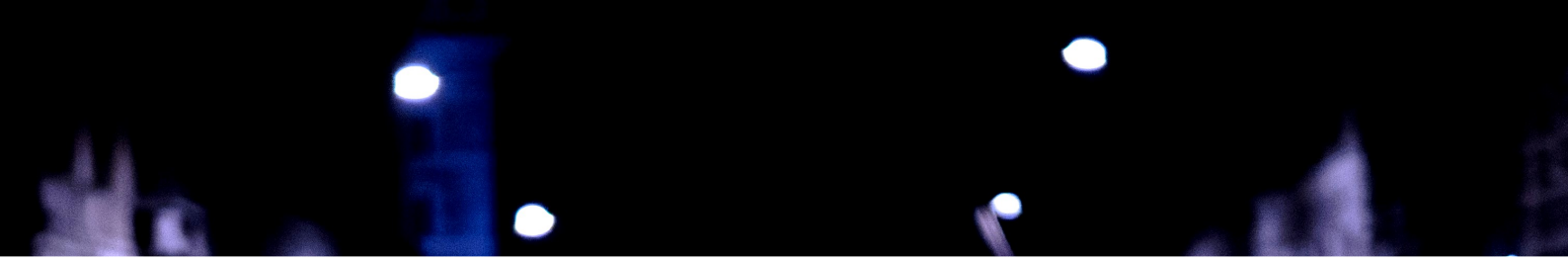
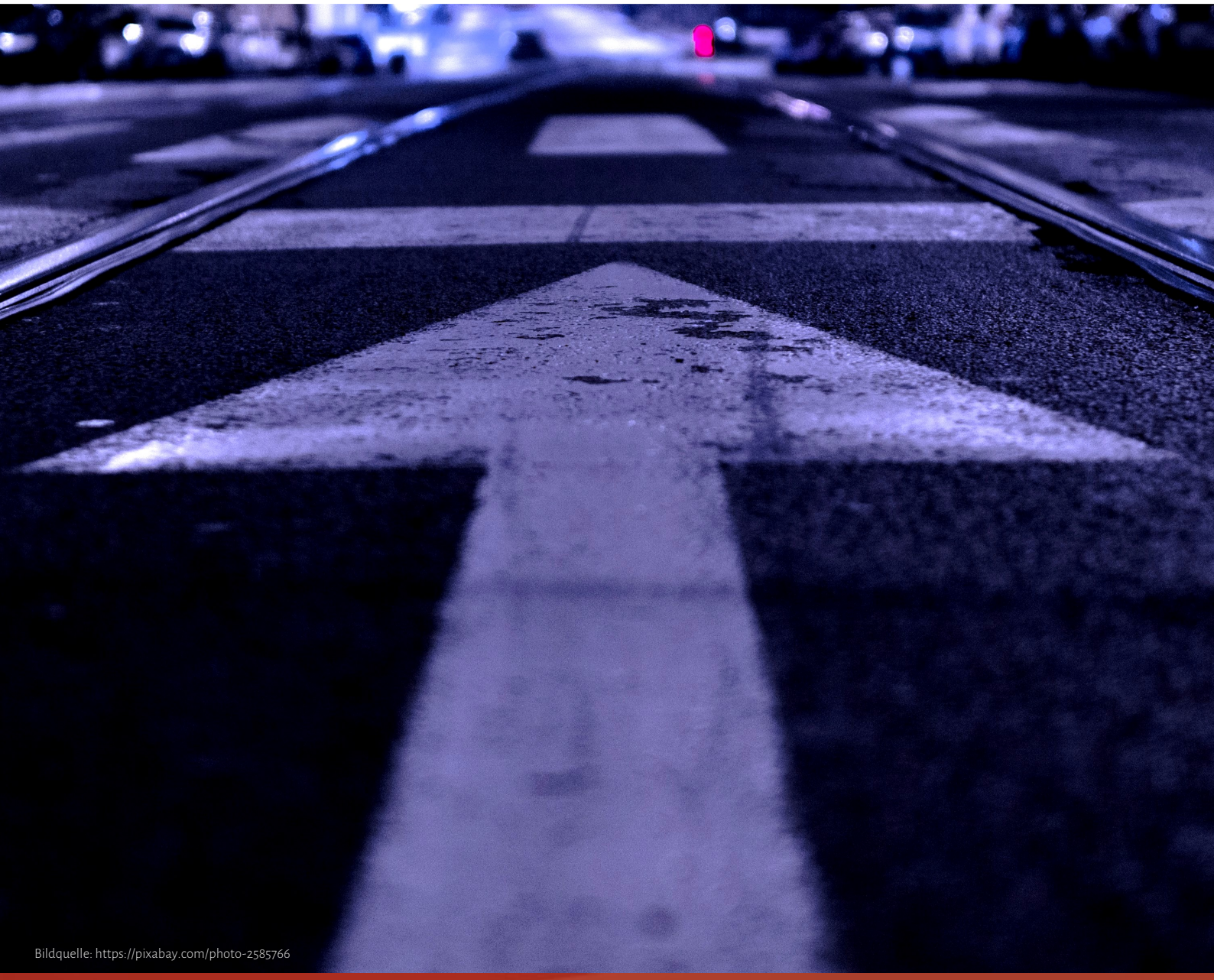


