Prototypische IT-Bedrohungsszenarien

Unter Beobachtung

Martin Wundram, Markus Loyen, Alexander Sigel

Cyberkriminalität bedeutet nicht immer, Großkonzerne anzugreifen und Regierungssysteme zu hacken. Zwar gibt es auch bei kleineren Firmen aufsehenerregende Vorfälle, doch die meisten Angriffe auf IT-Systeme sind weniger spektakulär und auffällig – und darum umso gefährlicher. Wie man Angriffen und manchmal den Tätern auf die Spur kommt, berichten drei Forensikexperten.

Wie angreifbar Unternehmen tatsächlich sind, merken sie häufig erst nach sogenannten Penetrationstests in ihre IT-Systeme oder bei einer Risikoanalyse der Infrastruktur. Je mehr Abläufe IT-gestützt sind, desto mehr Gelegenheiten bieten sich naturgemäß für Sicherheitsvorfälle. Dabei ist am Ende nicht alles, was die Experten zunächst als schweren Sicherheitsvorfall einstufen, auch ein ausgewachsener Spionageangriff. Bisweilen gehen Sicherheitsvorfälle auf technische Probleme (zum Beispiel einen instabil laufenden Server), aber auch auf die Bequemlichkeit oder Unwissenheit von Administratoren zurück.

Code-Injection: Auch derbe Scherze können zu Sicherheitsvorfällen führen. Denn es gibt sie noch oft, die eher vergnüglichen Hacks, die nächtens bei einem Glas Bier zustande kommen. Eine nebenbei gefundene Injection-Schwachstelle auf der Webseite eines Internet-Providers etwa führte zum Einfügen der launigen Falschmeldung „Vorstandsvorsitzender Mustermann tritt wegen Datenskandal zurück“ und einer freundlichen E-Mail an die Adresse seiner Assistentin. Zum Dank zurück kam per Post ein sehr nettes Schreiben inklusive Gutschein für zwei für ein üppiges Essen in einem Nobelrestaurant.

Missbrauch von Administratorrechten: Neben diesen vergleichsweise harmlosen Fällen gibt es solche, von deren Ausgang die persönliche Zukunft von Menschen abhängt. Vor einiger Zeit bemerkte die interne Revision eines mittelständischen Unternehmens in sehr ländlicher Umgebung, dass der zentrale Web-Proxy mehrfach den Abruf von Webseiten mit pornografischen Inhalten blockiert und dies protokolliert hatte. Einige der gesperrten Seiten enthielten Hinweise auf kinderpornografische Inhalte. Da sich diese Fälle wiederholten, aufgrund einer Betriebsvereinbarung jedoch keine IP-Adressen erfasst wurden, entschied sich die Revision, die Anwesenheitszeiten der Mitarbeiter mit den Zeitstempeln der gesperrten Abrufe abzugleichen. Die Geschäftsleitung nutzte das Zeiterfassungssystem jedoch nicht und so konnten die einzelnen Geschäftsführer mangels Nachweis der Abwesenheitszeiten nicht entlastet werden. Übrig blieben daher als potenzielle Abrufer nur wenige Mitarbeiter, die Geschäftsleitung sowie ein Abteilungsleiter.

Den Falschen im Visier

Abteilungsleiter A. stimmte einer zielgerichteten Auswertung seines Computers

zu, ebenso alle anderen Kollegen. Denn niemand wollte der Aufklärung eines so heiklen Falles im Wege stehen. Auch der Abteilungsleiter nicht – zumindest solange, bis auf seinem Laptop in einem Unterordner seiner „Eigenen Dateien“ etliche kinderpornografische Bilder gefunden wurden. Für die interne Revision war der Fall mit der Erstattung einer Strafanzeige zunächst abgeschlossen, galt es doch unter anderem, Schaden vom Unternehmen fernzuhalten. Für A. hingegen begann ein Spießrutenlauf: Gerichtsverhandlungen, Beteuerung der Unschuld, auf dem Land nicht wirklich anonymisierbare Berichterstattung in der lokalen Presse und warnende anonyme Zettel in der Nachbarschaft. Niemand glaubte dem bislang unbescholtenen A. Zwar fanden sich keine Spuren eines Abrufes von Webseiten auf seinem Rechner, aber die Bilder selbst sollten ja Beweis genug sein.

Ein hinzugezogener Gerichtssachverständiger fand bei der gründlicheren Auswertung des Laptops mehrere Auffälligkeiten. So waren alle relevanten Bilder bemerkenswert kryptisch benannt. Genauer: Die damals verbreitete Version des Browsers „Firefox“ speicherte Dateien im Cache ohne Dateinamenserweiterung. Alle Bilder im Fall hatten aber die Erweiterung *.jpg*, obwohl einige davon PNG-Dateien waren. Außerdem ließ sich über die Dateigrößen und die jeweiligen Erstellungszeitstempel abschätzen, dass die Bilder hintereinander mit circa 10 MByte/s auf die Festplatte kopiert wurden. Alles eher unüblich für einen gewöhnlichen Download von Webseiten inklusive Bildern. Im zugehörigen Ordner fand sich nach ein wenig File Carving (s. Glossar) schließlich auch eine zuvor gelöschte Lesezeichen-Datei, die dank der darin enthaltenen Einträge einem der drei IT-Administratoren des Unternehmens eindeutig zuzuordnen war.

```
[68] => [New_Anzahlverk
[69] => [New_BLZ] =>
[70] => [New_Bank] =>
[71] => [New_Bankkonto]
[72] => [New_KontoInhab
[73] => [New_Finanzamt]
[74] => [New_SteuerNr]
[75] => [New_HGBNr] =>
[76] => [New_UStID] =>
[77] => [New_Beschreibu
[78] => [New_uebergeord
[79] => [New_MAid] =>
[80] => [New_Vorname] =
```

Sicherheitslücken oder zu lax konfigurierte Webserver sind die Ursache, dass häufig vertrauliche Daten wie die abgebildeten ins Netz gelangen oder von Cyberkriminellen ausgelesen werden können (Abb. 1).

