)SCIP(MONTHLY SECURITY SUMMARY

Ausgabe Oktober 2018

Bildquelle: https://pixabay.com/photo-3610779/

FOKUS

ANGRIFFE AUF WINDOWS ACCOUNTS

Oktober 2018: Updates und „Updates“

Es ist nicht so lange her, da hat *HP* mittels eines *Firmware Upgrades* verhindert, dass Endnutzer auf Druckern des Herstellers günstigere *Tinten-Refills von Drittanbietern* nutzen können. Ein Schachzug, der sich lohnt: Gerade günstigere Drucker-Modelle werfen oftmals nur wenig Gewinn ab, so dass der Verkauf von Zubehörartikeln strategisch wertvoll ist. Seit einigen Tagen beschäftigt sich der *Attorney General* des US-Bundesstaates *Texas* mit einem ähnlichen Fall: Ein Konsument hatte herausgefunden, dass *Epson* auf den Zug aufgesprungen ist und ebenfalls Updates, die zusätzliche *Einschränkungen* implementieren, für seine Drucker verteilt.

Störend an beiden Geschichten ist, dass die Hersteller diese Restriktionen gegenüber ihren Kunden als *Sicherheitsupdates* getarnt haben. Das ist zum einen *irreführend* und, so muss man doch offen gestehen, etwas *hinterhältig*. Auf einer ganz anderen Ebene zementieren sie damit aber ein gefährliches Verhalten: Eine *Skepsis* und *Vorsicht* gegenüber neuen Sicherheitsupdates, gerade für Hardware-Komponenten.

Vor allem in Zeiten immer höherer Verbreitung für IoT-Geräte erweisen Hersteller wie *HP* und *Epson* der gesamten Technologiebranche hier einen Bärendienst. Und riskieren ultimativ, dass Konsumenten sich nach *ehrlicheren* Anbietern umsehen.

Stefan Friedli
Head of Auditing

Bildquelle: https://flic.kr/p/8Nmx6h

scip AG
Badenerstrasse 623
8048 Zürich
Switzerland

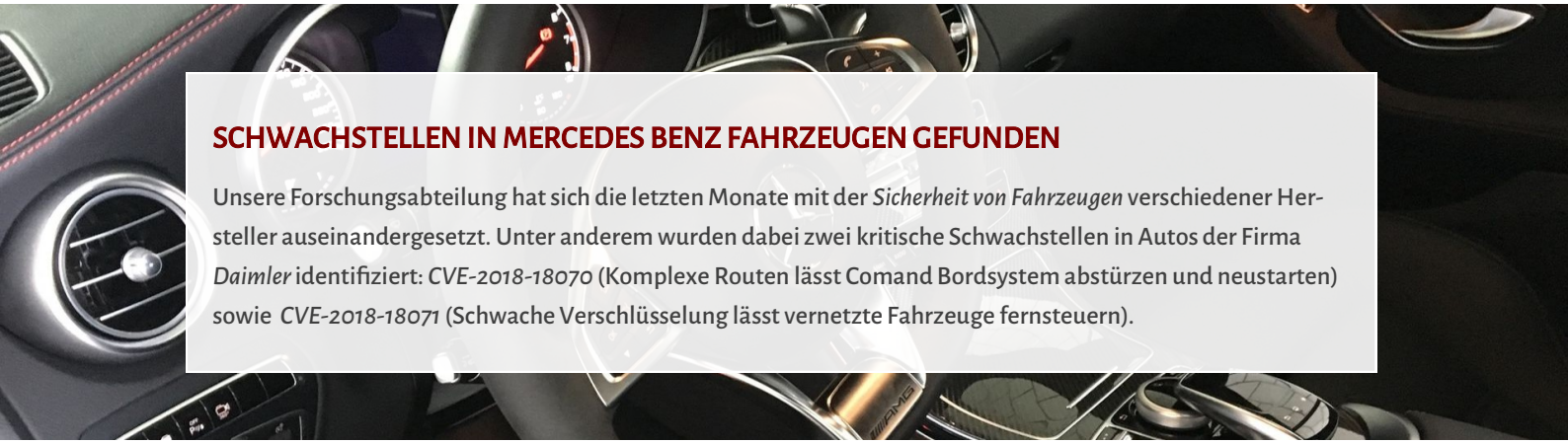
+41 44 404 13 13
info@scip.ch
https://www.scip.ch

NEWS

WAS IST BEI UNS PASSIERT?