)SCIP(MONTHLY SECURITY SUMMARY

Ausgabe November 2017



Bildquelle: https://pixabay.com/photo-2585766

FOKUS

ACTIVE DIRECTORY UND MAIL SECURITY

November 2017: Schweigen ist Gold?

„My voice is my password“. Mit dieser ikonischen Phrase authentisierte sich ein Protagonist im Film „Sneakers“ (1992) an einer biometrischen Sicherheitsschleuse. Während Voice Profiling als Authentisierungsmittel heute wenig Popularität geniesst, steht die Nutzung von Gesprochenem als primäres Benutzerinterface heute vor dem grossen Durchbruch: Bereit heute erfolgt nahezu ein Viertel aller Suchanfragen auf Mobilgeräten mittels Spracheingabe.

Es ist eine Frage der Zeit, bis Siri & Co., aber auch noch gänzlich unbekannte Use Cases, hier einmal mehr technologische Entwicklungen in unserem Alltag ermöglichen. Für den Themenbereich der Informationssicherheit heisst das: Mitdenken und bereit sein, für einen weiteren technologischen Fortschritt.

Aller Innovation zum Trotz: Auch bestehende Technologie entwickelt sich weiter. In unserer vorliegenden Ausgabe sprechen wir ausführlich über die Sicherheit von Active Directory und Mailsystemen und wünschen Ihnen bei der Lektüre der vorliegenden Ausgabe viel Vergnügen.

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?

INTERVIEW ZU SICHERHEIT VON FACEID

In der Ausgabe des 09. November 2017 der Zeitung *20 Minuten* diskutiert Stefan Friedli die Sicherheit von *Apple FaceID*. Der unkomplizierte *Sicherheitsgewinn* ist der massgebliche Vorteil des jüngsten Ansatzes auf dem *iPhone X*. Das ungekürzte Interview steht online zur Verfügung und seine umfassende Einschätzung zum Thema findet sich in unserem Fachartikel.

VORTRAG ZU SMART BUILDINGS AN MESSE SICHERHEIT

Vom 14. bis 17. November 2017 fand in Zürich die *Messe Sicherheit* statt. Am ersten Tag der Messe wurde durch Marc Ruef die *Keynote* halten. In diesem wurde aufgezeigt, wie durch das Ausnutzen von Schwachstellen in *IoT* und *Smart Homes* möglich wird, in Gebäude einzubrechen und dadurch den virtuellen Einbruch mit dem physischen zu kombinieren.

KEYNOTE ZU CYBERCRIME AN C+E FORUM

Am 02. November 2017 findet im *Ebianum* in Fisibach der Kundenevent von *C+E Forum* statt. An diesem wurde durch Marc Ruef die Keynote gehalten. In dieser hat er sich zum Thema *Cybercrime*, vor allem im Kontext mit der zunehmenden Vernetzung der heutigen Zeit, geäussert. Dabei wurde vor allem auf das Thema *IoT*, *Medical Devices* und *Smart Buildings* eingegangen.