Damit klärte sich ein diffiziler Fall endlich auf. Denn nach Konfrontation mit den gefundenen Spuren gestand der Administrator, selbst die Webseiten mit den fraglichen Inhalten abgerufen und über die administrative Freigabe aus dem eigenen Cache heraus die relevanten Bilder auf den Laptop von A. kopiert zu haben, mit der Absicht, sie dem verhassten Ableitungsleiter unterzuschieben. Dass er aus Versehen aus seinem Firefox-Profil auch die *bookmarks.html* mit kopiert hatte, hatte der Administrator zwar noch bemerkt und sie wieder gelöscht. Dumm für ihn, dass genau diese Datei wiederhergestellt werden konnte.

Captcha-Betrug mittels Booster: Ein internationaler Versandhändler bot kürzlich eine Mitmachaktion an, bei der Kunden und Interessenten ein zum jeweiligen Motto passendes Bild hochladen und die Bilder anderer bewerten konnten.

iX-TRACT

- Im Alltag sind es weniger die spektakulären Vorfälle, sondern kleinere und manchmal trivialere Vorkommnisse, die IT, Business und sogar die Existenz eines Unternehmens bedrohen können.
- Wenn ein Unternehmen seine IT im Griff und Standardmaßnahmen wie Abschottung seines Netzes, kontrollierte Zugriffe auf allen Ebenen et cetera umgesetzt hat, hat es die Voraussetzung geschaffen, Sicherheitsvorfälle zu vermeiden oder mindestens die Aufklärung zu vereinfachen.
- Unerlässlich für die nachträgliche Analyse von Vorfällen ist eine gute Zusammenarbeit von Administrator, IT-Abteilung und ermittelndem Experten. Besser als jede Aufklärung ist jedoch immer noch die Vermeidung.

Zum Schutz vor Mehrfachabstimmungen war ein als sicher angesehenes und verbreitetes Standard-Captcha-System jedem Voting vorgeschaltet. Die Angabe einer E-Mail-Adresse oder eines Kundenkontos war nicht nötig. Auf den Wochengewinner mit den meisten Stimmen warteten jeweils 1000 € und auf den Gesamtsieger zwei Monate später üppige 10 000 €. Dies lockte reichlich Teilnehmer an, der Marketingplan des Händlers ging zunächst auf.

Tatort Internet: Der Betrug mit den Klicks

Bald schon meldeten sich jedoch frustrierte Kunden, die über mangelnde Teilnahmechancen im Vergleich zum jeweils Meistgewählten berichteten. Wie konnte es sein, dass innerhalb kürzester Zeit ein eher weniger originelles Bild uneinholbar vorne lag? Die Antwort lieferte die Auswertung der Server-Logs. Von einer begrenzten Anzahl von IP-Adressen aus dem universitären Umfeld wurden je IP bis zu 8 Captchas/Votes in der Minute ausgefüllt. Das Logfile zeigte die Nutzung pro IP für mehrere Stunden am Abend und in der Nacht, unterbrochen von mehrstündigen Pausen hauptsächlich tagsüber. Außerdem wurden von allen auffälligen IP-Adressen aus verschiedene User-Agents verwendet, unter anderem auch der Browser eines älteren Smartphones, noch ohne Touchscreen. Es wäre also gar nicht möglich gewesen, so schnell Captchas über dieses Benutzer-Interface einzugeben.

Nach anfänglichem Leugnen bestätigten die ermittelten Voting-Gauner doch die Einschätzung der von uns unterstützten Sicherheitsabteilung: Sie hatten einen Captcha-Booster programmiert, ein kleines Skript, das auf dem PC des Voters für jede neue Stimmabgabe lediglich das jeweilige Captcha-Bild, ein Eingabefeld und einen Absenden-Button anzeigte. Die Webseite des Versandhändlers musste damit nicht mehr individuell und langwierig jedes Mal neu aufgerufen werden.

Während technische Dienstleister bei Online-Glücksspielen aufgrund der großen Summen, die im Spiel sind, auf ein sicheres Design der Anwendungen achten, finden sich gelegentlich im Webbrowser ablaufende Flash- oder HTML5-Spiele, bei denen Hacker den clientseitig generierten Highscore manipulieren können. Das ist besonders interessant, wenn auf den Langzeit-Besten eine Prämie ausgesetzt ist. In einem Fall hatte das verantwortliche IT-Unternehmen entschieden, dass eine bestimmte, dynamisch geschützte Übertragung des Spielstandes an den Server für die Sicherheit ausreicht. Dabei hatte man jedoch nicht bedacht, dass ein Angreifer mit frei verfügbaren Werkzeugen aus dem Datenstrom den unverschleierten ActionScript-Quelltext der Flashanwendung wiedergewinnen konnte, der dieses Geheimnis offenlegte und damit die Generierung beliebiger Highscores ermöglichte.

Datenabfluss ins Internet verhindern

Viele Experten messen den Sicherheitslücken in Webapplikationen noch zu wenig Bedeutung bei und würden daher eher eine Schwachstelle in einem komplexen Verschlüsselungssystem suchen als eine Cross-Site-Scripting-Schwachstelle. Doch Webseiten und ihre -anwendungen beziehungsweise die dahinterliegenden Systeme beinhalten nicht selten besonders vertrauliche Daten. Deren Verlust kann ein Unternehmen die Reputation und Kunden kosten.

Local-File Inclusion: Vor einigen Jahren meldete sich ein Benutzer bei dem Betreiber einer Plattform, der exklusive Partys in ausgewählten Locations koordiniert – mit Partnertausch und eindeutigen Absichten. Eine Teilnahme setzt zunächst eine Webregistrierung unter Angabe persönlicher Daten, Fotos und persönlicher sexueller Vorlieben voraus sowie ein abschließendes persönliches Vorabtreffen mit den Veranstaltern. Der Benutzer hatte auf dieser Plattform eine Local-File-Inclusion-Schwachstelle entdeckt und darüber den ungesalzenen, also ohne Hinzunehmen eines Zufallswerts generierten, DES-Passwort-Hash des Administrator-Accounts auf dem Dateisystem des Servers (*.htpasswd*-Datei) gefunden. Außerdem konnte er durch einen anschließenden Brute-Force-Angriff das Passwort in Klartext wandeln.