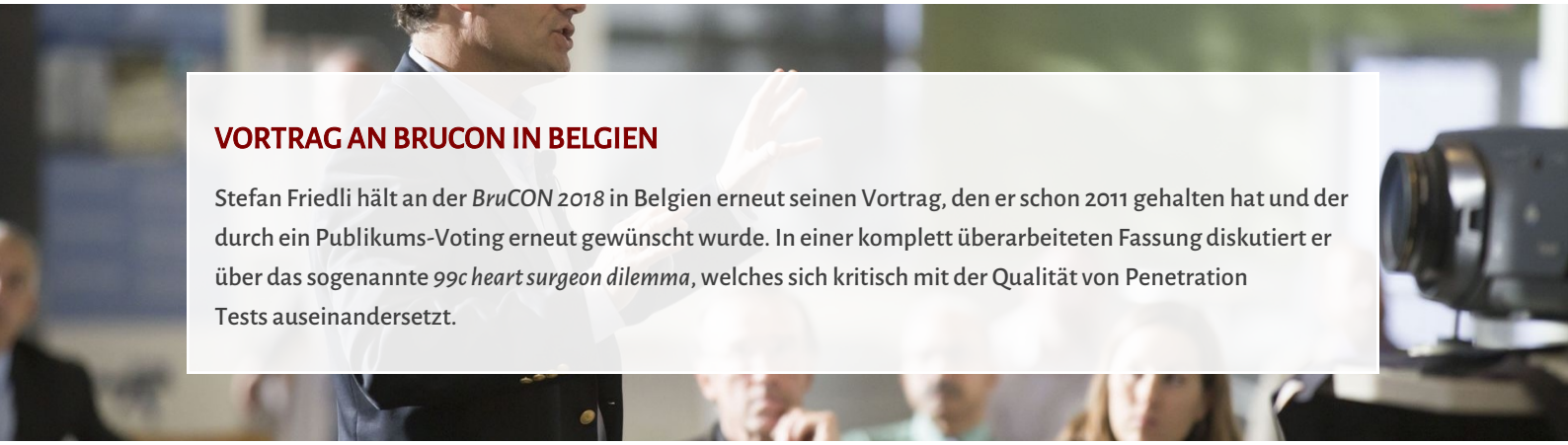
KEYNOTE ZU SICHERHEIT IM GESUNDHEITSBEREICH

Vom 23. bis 26. Oktober 2018 findet in Zürich die *IFAS 2018* statt. An der *Fachmesse für den Gesundheitsmarkt* zeigen über 330 Aussteller Neuheiten der Branche, vom drahtlosen Touch EKG über die smarte Datenerfassung bis hin zur Tennisarmbandage. Die Messe wird mit der *Keynote von Marc Ruef* eröffnet, der darüber diskutiert, welche Angriffsmöglichkeiten die Digitalisierung im Gesundheitsbereich mitbringen kann.



SCHWACHSTELLEN IN MERCEDES BENZ FAHRZEUGEN GEFUNDEN

Unsere Forschungsabteilung hat sich die letzten Monate mit der *Sicherheit von Fahrzeugen* verschiedener Hersteller auseinandergesetzt. Unter anderem wurden dabei zwei kritische Schwachstellen in Autos der Firma *Daimler* identifiziert: *CVE-2018-18070* (Komplexe Routen lässt Comand Bordsystem abstürzen und neustarten) sowie *CVE-2018-18071* (Schwache Verschlüsselung lässt vernetzte Fahrzeuge fernsteuern).



VORTRAG AN BRUCON IN BELGIEN

Stefan Friedli hält an der *BruCON 2018* in Belgien erneut seinen Vortrag, den er schon 2011 gehalten hat und der durch ein Publikums-Voting erneut gewünscht wurde. In einer komplett überarbeiteten Fassung diskutiert er über das sogenannte *99c heart surgeon dilemma*, welches sich kritisch mit der Qualität von Penetration Tests auseinandersetzt.

Weitere News zu unserer Firma finden Sie auf unserer Webseite.

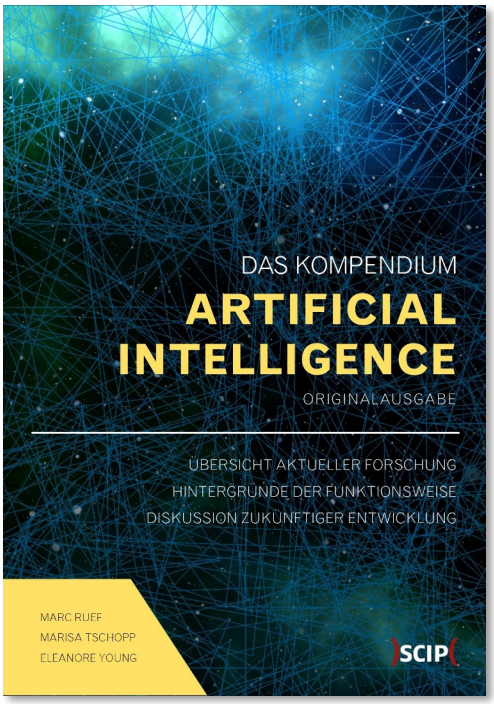
GEWINNSPIEL

UNSER NEUES BUCH ZU KÜNSTLICHER INTELLIGENZ

Unsere Sicherheits- und Technologie-Experten überzeugen seit jeher mit dem *Labs Buch*, das einmal jährlich erscheint und eine Auswahl unserer Fachartikel der vergangenen zwölf Monate zusammenfasst. Diese regelmässige Publikation wird nun um eine themenbezogene Buchreihe ergänzt. Der erste Titel setzt sich mit dem Thema *Künstliche Intelligenz* auseinander. Dabei werden organisatorische, technische und gesellschaftliche Aspekte diskutiert. Das eBook kann auf Amazon erworben werden und steht sowohl Deutsch als auch Englisch zur Verfügung.