Weitere News zu unserer Firma finden Sie auf unserer Webseite.

SCIP BUCHREIHE

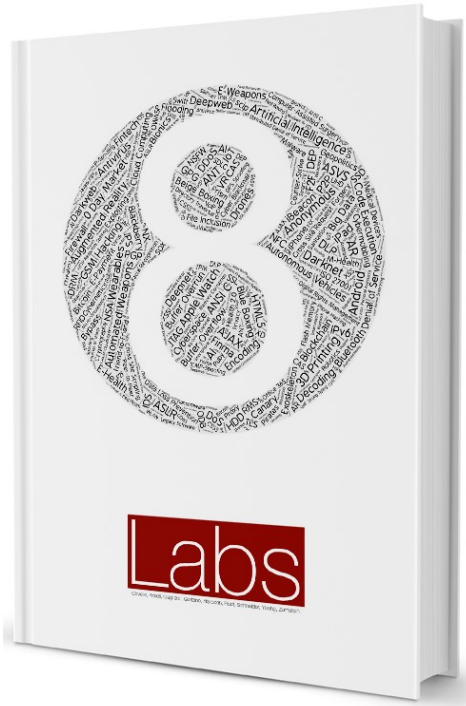
UNSER AKTUELLES BUCH

Heute, mehr als je zuvor, stehen *Cyberkriminalität* und *kritische Infrastrukturelemente* im Fokus des öffentlichen Interesses. Das *Internet der Dinge*, versteckte *Marktplätze für illegale Waren*, aber auch der Diskurs über die grundsätzliche Bedeutung von *Cybersecurity* für die moderne Gesellschaft – das alles sind Themen, mit denen sich die Mitarbeitenden der scip AG im vergangenen Jahr beschäftigt und in diesem Buch zusammengefasst haben.

Trotz aller Veränderung: Auch in der achten Ausgabe mischen sich altbekannte Themenkomplexe wie *Hardening*, *Verschlüsselung* und *organisatorische Fragen* der Informationssicherheit unter die zahlreichen zeitgenössischen Themen. Und so bietet auch diese Ausgabe, wie gewohnt, einen Einblick in das weite Tätigkeitsfeld der scip AG und ihrer Mitarbeitenden.

Mit einem exklusiven Vorwort von Ivan Büchi, Head of Digital Office bei der Glarner Kantonalbank.

Weitere Informationen auf unserer Webseite.



ISBN 978-3-9524389-4-7 [de]
ISBN 978-3-9524389-5-4 [en]

)SCIP(

RISIKEN SIND IMMER EINE HERAUSFORDERUNG

Bildquelle: https://pixabay.com/photo-2933984/

MICHAEL SCHNEIDER

BLOODHOUND
AUF DER JAGD NACH DOMAIN-ADMINS

Das *Active Directory* (AD) ist die zentrale Verwaltung von Zugangsdaten, Rollen und Berechtigungen. Neben der Windows-Infrastruktur werden weitere Anwendungen mittels *Single Sign-on* angebunden. Wer administrativen Zugang zum AD hat, kontrolliert Zugänge zu Anwendungen und deren Daten und kann sich *Kerberos-Tickets ausstellen*, die Zugriff auf Informationen erlauben. Ein Angreifer (Offense) im internen Netz wird daher versuchen privilegierte Berechtigungen im AD zu erlangen. Handumkehrt wird die zuständige IT-Abteilung (Defense) bemüht sein, genau dies zu verhindern. Ein Domänen-Benutzer verfügt bereits über umfangreiche Lese-Rechte im AD und kann bereits viele Informationen auslesen, unter anderem Eigenschaften von Benutzern, Gruppen, *Zugriffsrechte* (ACL) oder *Group Policies*. Diese Standard-Rechte erschweren die Verteidigung des ADs, da sich ein Angreifer dadurch viele Informationen beschaffen kann.