Der nun alarmierte Veranstalter bedankte sich gebührend und beauftragte bei einem Sicherheitsdienstleister die gründliche Suche nach weiteren potenziellen Schwachstellen. Ein Abfließen vertraulicher Daten konnte so schließlich verhindert werden. Auch lagerte der Verantwortliche den Datenbankserver auf ein eigenes gesondertes System inklusive gesicherter Schnittstelle aus.

Bei einem solchen Pentest machten die beauftragten Tester in einem anderen Fall einen aus IT-Sicht trivialen, dennoch interessanten „Beifang“. Die zu testende Flirtplattform bot als besonderen Dienst für ihre Nutzer und zum finanziellen Vorteil des Betreibers kostenpflichtige Sprachnachrichten, die man per Telefon im System für einen bestimmten Empfänger hinterlassen konnte. Diese wurden auf dem Webserver in einem einzigen Verzeichnis gespeichert. Es lag unachtsamerweise direkt im *DocumentRoot* des Webservers und erlaubte das einfache Abrufen des Inhaltes über den Aufruf des Verzeichnisses (www.flirtexample.com/voicemessages/).

Ein schlecht konfiguriertes Videokonferenzsystem war die Ursache, dass man dieses Unternehmen über Internet bei seinen Besprechungen belauschen konnte (Abb. 2).

Geheime Vorlieben nachlässig gespeichert

In den jeweiligen Dateinamen eincodiert waren der Zeitstempel der Erzeugung, die Benutzer-ID des Absenders und die des Empfängers. Gespeichert waren alle

jemals erzeugten Sprachnachrichten mit Interessens- und Liebesbekundungen, unabhängig davon, ob die jeweiligen Benutzer noch im System vorhanden waren oder nicht. Mit den Erkenntnissen des durchgeführten Pentests konnte das Unternehmen dieses gravierende Datenschutzproblem beheben, Sprachnachrichten auslagern und alte Nachrichten löschen.

Google-Hacking: Die Autoren haben selbst mit einer langjährig bekannten Trivialsuche („Google Dork“) wie *inurl: /backup* eine Datensicherung des Laptops eines US-amerikanischen CEOs mehrerer IT-Unternehmen gefunden, die dieser versehentlich für jeden abrufbar in das Verzeichnis */backup* auf seinen Webserver hochgeladen hatte. Dieser Datencontainer enthielt nicht nur eine logische Sicherung des aktuellen Laptops, sondern auch weitere ältere Sicherungen. Ein wenig wohlwollender „Einbrecher“ hätte beispielsweise umfänglich private E-Mails lesen, Steuererklärungen mit Abrechnungen zu Bonuszahlungen aus früherer Angestelltentätigkeit und mit Auszügen über Aktiendepots abgleichen und sogar vertrauliche Geschäftsstrategien der Unternehmen einsehen können. Entsprechend erschrocken, aber auch dankbar war der Betroffene über unseren Hinweis [1].

Ungeprüfte Datenbankabfragen: Das unkontrollierte Abfließen umfangreicher Datenbestände aus Webdatenbanken ist immer wieder ein Problem: Zufällig stießen Sicherheitsexperten auf eine PHP-Seite, die sich nach auffällig langer Wartezeit als ein circa 25 MByte großer Download und nach erster Analyse als umfangreiche Datenbank entpuppte. Damit fielen in Form eines PHP-Arrays rund 5000 Kundendaten in fremde Hände, die besonders vertrauliche Daten wie Kontoverbindungen enthielten. Es handelte sich nicht um Testdaten, weil exemplarisch überprüfte Datensätze realen Personen zuzuordnen waren und die Daten sich täglich änderten. Wie bei großen und stark frequentierten Webseiten so häufig, hatte auf Betreiberseite niemand das Datenleck bemerkt.

Viele Wege führen zu den Kundendaten

Im Nachgang zu diesem Zufallsfund machten die Sicherheitsexperten den eigentlichen Dateneigentümer in der Cloud ausfindig (es handelte sich nicht um den Betreiber der Infrastruktur) und informierten ihn über die Sachlage. Weil die verwendete CRM-Plattform auch anderorts zum Einsatz kommt, fanden sich schnell weitere betroffene Unternehmen. Zusätzlich führen zu freigiebig konfigurierte Webserver in solchen Fällen durch Directory Listing zu weiteren internen Dateien. Dabei fand sich wie so häufig auch ein Datenbank-Dump (Abb. 1).

Ab und an bedienen sich Datensauger individuell gefertigter Screen-Scraper. Gelegentlich sind Portale jedoch auch anfällig für einfaches und vor allem vollständiges Abgreifen aller Daten. In manchen Fällen ist etwa über den Webshop die Kundendatenbank im Netz erreichbar (zum Beispiel als unverschlüsseltes Quicken-Backup, das Anschriften und manchmal sogar Kreditkartennummern enthält).

Fehlende Datenseparierung: Der für einen Energieversorger durchgeführte Pentest des Web-Kundenbereichs förderte eine extrem simple, aber fatale Schwachstelle zutage. Durch bloßes Verändern einer ID in der Adresszeile (GET-Parameter) ließen sich sämtliche Rechnungen aller Kunden der letzten acht Jahre herunterladen, obwohl die Kunden selbst nur ihre aktuelle Rechnung und die des letzten Jahres zu Gesicht bekamen. Das ungeschützte und unbedachte Andocken vormals zentraler und isolierter Unternehmensdatenbestände an das Web-Frontend war hier eine Ursache.

Konfigurationsfehler: Wer seine Systeme sorglos konfiguriert, erspart dem Hacker dessen eigentliche Arbeit. Ein Bürodienstleister vermietet Konferenzräume mit IT-Infrastruktur auf Zeit. Bei einem Pentest stellte sich heraus, dass neben dem VoIP-System auch die Cisco-Router und Videokonferenzsysteme derart nachlässig konfiguriert waren, dass praktisch jeder via Internet Netzwerkeinstellungen verändern, Netzwerkverkehr mitsniffen und Telefonkonferenzen belauschen kann (Abb. 2). Bei Videokonferenzen genutzte Kameras ließen sich außerdem drehen und zoomen, sodass vertrauliche Texte auf Flipcharts besser lesbar wurden [2].