Machen Sie mit bei unserem Gewinnspiel und gewinnen Sie ein Exemplar des eBooks. Ganz einfach: Retweeten Sie unseren Tweet , liken Sie unser Instagram-Foto , teilen Sie unseren Facebook-Post oder den Google+ Post. Teilnahmeschluss ist der 24.09.2018. Die Gewinner werden persönlich informiert .

Weitere Informationen auf unserer Webseite.



ISBN 978-3-907109-14-4 [de]
ISBN 978-3-907109-15-1 [en]

HERAUSFORDERUNGEN LIEGEN VOR UNS

Bildquelle: https://pixabay.com/photo-2080138/

DOMINIK ALTERMATT

PRIVILEGIERTE WINDOWS ACCOUNTS DIE KONKRETE GEFAHR

Privilegierte Accounts sind als kritisch zu betrachtende Komponente einer IT-Infrastruktur anzusehen. Wer sich nicht mit den eminenten Risiken des Themas beschäftigt und seine privilegierten Windows Accounts, wie zum Beispiel Domain Administratoren, nicht adäquat schützt, exponiert seine Infrastruktur den wachsenden Bedrohungen von Cybercrime. Die Praxis zeigt, dass fahrlässiges Verhalten doch immer wieder anzutreffen ist. Sind gerade hoch privilegierte Accounts exponiert, reicht es oft schon aus, dass ein Angreifer den "richtigen" Client kompromittiert, um die Kontrolle über eine komplette Infrastruktur zu erlangen.

Privilegierte Accounts zu schützen ist in der Theorie nicht kompliziert, einige wenige Prinzipen sind zu beachten. In der Praxis sind dann doch viele unterschiedliche Faktoren mit einzubeziehen, um adäquates Handling und Management sicherzustellen. Dabei gibt es einige ganz praktische Massnahmen, welche gewisse Risiken minimieren, die sehr schnell und einfach implementiert werden können. In diesem Artikel sollen eben solche aber auch tiefgreifenderen Konzepte vorgestellt werden.

EXPONIERTE PRIVILEGIERTE ACCOUNTS

Wann sind privilegierte Accounts exponiert? Eine Art dies einfach zu erklären wäre: umso "näher" ein privilegierter Account dem Internet ist, umso exponierter ist er. Also mit Domain-Administrator-Rechten auf einem Standard-Client einzuloggen exponiert diesen Account. Die Sicht eines Angriffes ist meist auch von aussen nach innen, also zum Beispiel:

- Angriff von Internet auf einen Client
- Angriff von einem Client auf einen Server
- Angriff von einem Server auf einen sensitiven Server (zum Beispiel Domain Controller, Datenbanken)

Eine gängige Annahme in der IT-Security ist, dass stehts von einem kompromittierten Client ausgegangen werden muss. Folgend eine grobe Beschreibung von möglichen Aktionen eines Angreifers:

1. Zugriff auf ein System mittels Infizierung durch Schadsoftware (Social Engineering, Spear-Phishing) oder direkten physischen Zugriff (z.B. internen/externe Mitarbeiter), meist mit nicht-privilegierten Benutzer

2. Privilege Escalation zu lokalen Administrator-Rechten mittels Ausnutzen von Schwachstellen oder anderen Techniken

3. Beschaffung von NTML Hashes, respektive Auslesen der Hashes der auf dem System eingeloggten Benutzen (Mimikatz, responder.py, Network Sniffing z.B. mit ettercap)

4. Lateral Movement mit den zusammengetragenen Hashes oder Tickets (Pass the Hash oder Pass-the-Ticket, etc.) um Zugriff auf weitere Systeme zu erlangen (Bloodhound)

5. Wiederholen von Schritt 3 & 4 bis für das Angriffsziel geeignete Rechte im Netzwerk erlangt werden konnten

6. Zugriff auf das Zielsystem (z.B. Zahlungsserver) und Ausführen bösartiger Aktionen (z.B. betrügerische Zahlung ausführen)

Obige beschrieben Punkte können sehr langsam von statten gehen. Angreifer müssen vorsichtig und “lautlos” vorgehen, um eine allfällige Detektion zu verhindern. Für Schritt 1-5 des Angriffspfads können gut mehrere Monate aufgewendet werden.

Folgend einige Beispiele von exponierten privilegierten Accounts aus der Praxis:

- Sind öffentliche zugängliche Systeme vorhanden, z.B. ein Internet-PC in einem Hotel, lassen sich darauf schon mal in einem *unattended.txt* Domain Administrator Credentials finden

- Hat der Benutzer des infizierten Systems bereits lokale Administrator Rechte, können die NTLM Hashes ohne Privilege Eskalation ausgelesen werden (Entwickler, Superuser)

- Im Besten Falle für den Angreifer hat der eingeloggte Benutzer gleich Domain Admin Rechte (IT Administratoren, "Superuser")

- Es existieren "Service Principal Names" für persönliche Benutzer mit Domain-Administrator Rechten, welche mit Kerberoasting Attacken angegriffen werden können

- Standard Benutzer mit defacto Domain-Administrator Rechten durch verschachtelte AD-Gruppen. Dazu muss nicht eine *Member Of* Beziehung vorhanden sein, sondern auch Beziehungen wie *GenericAll* oder *AddMember*.