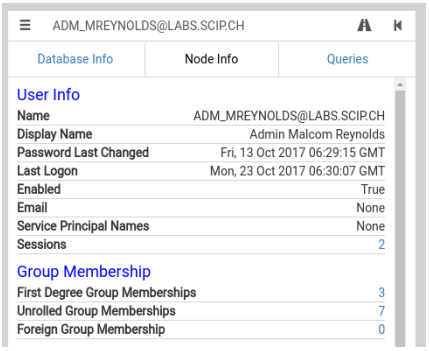
VORSTELLUNG VON BLOODHOUND

Am 4. August 2016 wurde an der *Defcon 24* anlässlich des Talks *Six Degrees of Domain Admin* von den Entwicklern und Penetration Testern Andy Robbins, Will Schroeder und Rohan Vazarkar das Tool *BloodHound* vorgestellt und zwei Tage drauf in der Version 1.0 veröffentlicht. Dieses Tool macht sich diese Konstellation der offenen Leserechte in einem Active Directory zu Nutze. Mittels eines sogenannten *Ingestor* werden Objektes des AD ausgelesen und anschliessend grafisch dargestellt. Das Tool generiert aus den abgefragten Daten eine Übersicht über Benutzer und Gruppen, welche Rechte diese haben und auf welchen Systemen diese angemeldet sind. Für einen Angreifer sind solche Zusammenhänge Gold wert. Er ist damit in der Lage, Wege zu Mitgliedern der Gruppe *Domain Admins* zu finden und gegebenenfalls diese anzugreifen. Doch auch für die Defense ist BloodHound von hohen Nutzen, da damit allfällige Schwächen identifiziert und anschliessend behoben werden können.

Etwa ein Jahr später wurde im Oktober 2017 die Version 1.4 von BloodHound veröffentlicht. Diese Version bringt verschiedene Verbesserungen mit sich. BloodHound zeigt nun Eigenschaften von Objekten, wie Benutzername, letzte Änderung des Passworts oder Zeitpunkt des Logins, an. Zudem wurde der bisher auf PowerShell v2 basierende Ingestor von Grund auf überarbeitet und mit C# neu geschrieben. Der neue C#-Ingestor heisst *Sharp Hound* und liegt als Binary oder PowerShell-Skript vor. Mit dem PowerShell-Skript wird das Binary zur Laufzeit entpackt und ausführt. Rohan Vazarkar beschreibt in seinem Blog-Post *SharpHound: Evolution of the BloodHound Ingestor* die Überarbeitung und neuen Funktionen von SharpHound.

SAMMELN VON DATEN

Zunächst werden Informationen des Active Directory mit SharpHound ausgelesen und im Backend gespeichert. Als Datenspeicher setzt Bloodhound *Neo4j* ein. Das Backend kann unter Windows, Linux oder macOS installiert werden. SharpHound generiert standardmässig CSV-Dateien, die ins Backend importiert werden. Mittels der Parameter *--Uri* und *--UserPass* werden die gesammelten Daten direkt in die Neo4j-Instanz geschrieben. Dies ist nützlich, wenn SharpHound auf verschiedenen Systemen ausgeführt wird oder einer Schleife läuft, um regelmässig Sessions auszulesen (Parameter *-c SessionLoop*). Je nach AD-Topologie und Netzwerk-Segmentierung ist die Auswertung von SharpHound unvollständig, da beispielsweise der Zugriff auf Server nicht möglich ist und damit Sessions nicht enumeriert werden. Falls möglich sollte SharpHound auf verschiedenen Systemen und Netzwerksegmente ausgeführt werden, um auch ansonsten *tote Winkel* zu erreichen.



SharpHound liest grundsätzlich *Trusts*, *Sessions*, *Local Admin* und *Group Membership* aus. Über den Parameter *-CollectionMethod* kann dies erweitert werden. Wir empfehlen für die initiale Datensammlung zusätzlich *Logged On*, ACL und Object Props zu sammeln. Bei *Logged On* sind administrative Rechte auf dem Zielsystem nötig, um die Benutzer auszulesen. Ein Angreifer, mit den Rechten eines *Domain User*, kann nicht an diese Daten gelangen. SharpHound legt eine *Cache-Datei* namens *BloodHound.bin* an, diese beschleunigt die Ausführung bei mehrmaligen Abfragen.