Trotz funktionierender, aber offensichtlich falsch konfigurierter Firewall hatten interne Geräte unnötigerweise externe IP-Adressen, zudem konnten über die Weboberfläche von Multifunktionsgeräten Vorschauansichten vertraulicher Dokumente (Thumbnails) sowie zuletzt gedruckte Dokumente, der Verlauf der empfangenen und gesendeten Faxe sowie Adresslisten eingesehen werden. Kurioserweise war mit der Datei *Ergebnisse_Netzwerkaudit.xls* ein vorheriges Auditergebnis abrufbar, ohne Erwähnung dieser Lücke.

Die Erfahrung zeigt: Dies ist kein Einzelfall. Immer wieder gelingt in Pentests ohne Schwierigkeiten der Zugriff auch auf höchst vertrauliche Daten über falsch konfigurierte Endgeräte, etwa über deren Weboberflächen. Selbst psychiatrische oder onkologische Befunde mancher Kliniken sowie Passwörter für das ActiveDirectory waren bei einigen Pentests offen für jeden über das Internet zugänglich.

Abfragen mit regulären Ausdrücken: Ein interessanter Fall bei der technischen Begleitung eines Start-up-Unternehmens ergab sich bei der Betrachtung der Konkurrenz in diesem Markt. Ein Wettbewerber warb mit besonders hohen Mitgliederzahlen und einem hohen Anteil zahlender Premiumkunden. Durch einen einfachen regulären Ausdruck (^ – *Caret*) gab das Suchformular nicht nur einen einzelnen Treffer, sondern alle Datensätze der Datenbank aus. Dies waren allerdings nur wenige Hundert Kunden, die zudem kaum Premium-Dienste gebucht hatten.

Übertreibungen der Konkurrenz entlarven

Damit war der Mitbewerber als Aufschneider enttarnt. Da für jeden Eintrag ein Registrierungsdatum ausgegeben wurde, ließ sich der bescheidene Mitgliederzuwachs auch grafisch darstellen (Abb. 3). Mit welchen Sicherheitsmechanismen man unerwünschte Datenbank-Einblicke via Internet verhindert, beschreibt [3].

Bei der Aufklärung sicherheitsrelevanter Vorfälle gehen IT-Forensik und IT-Sicherheit Hand in Hand. So wurde eine wichtige Webanwendung eines Reiseanbieters verunstaltet (defaced). Zu befürchten stand, dass mit dem fremden Zugriff auf die Seite auch der Verlust vertraulicher Kundendaten einherging. Der IT-Dienstleister erzeugte ein forensisches Abbild des Servers. Der Reiseveranstalter beauftragte IT-Forensiker, den Einbruch zu untersuchen. Dabei galt es zunächst besondere Herausforderungen zu überwinden: Das Linux-System war vollverschlüsselt. Zudem musste aus Sicherungen einzelner Festplatten das komplexe RAID wieder zusammengesetzt werden. Schließlich war auch die PHP-Webanwendung verschlüsselt und diese Verschlüsselung an die Hardware gebunden.

Letztlich konnten die Forensikexperten belegen, dass über eine Remote-File-Inclusion-Schwachstelle eine PHP-Shell installiert worden war. Eine Schwachstelle im schon lange nicht mehr gepatchten Betriebssystem hatte dem Angreifer mittels Rechteeskalation („privilege escalation“) eine Root-Shell geschenkt. Der Täter hatte zwar versucht, seine Spuren zu verwischen, indem er die Protokollierung der eingegebenen Befehle löschte, dank der bitgenauen Sicherung konnten die Experten die Protokolldateien aber aus dem freien Speicher teilweise wiederherstellen. Ein Abfließen vertraulicher Daten konnten sie nicht nachweisen.

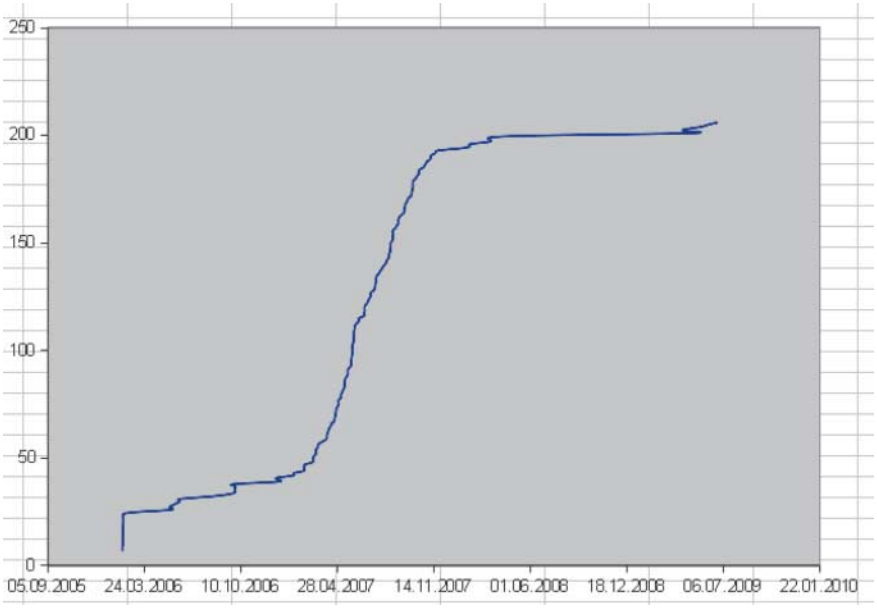
Gefahr durch Innentäter: An einem großen Industriestandort gab es immer wieder Probleme mit IT-Systemen und der -Infrastruktur. Da oft zwei der Administratoren als Helfer in der Not auftauchten und dabei die übrigen IT-Experten als Ahnungs- und Hilflose vorführten, kam der Verdacht auf, dass man es hier mit zwei profilierungsfreudigen „Feuerteufeln“ zu tun habe. Ein vorsichtig geführtes Gespräch konnte den Verdacht nicht ausräumen – im Gegenteil.