DEFENSIVE TECHNIKEN

Folgend nun einige Konzepte und Praktiken, die als Startpunkt oder Inspiration zur Sicherung der eigenen privilegierten Accounts dienen.

Mit privilegierten Accounts sind nicht nur Administratoren und Domain-Administratoren gemeint. Dazu gehören viele der Service Benutzer sowie Standard Accounts mit Zugriff auf sensitive Daten (Geschäftsleitung und Management, Finanzabteilungen, etc.).

Prozesse und interne Weisungen

Folgende Prinzipen und Konzepte sollten sich in den Security Policies für Identify and Access Management (IAM) grundsätzlich und Privileged Account Management (PAM) im Spezifischen wiederfinden:

- Kennen Sie Ihre Daten und Ihre Benutzer (Datenklassifikationen und Benutzerkonzepte)
- Least-Privilege Prinzip
- Segregation of Duties Prinzip
- Multi-Faktor Authentication für alle privilegierten Zugriffe
- Starke Passwort Policy (z.B. für Benutzer mit Domain-Administrator-Rechten 24+ Zeichen)
- Aufzeichnen der Aktivitäten von privilegierten Benutzer (Session Recording und Logging)
- Verbot der Nutzung von einem privilegierten Account durch mehrere Benutzer (Account Sharing)
- Verschärfte Audit-Prozesse von privilegierten Accounts
- Automatisierte IAM-Prozesse (löschen/ deaktivieren von privilegierten Accounts, wenn Mitarbeiter austritt, Abt. wechselt, Zugriff nicht mehr benötigt, etc.)
- Vermeiden von hardcodierten Passwörtern in Applikationen
- Privilegierte Zugriffe durch externen Partner nicht vergessen

Wer einen umgänglichen Anforderungskatalog für seine Security Policies bezüglich Access Management sucht, kann sich bei den Access Controls AC2, AC3, AC5 und AC6 aus dem Katalog des NIST Cybersecurity Framework bedienen.

Sind interne Weisungen und Policies vorhandenen, müssen diese auch um- und durchgesetzt werden können, ansonsten existiert die "Sicherheit" nur auf dem Papier. Daher gehören auch Prozesse zur Durchsetzung und Kontrolle der Weisungen wie auch Ressourcen für die Implementation und Betrieb stets dazu.

Unangenehm aber nötig ist die Definition über die Handhabung bei Verstössen gegen die Weisung. Es kommt vor, dass sich der eine oder andere IT-Mitarbeiter über die Jahre an Domain-Administrator -Rechte seines normalen Accounts gewöhnt hat und diese nicht gerne abgeben bez. nicht mit mehreren Accounts arbeiten möchte. Nichts destotrotz wird mit den "alten Gewohnheiten" das Risiko respektive die Exponierung von privilegierten Accounts teilweise massiv erhöht.

Windows Active Directory

Microsoft bietet eine umfassende und praktische Dokumentation mit dem Titel Best Practices for Securing Active Directory an. Darin finden sich diverse Kapitel, welche sich mit der Sicherung von Accounts und privilegierten Accounts beschäftigen.

Unter anderen sind folgende Themen aus den Microsoft-Unterlagen spannend:

- **Privileged Access Management Lösung (PAM) in AD DS**: Tool rund um das Management von privilegiertem Access; Risikominimierung von Pass-the-Hash; Isolation und Scoping von Privilegien; Multi-Faktor Authetication.

- **Just Enough Administration**: PowerShell Tool um die Anzahl von privilegierten Accounts zu minimieren; Erlaubt spezifische administrative Arbeiten (welche mit PowerShell erledigt werden können) ohne privilegierten Account.

Da die Dokumentation von Microsoft sehr umfangreich und weitreichend ist, anbei einige wenige Punkte, die gleich Umgesetzt werde können (Quickwins). In späteren Umsetzungsphasen können den obigen verlinkten Anleitungen von Microsoft im Detail umgesetzt werden.

Konsequente Einhaltung der Prozesse

- Prozess zur Review der Administratoren Gruppen im AD und lokal auf den Clients/Servern etablieren. Meist sind da zu viele Benutzer drin, welche die hohen Rechte nur temporär oder aus Bequemlichkeit "benötigen". Diese konsequent und regelmässig entfernen. Hierbei auch die Verschachtlung von Gruppen beachten.

- Tägliche Arbeiten auf Clients stets ohne privilegierte Accounts verrichten. Dies betrifft vor allem Entwickler, IT-Administratoren und IT Support Mitarbeiter.

- Verbot von Support-Arbeiten mit Domain-Administrator-Rechten auf den Clients/Servern

- Zugriff auf sensible Daten/Server sowie Arbeiten mit hoch privilegierten Accounts (z.B. Domain Admin) von einem dedizierten Admin-Jump-Host ermöglichen, respektive nicht von einem Client aus, der am Internet exponiert ist

- Der built-in Lokale Administrator Benutzer auf Servern und Clients sollte deaktiviert werden und dessen Passwort solle auf jedem Client/Server einzigartig sein. Dazu kann das Tool LAPS von Microsoft verwendet werden.

