Red Teaming: Taktische Informationsbeschaffung

Gesammeltes Wissen

Sascha Herzog

Das A und O bei Sicherheitstests ist es, im Vorfeld Informationen über das anzugreifende Ziel zu sammeln. Nur so kann man potenzielle Angriffe nachvollziehen und erschweren.

Das Thema des „Tactical Information Gathering“ wurde im letzten Artikel [1] ja bereits angeschnitten und mit einigen Beispielen hinterlegt. Hier wollen wir nun etwas tiefer in die Materie einsteigen und den Lesern ein paar Tools und Techniken vorstellen.

Die taktische Informationsbeschaffung hat zum Ziel, so viele relevante Informationen wie möglich für Angriffe in einem „Red Team Assessment“ über ein Zielunternehmen in Erfahrung zu bringen, um eine hohe Effizienz für die folgenden Attacken zu erreichen.

Die Informationsbeschaffung befasst sich meist mit Daten aus den Bereichen IT- und OT-Infrastruktur (Operational Technology; Sensorik und Maschinenintelligenz in Produktionssystemen sowie kritischen Infrastrukturen), von Mitarbeitern, Partnern und Dienstleistern, zur physischen Infrastruktur sowie zu Geschäftsprozessen und zur Businesslogik (dieser und alle weiteren Links zum Artikel sind über ix.de/ix1804092 zu finden). Zu diesem Zweck sollten mindestens Antworten auf die im Kasten „Hilfreiche Fragen …“ aufgelisteten Fragen gefunden werden.

Um die Thematik besser nachvollziehen zu können, soll hier wieder ein anonymes Beispiel aus einem unserer Red-Team-Projekte skizziert werden. Es soll die Möglichkeiten demonstrieren, die Angreifer durch eine professionelle Informationsbeschaffung erhalten. Unternehmen können so erkennen, welche relevanten Informationen über sie in öffentlichen Quellen zu finden sind, und die Angriffsmöglichkeiten stark einschränken.

Über die „Schatten-IT“ ins System eindringen

Für eine europäische Bank sollten wir möglichst vollumfänglich im Zuge eines Red-Team-Projekts rein auf Systemebene relevante Informationen für Angriffe sammeln. Nachdem wir die IKT-Systeme aller Tochtergesellschaften und Beteiligungen identifiziert hatten, wollten wir nun Schatten-IT-Systeme ausfindig machen. Diese Systeme, die zwar in irgendeiner Form

Hilfreiche Fragen bei der Informationsbeschaffung

- Welche Tochterunternehmen und Beteiligungen besitzt das Ziel?
- Welche aus dem Internet erreichbaren Systeme des Ziels können identifiziert werden (insbesondere Schatten-IT-Systeme)?
- Enthalten diese Systeme Schwachstellen, die für die weitere Informationsbeschaffung oder eine direkte Kompromittierung des Systems verwendet werden können?
- Welche dieser Systeme bieten Login-Möglichkeiten (HTTP-Formulare, FTP, SSH etc.) und verwenden keine Transportverschlüsselung?
- Tauchen identifizierte Systeme in Blacklists oder Threat-Intelligence-Datenbanken auf?
- Welche noch nicht registrierten Domains eignen sich für spätere (Spear-)Phishing-Angriffe?
- Welche Sicherheitstechnologien (Proxies, Firewalls, Endpoint-Protection etc.) werden eingesetzt?
- Welche Software (Betriebssystem, Browser, CRM etc.) setzen die Mitarbeiter ein?
- Wer sind die technischen Dienstleister des Ziels im Bereich Software, Hardware und Infrastruktur?
- Gibt es zu Mitarbeitern/Partnern/Dienstleistern bekannte Datenpannen, sogenannte Data Breaches?
- Haben Mitarbeiter/Partner/Dienstleister (un)bewusst interne Daten (Konfigurationen, technische Beschreibungen, Kundendaten, Sourcecodes, Passwörter etc.) geleakt?
- Welche Mitarbeiter eignen sich aufgrund ihrer Stellung im Unternehmen oder ihres psychologischen Profils besonders gut als Angriffsziel für Social-Engineering-Attacken?
- Lassen sich Kartendaten zu Standorten, Betriebsgelände und Gebäuden beschaffen, um Zugangsmöglichkeiten zu identifizieren?
- Gab es relevante Pressemeldungen (zum Beispiel: Ziel war im großen Stil von „NotPetya“ betroffen) oder öffentliche Skandale das Ziel betreffend?
- Was sind die Key-Assets, Flagship-Produkte und forcierten Strategien und Partnerschaften des Ziels?