Einige Zeit später funktionierte erstmals das PC-System nicht mehr, das die Funkanlage für die Werkfeuerwehr steuerte. Der PC konnte keine erfolgreiche Verbindung zum Funksystem aufbauen und damit keine der öfter notwendigen Frequenzwechsel mehr steuern. Die gesamte Funkanlage war schon sehr alt, das Handbuch nur eine Kopie von der Kopie, und die beiden Administratoren konnten sich das Problem leider überhaupt nicht erklären. Gemeinsam mit einem externen Sachverständigen untersuchte die Werkfeuerwehr an den Admins vorbei das System und fand den Fehler zügig: Die serielle Schnittstelle war in der Konfigurationsdatei von 1 auf 0 geändert worden und deshalb war keine Kommunikation mehr möglich.

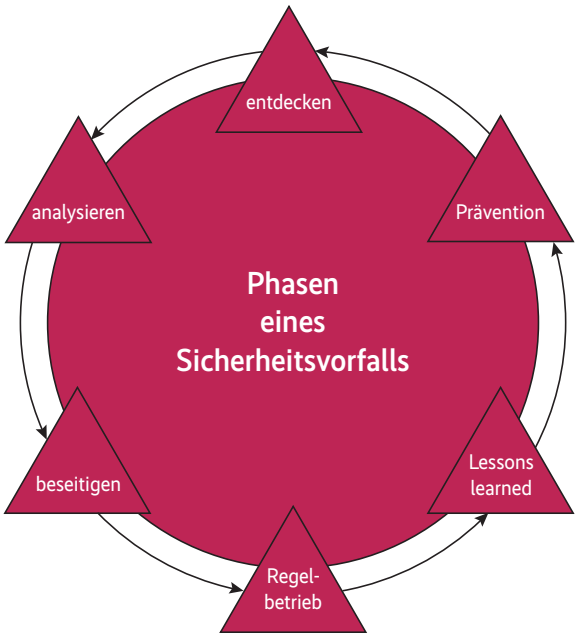
Der Administrator als böser Bube

Mit dieser Erkenntnis konfrontiert erklärte nun einer der beiden Administratoren ausweichend, dass er genau das schon oft gemacht habe und dass der Wechsel des COM-Ports „hin und her“ zwischen 0,1 und 2 bei den vielen in der Vergangenheit aufgetretenen Kommunikationsproblemen immer geholfen hätte. Die im Anschluss durchgeführte IT-forensische Auswertung zeigte hingegen einen seit dem Jahr 2000 nur wenige Male benutzten Editor und aufgrund der Spuren im freien Speicher lediglich eine alte Konfigurationsversion mit der COM-Variante 2 sowie einige mit der COM-Variante 1. Der überhaupt nicht im System existierende COM-Port 0 fand sich lediglich in der aktuellen Konfigurationsdatei wieder. Mit dieser abweichenden Erkenntnis konfrontiert, gaben beide IT-Experten die Sabotage zu.

Bei einem produzierenden Industrieunternehmen mit komplexer IT-Infrastruktur kam es über einen längeren Zeitraum immer wieder zur vollständigen Löschung von Smartphones von Mitarbeitern. Das war so lange nicht problematisch, bis auch das Gerät des Chefs betroffen war. Verdächtigt wurden ausgewählte IT-Administratoren. Natürlich gab es Standard-Kennwörter für wichtige



Vorsicht vor Übertreibungen, denn mit regulären Ausdrücken lassen sich schlecht gesicherte Datenbanken auslesen – sehr zur Freude der Konkurrenz. Hier die Kundenregistrierung einer Webplattform im Zeitverlauf (Abb. 3).



Wichtig bei Sicherheitsvorfällen ist eine zügige Analyse und Aufklärung sowie das Einfließen der daraus resultierenden Erfahrung in die Vermeidung zukünftiger Vorkommnisse (Abb. 4).

Server – darunter für den primären Domänencontroller – die seit Ewigkeiten niemand mehr geändert hatte. Auch früher ausgeschiedene IT-Mitarbeiter hätten dieses Passwort kennen können.

Man schaltete externe Spezialisten ein. Besonders knifflig war, dass die Tätigkeit verdeckt sowie datenschutzkonform erfolgen musste. Wochen später, nach etlichen bitgenauen Images und der Auswertung mehrerer Gigabyte an Logdaten verschiedenster Couleur verdichteten sich die Spuren: Dank BlackBerry Enterprise Server war die Unternehmens-Firewall und das Unternehmens-VPN umgangen worden. Auf einem der Exchange-Server fand sich ein zusätzlich installierter Telnet-Server. Dorthin verband sich vom BlackBerry aus ein Telnet-Client. So wurde ein auf dem Server an unverdächtiger Stelle liegendes und mit einem harmlosen Dateinamen versehenes PowerShell-Skript gestartet, das Exchange spezifikationsgemäß veranlasste, ausgewählte Clients remote zu löschen, wenn sie sich das nächste Mal mit Exchange verbinden. Die Überprüfung von Anwesenheitszeiten und VPN-Logs war nicht aussagekräftig, weil der Angriff über einen nicht geloggten privaten Zugang und zu unterschiedlichen Zeitpunkten erfolgt war.

Vermeintliche Sabotage: Die nahe gelegene Auslandsniederlassung eines Konsumgüterherstellers litt unter Netzwerkproblemen. Das per VoIP angebundene Callcenter meldete immer wieder Probleme mit der Gesprächsqualität bis hin zu ärgerlichen Aussetzern, überdies dauerten Zugriffe auf den Dateiserver mitunter auffällig lang. Der Niederlassungsleiter hatte den in Teilzeit arbeitenden Administrator im Generalverdacht und ging von Sabotage, wenigstens jedoch von vorsätzlich schlampiger Arbeit aus. Daher startete er ein Geheimprojekt, bei dem ein Sachverständiger ohne Wissen des Administrators im Netzwerk ermitteln und die Ursache finden sollte.