Passwort Policy

Sehr starke Passwort Policy (komplexe und keine sprechenden Passwörter, min. 24 Zeichen), für mindestens folgenden Benutzer/Gruppen:

Domain Administrators, Enterprise Administrators, Schema Administrators, Account Operators, Backup Operators, BUILTIN\Administrators, Service Accounts für Softwareinstallationen und Updates, Service Accounts für Security Scans und Antivirussoftware.

Client und Server Hardening

Folgende Group Policy Logon Rights Restrictions verhindern viele der Lateral Movement Techniken:

Deny access to this computer from the network; Deny logon as a batch job; Deny logon as a service; Deny logon locally; Deny logon through Remote Desktop

Einsatz des Tools Bloodhound für AD. Damit lässt sich in kurzer Zeit ein Bild darüber verschaffen welche Benutzer mit welchen Rechten auf welchem System eingeloggt sind. Damit lassen sich mögliche Angriffspfade und ein entsprechendes Nichteinhalten von internen Richtlinien erkennen, sowie das Erkennen von Schwachstellen an denen nachgebessert werden kann.

Logging und Monitoring

Zu Letzt das Thema Logging und Monitoring von privilegierten Account:

- Grundsätzlich Advanced Audit Policies aktivieren
- Security Log Monitoring zentralisieren, z.B. mit Graylog
- Die Cheat-Sheet Sektion von malwarearchaeology.com bietet gute Einstiegshilfen bezüglich was und warum geloggt und alarmiert werden kann
- Microsoft bietet eine erweiterte Liste von wichtigen Event IDs, welche bei Analyse und Alerting hilfreich sein können

Nicht in der obigen Liste geführt wird Netzwerksegmentierung, mindestens zwischen der Client- und Server-Population. Falls nicht vorhanden, ist einiges an Aufwand nötig um dies umzusetzen. Jedoch gehört die Abschottung von den Servern zu den am Internet exponierten Clients zu den Grundpfeilern eines modernen Security-Konzepts.

FAZIT

Priviligierte Benutzer werden in der Praxis noch nicht flächendeckend und ausreichend geschützt. Dadurch werden Angriffe auf eine entsprechende Infrastruktur vereinfacht. Fehlt dazu noch eine adäquates Security Logging und Monitoring, kann eine allfällige Kompromittierung für lange Zeit nicht erkannt werden. Unter Umständen wird so die gesamte Infrastruktur teils fahrlässig exponiert.

Microsoft hat mit ihrer aktuellen Software auf die gängigen Angriffs-Pfade reagiert und umfangreiche Dokumentationen dazu erstellt sowie Funktionen und Tools bereitgestellt, um unter anderem den Missbrauch von privilegierten Accounts zu erschweren. Jedoch sind die Risiken und Lösungen doch noch in einigen Unternehmen nicht bekannt. Abschliessend sind die hier vorgestellten Punkte nicht, aber die Konzepte und Tools können in den gängigen AD-Umgebungen als Startpunkt und Inspiration dienen.

Dominik Altermatt

WEB APPLICATION PENETRATION TEST

UNSER BELIEBTESTES PAKET
★★★★★

Kickstart

Für eine einfache, kostengünstige Identifikation von typischen Schwachstellen oder periodischen Prüfungen.

5‘000
CHF

Am besten geeignet für:

- Kleine Anwendungen ohne sensitive Informationen (z.B. Microsites)
- Neuere und kleinere Releases von bestehenden, schon geprüften Seiten

Standard

Bewährt: Vollumfängliche Prüfung nach OWASP Testing Guide mit umfangreichem Reporting und Massnahmen.

13‘370
CHF

Am besten geeignet für:

- Die meisten Webseiten und Webapplikationen
- Anwendungen im Umgang mit sensitiven Daten
- Webseiten mit den ASVS Anforderung Standard oder Advanced

Advanced

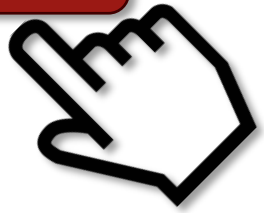
Für hochsichere Ziele: Unser bewährter Testansatz, der auf Ihre individuellen Bedürfnisse zugeschnitten wird.

29‘990
CHF

Am besten geeignet für:

- Komplexe Seiten und Applikationen mit überdurchschnittlichen Anforderungen
- Applikationen mit kundenidentifizierenden Daten
- Seiten mit den ASVS Anforderungen Standard oder Advanced

EINFACH ONLINE BESTELLEN



MICHAEL SCHNEIDER

KERBEROASTING ABGREIFEN VON CREDENTIALS

An der *Area 41* vom 15. und 16. Juni 2018 haben wir den Workshop *Adversary Simulation* veranstaltet. Über den Aufbau der Workshop-Testumgebung habe ich im Juni geschrieben. In diesem Workshop konnten Teilnehmer Angriffe in einer Windows Active Directory-Umgebung simulieren und Schwachstellen ausnutzen um sich erweiterte Rechte zu verschaffen. Eine mögliche Angriffstechnik in der AD-Infrastruktur war *Kerberoasting*. In diesem Artikel stelle ich Kerberoasting vor, wie ein Angriff ausgeführt wird und detektiert werden kann.