zum Zielunternehmen gehören, jedoch der eigenen IT-Abteilung meist unbekannt oder zumindest nicht Teil des internen IT-Service-Managements sind, bieten Angreifern oft eine lohnenswerte Angriffsfläche.

Dies können Webserver sein, die für Kampagnen schnell von einer Werbeagentur extern aufgesetzt wurden und einen Hostname aus der unternehmenseigenen Domain erhalten haben (zum Beispiel *kampagne.company.tld*), mittels statischer IP-Adressen eines Internetproviders angebundene Steueranlagen (Industrial Control Systems; ICS) oder Hosts, die von unachtsamen Technikern mittels DynDNS-Zuweisung über dynamische IP-Adressen angebundenen wurden und einen Netzwerkübergang ins interne Firmennetz ermöglichen.

Über Google lassen sich häufig hilfreiche technische Dokumente finden (Abb. 1).

In unserem Fall fanden wir über eine Google-Suche (Abbildung 1) viele technische Dokumente über eingesetzte Software, Netzwerke und technische Konzepte eines Serviceproviders der Bank, worunter sich auch eine interne Präsentation über die Überwachungsmaßnahmen für die Bank befand.

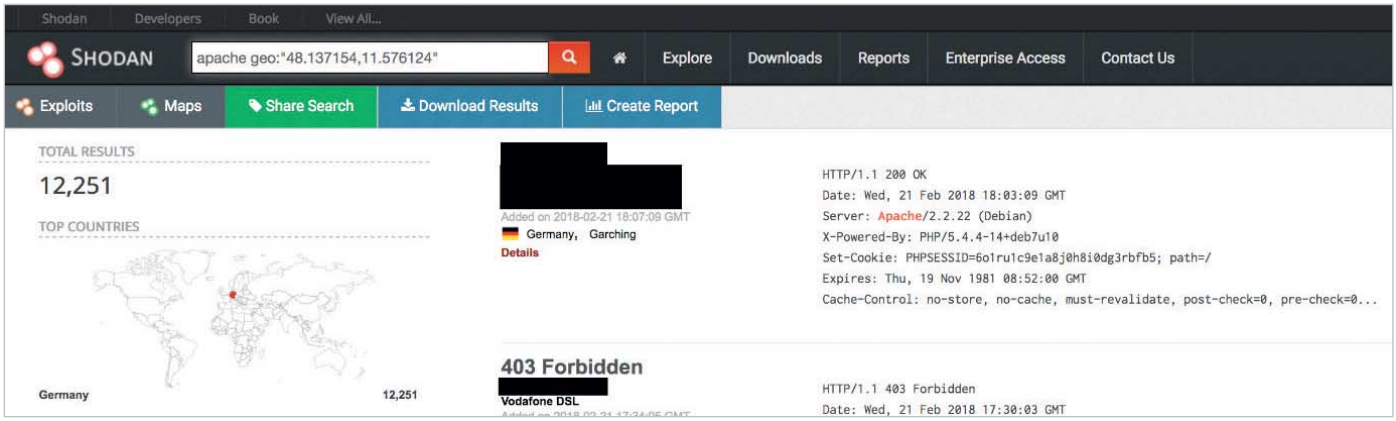
In diesem Dokument beschrieben die technischen Dienstleister sehr ausführlich, welche Videoüberwachungssysteme sie in diversen Filialen verbaut hatten. Nachdem wir uns einen Tag tiefer gehend mit dem Videoüberwachungssystem und

```
      timeout = setTimeout( live1,  100 );


live1()

document.getElementById( 'thePic' ).onload = wait1;
document.getElementById( 'thePic' ).src = "http://19[redacted]/picture.jpg?name=admin&passwd=[redacted]cam=5&index=0&width=" + document.getElementById( 'thePic' ).
new Date().getTime();
```

Auch Glück gehört bisweilen dazu: Passwörter im Klartext sparen Sicherheitstestern viel Arbeit – Angreifern allerdings auch (Abb. 2).