Während des vorab geplanten Termins, als erste Netzwerksensoren bereits platziert waren, erschien jedoch aus heiterem Himmel besagter Admin im Büro, der an diesem Tage eigentlich Urlaub hatte. Das machte die Ermittlungen deutlich schwieriger: mit fremder Hardware im Reich des IT-Experten. Dieser wollte an seinem Urlaubstag übrigens pflichtbewusst einen wichtigen Server aktualisieren. Erste Diagnosen unter Auswertung des gesamten externen und internen Datenverkehrs ergaben schnell einen ersten Befund: Der Upload lag regelmäßig für kürzere Zeiten bei fix 2 MBit/s, verursacht nahezu ausschließlich durch HTTP-Datenströme. Die 15 VoIP-Leitungen hatten daran nur einen sehr kleinen Anteil. Bei einer Standleitung mit synchron 2 MBit/s stand damit die wahre und zugleich simple Problemursache nach Wochen des Leidens schnell fest: eine durch Web-Downloads verstopfte Leitung.

Sabotage oder doch „nur“ technisches Problem?

Durch fehlendes Traffic-Shaping fehlte den empfindlichen VoIP-Verbindungen die verlässlich notwendige Bandbreite – gut zu erkennen in einer Wireshark-Visualisierung mit Gegenüberstellung des gesamten Datenverkehrs und des in Spitzenzeiten zwangsweise pendelnden VoIP-Traffics. Der daraufhin entlastete Administrator wurde endlich eingeweiht und zur weiteren Problemanalyse in die Gespräche und Untersuchungen einbezogen. Er hatte auch gleich eine Erklärung für die von der Geschäftsleitung pauschal geschilderten Performanceprobleme im

LAN. 20 bis 30 MByte große Excel-Dateien benötigen in einem 100-MBit-Netzwerk nun einmal einige Sekunden Übertragungszeit. Fall gelöst, Admin entlastet, Team wieder an einem Tisch.

Kein Hacker, nur ein Ressourcenfresser

Solche Fälle sind gar nicht so selten. In einer ähnlichen Situation litt ein mittelständisches Fertigungsunternehmen in der Automobilbranche seit Wochen unter einer extrem langsam arbeitenden IT-Infrastruktur. Man hatte beinahe alles schon versucht: Austausch von Kupferleitungen gegen Glasfaser zur Ausschaltung von Störungen durch eventuelle starke elektromagnetische Strahlung, den Einbau von 6 GByte RAM in einem 32 Bit-Serversystem und ganz besonders das Hin- und Herschieben der Verantwortung zwischen einem IT-Dienstleister für die Infrastruktur und einem anderen für das stark verzögert arbeitende ERP-System.

Letztendlich, so vermutete man, mussten wohl Hacker der Konkurrenz am Werk sein, die das Netzwerk sabotiert hatten. Die tatsächliche Ursache hingegen war eine über Wochen unbemerkt ausgefallene Battery Backup Unit des RAID-Controllers im Server. Der Controller schaltete seinen Cache ab, die Festplattenperformance ging in den Keller und damit auch die Verarbeitungsgeschwindigkeit der betagten und Disk-I/O-intensiven ERP-Software.

Nicht regelgerechter Fernzugriff: Bei einem weltweit tätigen Industrieunternehmen mit mehreren Tausend Clients und einigen Hundert Servern hatte eine aufmerksame IT-Mitarbeiterin zufällig entdeckt, dass der IT-Dienstleister eine bestimmte, nicht genehmigte Remote-Management-Software eingesetzt haben musste, da diese sich an einer Stelle nicht wieder sauber deinstalliert hatte. Da diese Software technisch die Möglichkeit bietet, Mitarbeiter und deren Daten so aus der Ferne zu überwachen, dass diese weder zustimmen müssen noch die Überwachung überhaupt bemerken, war die Geschäftsleitung in heller Aufregung, ein ausländischer Mitbewerber könnte dies gezielt einsetzen, um Geschäftsgeheimnisse zu entwenden.

Wenn Faulheit wie Spionage aussieht

Es wurden ausgewählte Clients bitgenau IT-forensisch gesichert sowie Registry-Einträge, Konfigurationseinstellungen und Logfiles auf Servern und Clients teilautomatisiert eingesammelt und durchgesehen. Es zeigte sich, dass diese Soft-

Checkliste zur Einschätzung der Gefährdung eines Unternehmens

– Zeigt die Geschäftsführung den erklärten Willen, für die Prävention Ressourcen (beispielsweise Personal) zur Verfügung zu stellen?

– Steht ein ausreichendes Budget für die Integration beziehungsweise planvolle Vorbereitung der Nutzung neuer Technologien zur Verfügung?

– Wurden Schutzbedarf und darauf beruhende Gefahren als Teil eines ganzheitlichen betrieblichen Kontinuitätsmanagements (BKM) analysiert?

– Wird die IT-Infrastruktur in Audits regelmäßig auf IT-Sicherheit, insbesondere konkrete Sicherheitslücken, überprüft? Sind dabei auch Angriffsvektoren durch Innentäter berücksichtigt?

– Besteht der Wille, erkannte Probleme im festgelegten Umfang zu beseitigen und darüber hinausgehende Präventivmaßnahmen zu ergreifen?

– Werden die Präventions- und Reaktionspläne getestet?

– Erhalten Administratoren und IT-Anwender regelmäßig Schulungen, damit sie Gefährdungspotenziale besser einschätzen und qualifizierter reagieren können?

– Wird eine aktive Sicherheitskultur gelebt und gefördert?

Je mehr Fragen mit „nein“ beantwortet werden, desto größer ist der Handlungsbedarf in Sachen Sicherheitskultur und desto weniger sind Unternehmen für Sicherheitsvorfälle und Angriffe auf ihre IT gerüstet.

ware auf zahlreichen Systemen eingesetzt worden war. Bei einer Festplatte eines Rechners, von dem aus Überwachungen stattgefunden hatten, konnten die Experten nur noch bestätigen, dass diese gerade datenschutzkonform vollständig durch Überschreiben mit Zufallsmuster gelöscht worden war. Auch fand man überflüssige administrative Freigaben gesamter Volumes für Windows-Rechner von Schlüsselpersonen. Letztlich jedoch konnte Entwarnung gegeben werden: Mehrere Administratoren hatten eine Software eingesetzt, die nicht den IT-Richtlinien entsprach, nicht datenschutzkonform und nicht lizenziert war. Und das alles nur, um sich die Arbeit ein wenig zu erleichtern. Der Verdacht auf Spionage erwies sich als unbegründet, ärgerlich und teuer war es trotzdem.