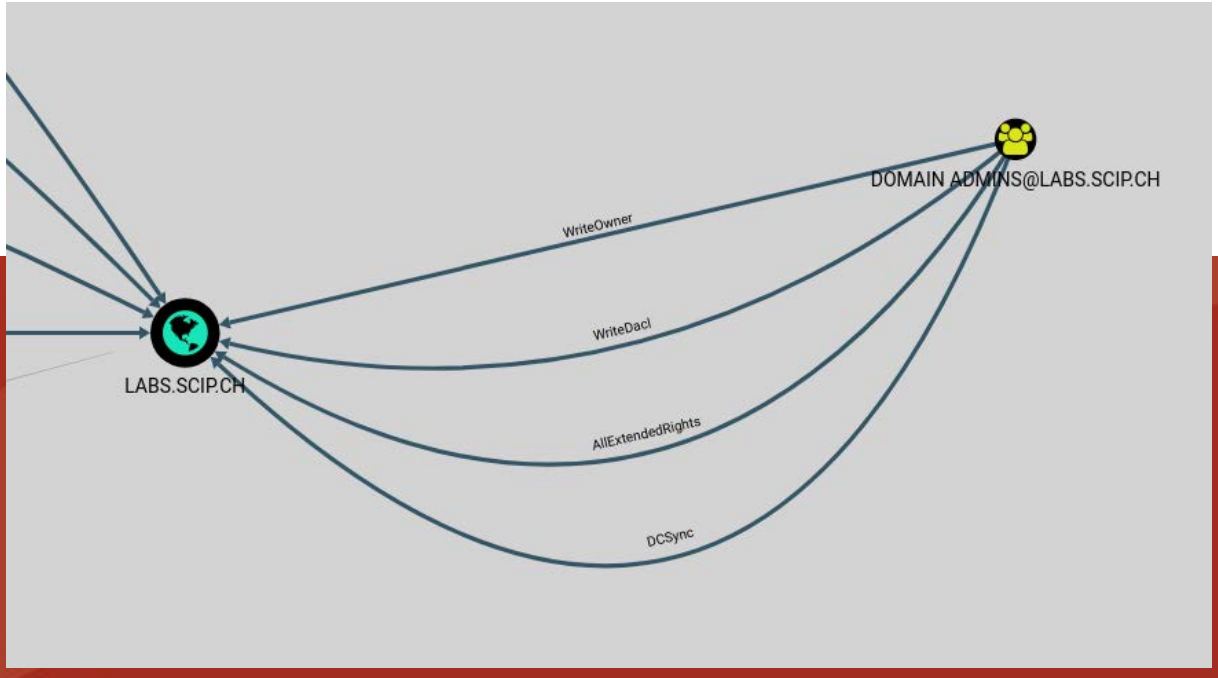
Nützlich für Angreifer sind die Optionen *--Stealth* und *--ExcludeDC*. Letztere verhindert, dass Session-Informationen von *Domain Controllern* (DC) abgefragt werden. Dies verhindert die Entdeckung eines Scans durch Microsoft ATA, da ATA in diesem Kontext nur DCs überwacht.

VISUALISIERUNG VON AD-OBJEKTEN

BloodHound stellt die gesammelten Daten dar, unter *Node Info* werden kontextbezogen Informationen zum jeweiligen Objekt bereitgestellt.

Von einer Node kann weiter navigiert werden, beispielweise in welchen Gruppen ein Benutzer Mitglied ist oder auf welchen Systemen der Benutzer lokale Administratoren-Rechte besitzt. Dabei wird unterschieden, ob diese Rechte direkt vergeben oder via Vererbung erlangt werden.

Mit der Version 1.4 gab es eine weitere Funktion, die anzeigt welche Benutzer oder Gruppen über *DCSync-Rechte* verfügen.



Die DCSync-Rechte erlauben es, Objekte zu replizieren. Ein Angreifer kann dies Nutzen, um mit *Mimikatz* an die Zugangsdaten des Accounts *krbtgt* zu gelangen.

