch-mechanische Schutzelemente sowie analoge Anzeigen, dass jede Aktion sofort auffällt – und zwar eben nicht nur in der Leitstelle. Was die Bediener in der Leitstelle sehen, können Angreifer manipulieren. Schon die Zeiger im Umspannwerk sind für sie aber außer Reichweite. Nimmt man die Stadtwerke Ettlingen als repräsentativ an, würde sich ein „Cyber“-Angriff auf einen Lokalversorger für die betroffenen Bürger wohl wie ein kurzer Stromausfall anfühlen.

Die Situation stellt sich allerdings komplett anders dar, sobald „SmartGrid“ ins Spiel kommt. Der Angriff wird nicht schwieriger, doch Betreiber können die Kontrolle nicht so einfach wiedererlangen. Schon in 2009 wurde ein Stromzähler-Wurm entwickelt, der sich über Funk verbreitet. Marc Elsbergs Roman „Blackout“ illustriert in bedrückendem Detail die Auswirkungen eines koordinierten Angriffs auf diese „weiterentwickelte“ Stromversorgung. Da Namen durchaus zur allgemeinen Bewertung einer Technologie beitragen, sollten man also vielleicht unsere heutigen, recht stabilen Stromnetze besser als „SolidGrid“ bezeichnen. (ju) c't

© Copyright by Heise Zeitschriften Verlag
Persönliches PDF für alle Leser der c't aus 30625 Hannover