WAS IST KERBEROASTING

Die Kerberoasting-Attacke wurde von Tim Medin bei seiner Präsentation *Attacking Microsoft Kerberos Kicking the Guard Dog of Hades* an der *Derbycon 2014* vorgestellt. Die Attacke beschreibt eine effektive Methode als normaler Domänen-Benutzer an Credentials von Service-Accounts zu gelangen. Dieser Angriff ist vor allem erfolgreich, wenn schwache Passwörter für Service-Accounts genutzt werden.

Um die Kerberoasting-Attacke verstehen zu können, sind Kenntnisse über die *Kerberos-Implementierung* von Windows von Nutzen. Die Grundlagen erklärte Oliver Kunz in seinem Artikel *Kerberos Key Distribution Center Proxy*. Kurz zusammengefasst erhält ein Benutzer bei seiner Anmeldung ein *Ticket-Granting-Ticket* (TGT) vom *Key Distribution Center*. Das TGT wurde vom Account *krbtgt* signiert und gilt als Beweis der Identität des Benutzers. Mit dem TGT kann der Benutzer *Service-Tickets* (TGS) für spezifische Ressourcen der Domäne beantragen. Ein Bestandteil eines TGS ist verschlüsselt mit dem *NTHash* (NTLM Hash) des Service-Accounts der angefragten Ressource. Windows verwendet *Service Principal Names* (SPNs), um zu ermitteln, welcher Service-Account zur Verschlüsselung des TGS genutzt wird. Es gibt zwei Typen von SPN:

- Host-basierte *SPNs*, welche mit dem Computer-Account verknüpft sind
- sowie *SPNs*, die mit einem Domain-User-Account verbunden wurden.

Für Kerberoasting sind hostbasierte-Accounts nicht interessant, da ein Computer-Account im Active Directory über ein zufällig generiertes 128 Zeichen langes Passwort verfügt, welches alle 30 Tage gewechselt wird. Wird jedoch ein SPN für einen Domain-User-Account registriert, unter anderem für den Betrieb von Microsoft-SQL-Server-Instanzen, dann wird der NTHash des Passworts des Benutzers verwendet. Wenn ein schwaches Passwort für einen Service-Account gewählt wird, hat ein Angreifer gute Möglichkeiten dieses zu errechnen.

Jeder Domänen-Benutzer kann TGS für beliebige Dienste, die über einen registrierten SPN verfügen, bei einem Domain-Controller anfragen. Der Domain-Controller prüft bei der Erstellung des TGS nicht, ob der anfragende Benutzer Zugriff auf die jeweilige Ressource hat. Die Prüfung des Zugriffs wird in der Kerberos-Implementation von Windows dem dafür verantwortlichen Dienst überlassen. Ein Angreifer kann dieses Ticket nutzen, um offline das Passwort des Service-Accounts zu errechnen, da das Ticket mit dem NTHash des Service-Accounts verschlüsselt wurde.

Die Kerberoasting-Attacke in einem Satz erklärt bedeutet, dass jeder gültige Domänen-Account ein Kerberos-Service-Ticket für einen beliebigen Dienst beantragen und anschliessend das Ticket für Offline-Passwort-Cracking-Versuche verwenden kann.

DURCHFÜHREN VON ANGRIFFEN

Es gibt verschiedene Möglichkeiten TGS anzufragen, von der Windows-Built-In Funktion *SetSPN.exe* über PowerShell- und Python-Scripts. Das Projekt PowerShell Empire verfügt über ein Modul namens *Invoke-Kerberoast*, das alle SPN einer Domäne ermittelt und für jeden Service-Account ein TGS beantragt. Das TGS kann direkt im passenden Format für *hashcat* ausgegeben werden.

Als Alternative empfiehlt sich Impacket's *GetUserSPN.py*, ein Python-Script, das den Vorteil bietet unter Linux zu laufen und keinen Gebrauch von üblicherweise überwachten Funktionen wie *cmd.exe* oder *powershell.exe* zu machen. Für GetUserSPN.py werden Benutzername und Passworts eines Domänen-Benutzers benötigt.

```
PS C:\> Invoke-Kerberoast -OutputFormat Hashcat

TicketByteHexStream  :
Hash                 : $krb5tgs$23$*srv_database_app01$labs.scip.ch$MSSQLSvc/app01.labs.scip.ch*$0DA02EDC4A5C472A5C66D6
                       A1E4FAF31B$B85C9821DFBB21A3935074934E538B4B7FE72FA413418410C1BBDCAFAD2755678A2E2BBF7816B05593A9F
                       <redacted by scip AG>
SamAccountName       : srv_database_app01
DistinguishedName    : CN=Service Database App01,OU=Service,OU=Accounts,OU=Labs,DC=labs,DC=scip,DC=ch
ServicePrincipalName : MSSQLSvc/app01.labs.scip.ch
```

Die Dauer des Cracking-Vorgangs hängt von der Komplexität der Passwörter ab. Einfach Passwörter können innerhalb von Minuten geknackt werden. Strategien zum Errechnen von Passwörtern hat Eleanore Young in ihrem Artikel *Passwortsicherheit – Wenn Passwörter so klar wie Glas* sind vorgestellt.