WEGE ZUM DOMAIN-ADMIN

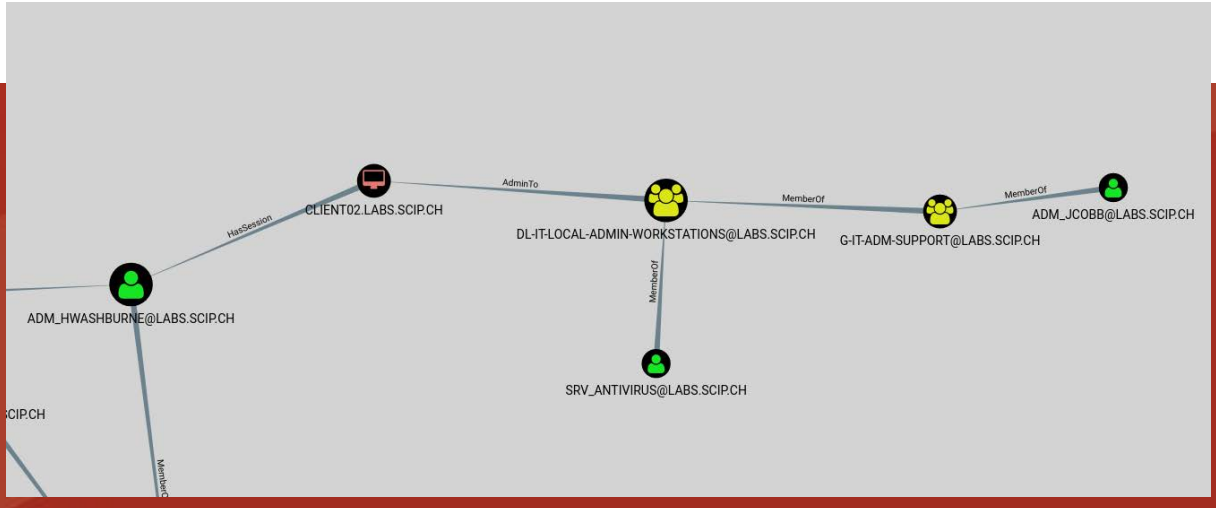
Wir haben BloodHound in unserem Lab *lab.scip.ch* auf die Mitglieder der Gruppe *Domain Admins* angesetzt, um zu eruieren, wie sich ein Angreifer Domain-Admin-Privilegien beschaffen könnte. Im ersten Beispiel ist der Domain-Admin *adm_hwashburne* auf dem Computer *client02* angemeldet.

Der Benutzer *adm_jcobb*, der als Mitglied der IT-Supporter-Gruppe (*G-IT-ADM-Support*) lokale Administratorenrechte auf allen Workstations der Domain besitzt, wäre so in der Lage, an Domain-Admin-Zugangsdaten zu gelangen. Ebenso könnten Angreifer den Service-Benutzer für die Workstation-Antivirensoftware (*srv_antivirus*) dazu missbrauchen. Aus Sicherheitsgründen sollte sich ein Account mit Domain-Admin-Rechten nicht auf einer Workstation oder anderen nicht spezifisch gehärteten Systemen anmelden.

Beim zweiten Beispiel läuft auf dem Computer *file01* ein Backup-Job, der durch den Service-Benutzer *srv_backup* ausgeführt wird. Dieser Benutzer verfügt über Domain-Admin-Rechte.

Der Benutzer *adm_zwashburne*, ein Mitglied der IT und Administrator von Member-Servern, hätte somit die Möglichkeit an Domain-Admin-Zugangsdaten zu gelangen. In diesem Fall stellt sich die Frage, ob der Backup-Servicebenutzer wirklich Domain-Admin-Rechte benötigt oder dedizierte Rechte nicht ausreichen.

Im dritten Beispiel besteht die Möglichkeit, dass ein Domänenbenutzer auf direktem Weg Domain-Admin-Rechte erlangen kann. Der Benutzer *rtam* ist Entwickler und hat auf dem Applikationsserver *app01* Administratorenrechte erhalten. Gerade auf diesem Server ist der Domain-Admin *adm_hwashburne* angemeldet.