Datenklau mit USB-Sticks & Co.: Vergleichsweise häufig kommt es vor, dass Unternehmen den Verdacht äußern, vertrauliche Daten könnten abgeflossen sein. Es ist schwierig, aber je nach Rahmenbedingungen nicht unmöglich, den Nachweis über einen tatsächlichen Datenverlust zu führen. Mal verraten aus dem freien Speicher wiederherstellbare Teile aus Web-Mails, welche Informationen und Anhänge versendet wurden, mal gibt es Vorschaubilder oder Indexeinträge zu Daten auf ehemals angeschlossenen Datenträgern. Und manchmal helfen auch Namen und Zeitstempel zuletzt bearbeiteter oder angeschauter Dateien. Sicheren Schutz vor dem Herausschleusen von Daten aus Unternehmen bietet aber nur Software, die Datenträger und Datentransfers per Gruppenrichtlinie einschränkt sowie inhaltlich überwacht. Ihr Einsatz erfordert aber zwingend, dass rechtliche Fragen der Mitarbeiterüberwachung geklärt sind.

Datenklau mit kreativen Methoden

Im folgenden Fall war durch geschickte Analysen nachvollziehbar, wie Daten das Unternehmen verlassen hatten, obwohl der verdächtigte Mitarbeiter besonders kreativ bei der Methode des Datendiebstahls war. Das Unternehmen hatte die USB-Ports gesperrt und die Nutzung externer Datenträger verboten. Der Mitarbeiter jedoch kopierte die Daten über seinen Dienst-PC vom Server auf sein an seinen Dienst-PC über Cradle angeschlossenes digitales Diktiergerät und konnte sie zu Hause auf seinen PC übertragen. Die Windows-Registry und die Auswertung von MRU-Listen des Dienst-PCs belegte den Kopiervorgang vertraulicher Daten auf das Gerät, auf dem sich normalerweise nur Sprachnotizen befinden. Der Arbeitgeber stellte das Diktiergerät sicher und beauftragte eine forensische Analyse. Mittels Carving waren umfängliche vertrauliche Daten wiederherstellbar und der Fall gelöst.

Bei der nachträglichen Betrachtung von Sicherheitsvorfällen zeigt sich, wie unterschiedlich die Betroffenen die Gefährdungslage einschätzen und ihre Prioritäten setzen. Danach bemisst sich der Aufwand, mit dem sie die Aufklärung und Aufarbeitung des jeweiligen Falles betreiben. So herrscht etwa bei einigen Unternehmen noch immer die Auffassung, die eigene Webseite (inklusive Webanwendungen) sei eine bessere Litfaßsäule oder eine Art „Graffiti“ und könne leicht wieder „übermalt“ werden.

Nicht selten gibt es auch den Fall, dass selbst Unternehmen mit erhöhtem Schutzbedarf zwar eine Trennung zwischen internem und externem Netz beispielsweise durch Firewalls vollziehen, dann aber keine weitere oder nur eine unvollständige Separierung mehr im internen Netz durchführen. Eindringlinge und ganz besonders Innentäter können so relativ frei in einem einmal kompromittierten Netz agieren, die Aufklärung wird durch fehlende zentrale Knotenpunkte erschwert.

Es zeigt sich aber auch, dass Organisationen, die früh und konsequent gemein-

Glossar

File Carving: Toolgestütztes Wiederherstellen von Dateien ohne Zugriff auf das Dateisystem anhand von Signaturen.

Google Dorks: Spezielle Suchanfragen, mit denen man via Google-Suche (oder mit anderen Suchmaschinen) unsichere PHP-Installationen, Informationslecks und vieles mehr auf Webservern finden kann.

Local-File-Inclusion-Schwachstelle: Schwachstelle, die darauf beruht, dass Benutzereingaben nicht geprüft werden und ein Angreifer über manipulierte Eingaben beliebig oft Dateien auf dem Server einbinden und anzeigen lassen kann.

Pentest/Penetrationstest: Von beauftragten Sicherheitsexperten gezielt durchgeführte Einbruchstests in Systeme, um potenzielle Sicherheitslücken und Schwachstellen zu entdecken.

Screen-Scraper: Werkzeuge, mit denen man gezielt Bildschirminhalte auslesen und maschinell weiterverarbeiten kann. Bei Webseiten versteht man unter Web Scraping zum Beispiel das Extrahieren von beispielsweise Formulardaten.

sam mit eigenen „allgemeinen“ IT-Experten und externen Sicherheitsdienstleistern oder der eigenen Sicherheitsabteilung einen Untersuchungsplan entwickeln und diesen umsetzen, schneller zu Ergebnissen und einer Aufklärung der unangenehmen Lage gelangen. Diesen Fällen gemeinsam ist oft der hilfreiche Input der eigenen IT-Administratoren, denn sie haben die größte Erfahrung mit der im Unternehmen eingesetzten Technik. Zwar verläuft jeder Sicherheitsvorfall anders, das grobe Raster der Vorgehensweise bleibt jedoch gleich (Abb. 4).

Vermeidbare Hürden bei der Aufklärung

Selbstverständlich gibt es viele große wie kleine Unternehmen mit adäquaten Sicherheitsmaßnahmen und vorbildlicher Störfallreaktion. Was aber, wenn die IT-Systeme selbst „kugelsicher“ sind, externe und nur flüchtig bekannte Besucher sich jedoch frei und unbeaufsichtigt im Gebäude bewegen können oder sämtliche Mitarbeiter unkontrollierten Zutritt in alle IT-Räume haben? Denn Informationssicherheit umfasst nicht nur die IT selbst, sondern auch alle im Umfeld beteiligten Systeme, Prozesse und Menschen.