ERKENNEN VON ANGRIFFEN UND GEGENMASSNAHMEN

Die effektivste Massnahme gegen Kerberoasting ist die Verwendung von starken Passwörtern, die länger als 27 Zeichen sind. Es sollte dabei sichergestellt werden, dass sämtliche Service-Accounts über solche sicheren Passwörter verfügen und diese auch regelmässig geändert werden können.

Um die Ausstellung von TGS überwachen zu können, muss die Einstellung *Audit Kerberos Service-Ticket Operations* aktiviert werden. Danach kann nach der *Event-ID 4769* (A Kerberos service ticket was requested) gesucht werden. Das Erkennen von Angriffen ist nicht trivial, da das Anfragen und Ausstellen von TGS im normalen Betrieb jedes Mal geschieht, wenn Benutzer Zugriff auf Ressourcen benötigen. Dabei kann einerseits nach Benutzer gesucht werden, die eine exzessive Anzahl von solchen Ereignissen in kurzer Zeit generieren. Zusätzlich kann ein Honeypot-Account angelegt werden, bei dem manuell das AD-Attribut *adminCount* auf 1 gesetzt und ein SPN-Eintrag angelegt wird. Danach können die Ticket-Events auf diesen Account gefiltert werden.

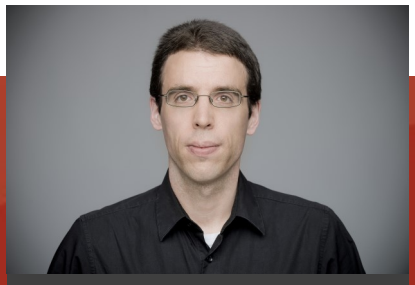
In der Detailansicht des Events wird dabei ersichtlich, welcher Account das Ticket angefordert hat.

full_message

```
A Kerberos service ticket was requested.

Account Information:
        Account Name:           rtam@LABS.SCIP.CH
        Account Domain:         LABS.SCIP.CH
        Logon GUID:             {4636F275-64FB-32E4-C74C-FE1D940AD12F}

Service Information:
        Service Name:           srv_database_app01
        Service ID:             S-1-5-21-3685327493-4069616680-3530608807-2610

Network Information:
        Client Address:         ::ffff:192.168.244.200
        Client Port:            60252

Additional Information:
        Ticket Options:         0x40810010
        Ticket Encryption Type: 0x17
        Failure Code:           0x0
        Transited Services:     -
```

FAZIT

Kerberoasting ist eine *effiziente Technik* für Angreifer, welche über wenig Rechte innerhalb einer Domäne verfügen. Je nach Stärke der Passwörter verfügt ein Angreifer innert kurzer Zeit über mehrere Accounts, welche für weitere Angriffe und Informationsbeschaffung verwendet werden können. Der Angriff selbst kann nicht verhindert, aber durch die Wahl von starken Passwörtern erschwert werden. Service-Accounts sollten daher analog wie privilegierte Accounts behandelt werden. Dazu gehört das Erstellen einer Liste von Service-Accounts, die Überprüfung der letzten Passwort-Änderung sowie ein Prozess, wie deren Passwörter regelmässig geändert werden können.



Michael Schneider

)SCIP(

EINE DER GROSSEN HERAUSFORDERUGEN

BLEIBT NACHHALTIGKEIT

Bildquelle: https://pixabay.com/photo-3579931/

VULNERABILITY SUMMARY

AUSGEWÄHLTE SCHWACHSTELLEN DES AKTUELLEN MONATS

1

ORACLE DATABASE SERVER UNBEKANNTE SCHWACHSTELLE

Eine Schwachstelle wurde in Oracle Database Server 11.2.0.4/12.1.0.2/12.2.0.1/18c gefunden. Sie wurde als sehr kritisch eingestuft. Es geht hierbei um eine unbekannte Funktion der Komponente Java VM. Der Angriff kann über das Netzwerk passieren. Das Ausnutzen erfordert keine spezifische Authentisierung. Als 0-Day erzielte der Exploit wohl etwa $100k und mehr auf dem Schwarzmarkt. Ein Upgrade vermag dieses Problem zu beheben.

» https://vuldb.com/de/?id.125366

2

ORACLE JAVA SE 8U182/11 SCRIPTING UNBEKANNTE SCHWACHSTELLE

Eine Schwachstelle wurde in Oracle Java SE 8u182/11 ausgemacht. Sie wurde als sehr kritisch eingestuft. Die Ausnutzbarkeit gilt als schwierig. Umgesetzt werden kann der Angriff über das Netzwerk. Das Ausnutzen erfordert keine spezifische Authentisierung. Technische Details oder ein Exploit zur Schwachstelle sind nicht verfügbar. Ein Exploit zur Schwachstelle wird momentan etwa USD $25k-$50k kosten. Ein Aktualisieren vermag dieses Problem zu lösen.