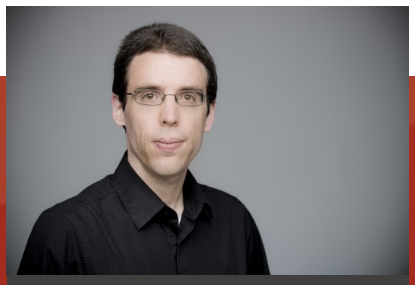
Die Rechte des Accounts *rtam* können direkt auf die Stufe eines Domain-Admins eskaliert werden. Es handelt es sich hier um eine unsichere Rechtevergabe. Ein normaler Benutzeraccount sollte nie über Administratorenrechte auf einem Server verfügen. Es sollten stets getrennte Accounts eingesetzt werden: Normale Accounts zur grundlegende Arbeiten und solche, die über administrative Privilegien verfügen. Für Entwickler oder andere Benutzergruppen sollten zudem keine Sonderrechte gelten, auch wenn es sich nur um eine Ausnahme respektive in diesem Fall um einen einzelnen Server handelt. Diese Fehlkonfiguration ermöglicht es, die Kontrolle über die Domäne zu übernehmen.

FAZIT

Die Beispiele zeigen den Nutzen für Offense und Defense gleichermassen. Die Offense fand mehrere interessante Ziele, die zur Rechteerweiterung ausgenutzt werden können. Durch Datensammlung in BloodHound können solche Angriffswege effizient ermittelt werden, ohne Systeme manuell und ohne gezieltes Vorgehen zu untersuchen.

Die Defense spürte mehrere potentielle Schwachstellen auf und kann entsprechende Gegenmassnahmen einleiten. So sollte beispielsweise eine Policy definiert werden, die es verhindert, dass sich Domain-Admin-Accounts auf Workstations anmelden.

Ich kann es nur empfehlen BloodHound in der eigenen AD-Infrastruktur laufen zu lassen und zu analysieren, wie im eigenen Netzwerk der direkteste Weg zum Domain-Admin aussieht. Weidmannsheil!



Michael Schneider

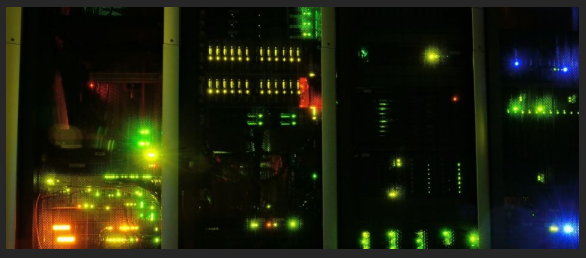
UNSERE SPEZIALISTEN SETZEN SICH TÄGLICH MIT DEM THEMA CYBERSECURITY AUSEINANDER. DIESER ERFAHRUNGSSCHATZ LÄSST KEINEN ZWEIFEL DARAN, DASS

WIR ÜBERZEUGEN

UND INSPIRIEREN KÖNNEN. BUCHEN SIE UNS FÜR IHREN EVENT, DAMIT WIR AUCH IHR PUBLIKUM MITREISSEN UND FÜR DAS THEMA BEGEISTERN KÖNNEN.

CYBERCRIME & DARKNET

Das Darknet gilt als verborgener Bereich des Internets, der durch Cyberkriminelle genutzt wird und schwierig zugänglich ist. Wir zeigen anhand konkreter Fälle, wie man sich im Darknet bewegt.

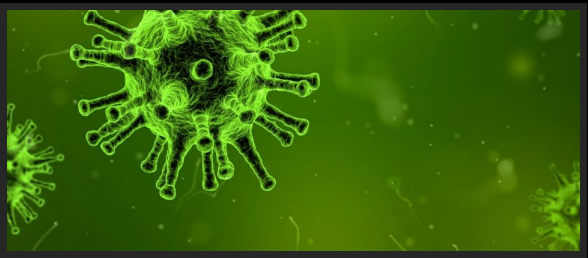


INTERNET OF THINGS

Das Thema IoT schleicht sich in unseren Alltag und beginnt uns zu beherrschen. Welche verheerenden Folgen Angriffe auf die digitale Infrastruktur haben, zeigen unsere aktuellen Forschungsresultate.