Aus der Sicht derjenigen, die die Sicherheitsvorfälle analysieren sollen, ergeben sich oft ähnliche Herausforderungen bei der Untersuchung und Aufarbeitung. Berücksichtigt man einige Faktoren jedoch schon im Vorfeld, lassen sich manche Vorfälle schneller aufklären.

In vielen IT-Umgebungen ist das Administratorpasswort für alle Systeme identisch und wird zudem selten oder nie geändert. IT-Richtlinien, dass Passwörter komplex sein müssen, man sie regelmäßig ändern muss und nicht weitergegeben darf, werden in der Praxis vielfach nicht umgesetzt oder umgangen. Dann ist es schwierig oder sogar unmöglich, festzustellen, welcher Administrator welche Aktionen ausgeführt hat oder ob es ein externer Angreifer war.

Fälle, in denen der Administrator selbst im Fokus steht, gestalten sich oft besonders anspruchsvoll, da Administratoren aus gutem Grund zum einen eine besondere Vertrauensrolle innehaben und zum anderen etwaige Untersuchungs- oder Gegenmaßnahmen schnell erkennen und enttarnen können. Hier ist ein besonders geschicktes Vorgehen mit gründlicher Vorbereitung und Fingerspitzengefühl nötig sowie gelegentlich verdeckte Vorgehensweisen.

Auch erschweren immer wieder unklare und unvollständige Dokumentationen der Betroffenen das Nachvollziehen relevanter Vorgänge. Besonders problematisch ist jedoch, dass verstärkt kleinere und mittelständische Unternehmen bei Sicherheitsvorfällen zu lange mit dem Beauftragen von Fachleuten warten und zunächst eigene, nicht immer ausreichend qualifizierte Analyse- und Gegenmaßnahmen ausprobieren. Dabei kann es zur Zerstörung oder Veränderung von Datenbeständen kommen, die als Beweismittel eine wichtige Rolle spielen.

Aufgrund des Integrationsbedarfs neuer Endgeräte und IT-Systeme, die in den letzten Jahren zunehmend in Unternehmen Eingang gefunden haben, ist der Schutzbedarf noch weiter angestiegen. Die Erfahrungen und die voran skizzierten Fälle zeigen, dass die neuen Systeme in Sicherheitserwägungen vielfach nicht ausreichend berücksichtigt werden – nicht zuletzt aufgrund der gestiegenen Komplexität der Einzelprodukte. Gelegentlich führen selbst triviale Probleme zu kritischen Situationen, die meist aber vermeidbar gewesen wären. Deshalb ist bei Sicherheitsvorfällen im Mittelstand verstärkt festzustellen, dass ähnliche Ursachen und Reaktionsmuster die Entstehung von Sicherheitsvorfällen begünstigen. Die Fragen im Kasten „Checkliste…“ liefern eine erste Einschätzung, wie es um die Sicherheitskultur bestellt und das Unternehmen in Ernstfall vorbereitet ist.

Lessons learned und was zu tun bleibt

Jeder Sicherheitsvorfall liefert, unabhängig von seinem Ausgang für die Betroffenen sowie die beteiligten IT-Experten, wertvolle Erfahrungen und Erkenntnisse zur Vermeidung oder wenigstens zur Aufklärung zukünftiger Fälle. Als IT-Sicherheitsberater, Pentester oder Auditor mag zwar das Wissen in den Bereichen Sicherheit und Forensik besonders ausgeprägt sein. Kaum jemand verfügt jedoch über jahrelange Erfahrung in der Administration aller am Markt erhältlicher IT-Systeme. Die enge Zusammenarbeit mit Betroffenen ist daher meist nötig und sinnvoll, insbesondere auch, um die notwendigen Ressourcen und Informationen zu erhalten. Das Einbeziehen von IT-Administratoren ist manchmal sogar die einzige Möglichkeit, um effizient zu einer Klärung eines Vorfalls zu gelangen – vorausgesetzt, der Administrator war nicht selbst der Schuldige.

Als IT-Sicherheitsvorfälle eingestufte Ereignisse müssen stets gründlich untersucht werden. Nicht immer, aber gelegentlich sind spektakuläre Hacks oder kriminelle Energie die Ursache. Weitaus häufiger sind menschliche oder technische Fehler wie Nachlässigkeit, mangelnde Erfahrung, Arroganz, Versehen, Zeitnot oder Designfehler die wahre Ursache des Übels. Letztlich hilft rechtzeitiges Vorbeugen noch immer am besten. Das braucht aber Überzeugungskraft und Budget, um eine umfassende Sicherheitskultur einzuführen. Insbesondere gewachsene Infrastrukturen bergen die größten Risiken, da Unternehmen sich häufig unbemerkt in eine digitale Sackgasse gefahren haben, die sie nur mit einem großen finanziellen Kraftakt verlassen können. Ohne Administratoren oder IT-Beauftragte unter Pauschalverdacht zu stellen: Vertrauen ist gut und notwendig, vorausschauende Prävention und eine regelmäßige Überprüfung auf die Einhaltung von Regeln ist aber gleichermaßen bei allen erforderlich. (ur)

Martin Wundram

ist von der IHK zu Köln öffentlich bestellter und vereidigter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung.

Markus Loyen

ist Geschäftsführer der CORIFOR GmbH & Co. KG und berät rund um die Themen IT-Sicherheit und -Forensik.

Alexander Sigel

ist Geschäftsführer der DigiTrace GmbH und als Berater und Sachverständiger für IT-Forensik tätig.

Literatur

[1] Martin Wundram, Alexander Sigel; Mit Suchmaschinen-Hacks gravierende Informationslecks aufdecken: Fünf aktuelle Fälle, in: Hakin9 – IT Security Magazin, 07/2011, S. 42 – 45

[2] Martin Wundram, Alexander Sigel; Praktisches Pentesting von Multifunktionsdruckern mit SHODAN und PRAEDA, in: Hakin9 – IT Security Magazin; 09/2011, S. 23 – 29

[3] René Keller, Jörn Wagner, Martin Wundram; Webapplikationssicherheit; Abgedichtet; Webanwendungen vor Missbrauch schützen; *iX* 2/2010, S. 52