» https://vuldb.com/de/?id.125513

3

LINUX KERNEL BIS 4.14.10 PSEUDO TERMINAL DRIVERS/TTY/N_TTY.C DENIAL OF SERVICE

In Linux Kernel bis 4.14.10, ein Betriebssystem, wurde eine problematische Schwachstelle ausgemacht. Betroffen ist eine unbekannte Funktion der Datei drivers/tty/n_tty.c der Komponente Pseudo Terminal. Durch das Manipulieren mit einer unbekannten Eingabe kann eine Denial of Service-Schwachstelle ausgenutzt werden. Der Angriff muss lokal angegangen werden. Ein Aktualisieren auf die Version 4.14.11 vermag dieses Problem zu lösen.

» https://vuldb.com/de/?id.125737

4

DAIMLER MERCEDES COMAND 17-13.0 50.12 NAVIGATION ROUTE DENIAL OF SERVICE

In Daimler Mercedes Comand 17-13.0 50.12 wurde eine Schwachstelle ausgemacht. Sie wurde als problematisch eingestuft. Durch Beeinflussen mit einer unbekannten Eingabe kann eine Denial of Service-Schwachstelle (Loop) ausgenutzt werden. Zur Ausnutzung ist eine einfache Authentisierung erforderlich. Insgesamt 88 Tage schien es sich um eine nicht veröffentlichte Zero-Day Schwachstelle gehandelt zu haben.

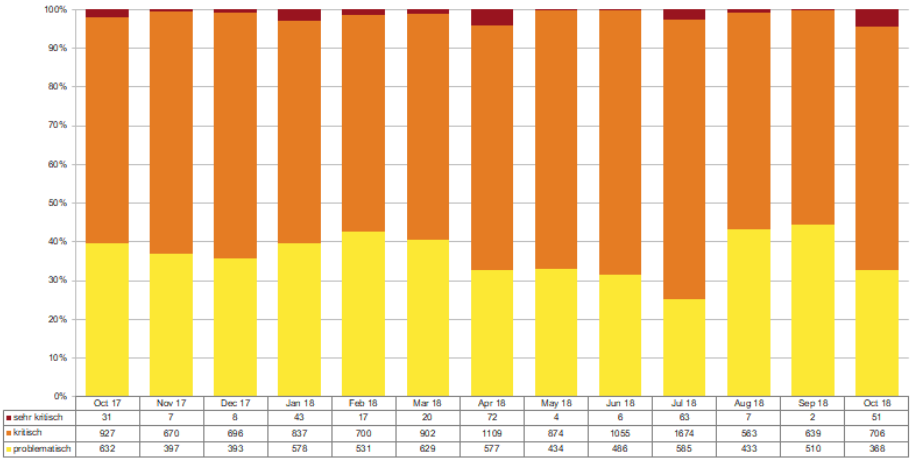
» https://vuldb.com/de/?id.125080

VULNERABILITY LANDSCAPE

AKTUELLE STATISTIKEN AUS UNSERER VULDB

MEISTEXPONIERTE PRODUKTE IM VERGANGENEN MONAT

VERLAUF DER RISIKEN DER VERGANGENEN 12 MONATE



	Oct 17	Nov 17	Dec 17	Jan 18	Feb 18	Mar 18	Apr 18	May 18	Jun 18	Jul 18	Aug 18	Sep 18	Oct 18
sehr kritisch	31	7	8	43	17	20	72	4	6	63	7	2	51
kritisch	927	670	696	837	700	902	1109	874	1055	1674	563	639	706
problematisch	832	397	393	578	531	629	577	434	486	585	433	510	368

Datenquelle: https://vuldb.com/de/

SCIP MONTHLY SECURITY SUMMARY

IMPRESSUM

ÜBER DEN SMSS

Das *scip Monthly Security Summary* erscheint monatlich und ist kostenlos.

Anmeldung: smss-subscribe@scip.ch
Abmeldung: smss-unsubscribe@scip.ch

Informationen zum Datenschutz.

Verantwortlich für diese Ausgabe:
Stefan Friedli & Marc Ruef

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion des Herausgebers, den Redaktoren und Autoren nicht übernommen werden. Die geltenden gesetzlichen und postalischen Bestimmungen bei Erwerb, Errichtung und Inbetriebnahme von elektronischen Geräten sowie Sende- und Empfangseinrichtungen sind zu beachten.

ÜBER SCIP AG

Wir überzeugen durch unsere Leistungen. Die scip AG wurde im Jahr 2002 gegründet. Innovation, Nachhaltigkeit, Transparenz und Freude am Themengebiet sind unsere treibenden Faktoren. Dank der vollständigen Eigenfinanzierung sehen wir uns in der sehr komfortablen Lage, vollumfänglich herstellerunabhängig und neutral agieren zu können und setzen dies auch gewissenhaft um. Durch die Fokussierung auf den Bereich Information Security und die stetige Weiterbildung vermögen unsere Mitarbeiter mit hochspezialisiertem Expertenwissen aufzuwarten.

Weder Unternehmen noch Redaktion erwähnen Namen von Personen und Firmen sowie Marken von Produkten zu Werbezwecken. Werbung wird explizit als solche gekennzeichnet.

scip AG
Badenerstrasse 623
8048 Zürich
Switzerland

+41 44 404 13 13
www.scip.ch