Suchmaschinen wie Shodan erlauben die Suche nach geografischen Standorten, eine Fundgrube für Angreifer (Abb. 3).

seinen Komponenten auseinandergesetzt und jedes online verfügbare Handbuch dazu gelesen hatten, konnten wir uns Google-, Shodan- und Censys-Dorks erstellen – also spezielle fortgeschrittene Abfragen – und eben solche Systeme im Internet ausfindig machen.

Glückstreffer: Passwort im Klartext

Bevor wir uns die Mühe machten, ein solches System selbst zu kaufen und die Firmware der Komponenten per Reverse Engineering zu rekonstruieren, um Schwachstellen darin aufzuspüren, suchten wir erst mal nach einfach zu findenden Bugs in online zugänglichen Systemen. In diesem Fall hatten wir tatsächlich sehr großes Glück und fanden im JavaScript-Code einer noch vor der Authentifizierung eingebundenen Datei den Admin-Usernamen und das Passwort im Klartext (Abbildung 2).

Eine ungeschickte Konfiguration der Systeme erlaubt auch Zugriffe auf versteckte Kameras, was normalerweise dem Sicherheitspersonal vorbehalten sein sollte (Abb. 4).

Dieser epochale Fehler des Videoüberwachungsherstellers sparte sicher zwei bis fünf Tage Reverse Engineering. Gewappnet mit dieser kleinen, aber sehr feinen Waffe, suchten wir die Geokoordinaten aller Bankfilialen heraus und glichen sie mit unseren Shodan-Dorks ab. In Shodan lässt sich einfach im Umkreis von Geokoordinaten suchen, was natürlich für solche Angriffe sehr vorteilhaft ist. Die Suche in Abbildung 3 zeigt zum Beispiel Apache-Server im Umkreis Münchens.

Auch hierbei hatten wir wieder Glück und konnten vier Videoüberwachungssysteme von Filialen der betreffenden Bank identifizieren, wovon eine sogar das im Handbuch beschriebene Standardpasswort für die Anmeldung verwendete. Nachdem wir unseren Kunden informiert hatten und die IP-Adressen der Systeme als statische Provider-IPs des Kunden nachverfolgen konnten, durften wir auf die Systeme zugreifen und weitere koordinierte Aktionen ausführen.

Der Videocontroller hatte nicht nur normale Überwachungskameras angeschlossen, sondern auch die versteckten Kameras der Geldautomaten in den Filialen, was es uns ermöglicht hätte, Bankkunden beim Geldabheben zu beobachten (Abbildung 4).

In der Weboberfläche der Videocontroller fanden sich weitere Benutzer und Passwörter des Dienstleisters im Klartext, die wir für weitere Systeme im späteren Verlauf des Red-Team-Assessments nutzen konnten. Wir konnten zeigen, dass die Controller Verbindungen in das interne Banknetz hatten, womit sie sich natürlich als Sprungpunkt für Lateral-Movement-Aktionen eigneten. Verständlicherweise wollte der Kunde die angreifbaren Überwachungssysteme schnellstmöglich vom Netz nehmen.

In den folgenden Artikeln unserer Red-Team-Serie beleuchten wir die weiteren Phasen der Assessments und versuchen jedes Mal kurz auf die taktische Informationsbeschaffung einzugehen, die nötig war, um diese Angriffe elaboriert durchführen zu können. (ur@ix.de)

Sascha Herzog

ist technischer Geschäftsführer und Penetrationstester bei der NSIDE ATTACK LOGIC GmbH in München.

Literatur

[1] Sascha Herzog; Awareness; Mit allen Mitteln; Sicherheitstests: Angriffe auf Technik und Mensch; *iX* 2/2018, S. 78

Alle Links: ix.de/ix1804092