ARTIFICIAL INTELLIGENCE

Künstliche Intelligenz beginnt immer mehr Einfluss auf unser tägliches Leben zu nehmen. Die dadurch gewonnenen Chancen bringen aber auch Risiken mit, wie wir an konkreter Forschung illustrieren können.



MALWARE & RANSOMWARE

Unser Red Team führt offensive Penetration Tests durch, bei denen individuelle Malware für den Kunden entwickelt wird. Unser Wissen zeigt konkret, wie böswillige Viren-Entwickler denken und handeln.

Weitere Informationen auf unserer Webseite

www.scip.ch

ELEANORE YOUNG

SICHERUNG VON EMAIL IHRER DOMAIN - SPF, DKIM UND DMARC

Das *Simple Mail Transfer Protocol* (SMTP) besitzt keine intrinsische Methoden, um die Authentizität, Integrität und Vertraulichkeit einzelner Nachrichten zu gewährleisten. Somit ist es für Dritte relativ einfach, den Ursprung einer Email vorzutäuschen, eine Email abzufangen oder gar zu verändern. Es ist sogar so, dass es allen erlaubt ist, eine beliebige Domäne als Quelle der Email anzugeben.

Über die Jahrzehnte wurden mehrere zusätzliche Protokolle entwickelt, um die vorhin genannten Schwachstellen von Email anzugehen. Einige sind dafür gedacht, die Identität einzelner Nutzerinnen zu beweisen (z.B. PGP/GPG oder andere Public Key Kryptographie auf Basis von Individuen), während sich andere Methoden darauf konzentrieren, die Authentizität und Integrität aller Email Nachrichten einer bestimmten Domäne zu gewährleisten. In diesem Artikel werden wir drei Protokolle der letzteren Kategorie betrachten.

SPF – SENDER POLICY FRAMEWORK

Das SPF wurde dafür entwickelt, damit die Besitzerin einer Domäne explizit aufführen kann, welche Hosts von dieser Domäne aus Email versenden dürfen. Empfängerinnen (oder deren Server) können die SPF -Einträge verwenden, um die Authentizität einer erhaltenen Email mittels mehreren *Domain Name System* (DNS) Abfragen zu überprüfen. Das SPF vermag jedoch nicht die Authentizität von Email kryptographisch zu sichern, sondern besteht lediglich aus einer Abfolge von Regeln, die *Hostnamen und IP-Adressen verbinden*.

Eine Domäne kann ihre SPF-Regeln mittels eines DNS *TXT* Eintrags spezifizieren. Im Falle, dass die Domäne nicht ihre eigenen Email-Server betreibt, sieht der SPF-Eintrag meist wie folgt aus:

```
"v=spf1 include:spf.protection.outlook.com
-all"
```

Hier ist zu beachten, dass der SPF-Eintrag mit einem Header beginnt, der die Version von SPF angibt (v=spf1). Dieser Header wird dann gefolgt von Direktiven (od. *Mechanismen*), welche die SPF-Policy in einer links-nach-rechts Richtung angeben. Das SPF erkennt acht solcher Direktiven, welche wir später im Detail anschauen werden. Eines der zwei in der obigen SPF-Regel enthaltenen Direktiven, nämlich *include*, bindet die SPF-Konfiguration einer anderen Domäne mit ein. Die SPF-Policy dieser Domäne ist bedeutend länger und bindet selbst zwei andere Domänen rekursiv ein. Es ist zu beachten, dass der *SPF Proposed Standard* vorsieht, dass die Gesamtzahl an DNS-Abfragen beschränkt werden soll (meist 10 Abfragen).

```
"v=spf1 ip4:207.46.101.128/26
ip4:207.46.100.0/24 ip4:207.46.163.0/24
ip4:65.55.169.0/24 ip4:157.56.110.0/23
ip4:157.55.234.0/24 ip4:213.199.154.0/24
ip4:213.199.180.0/24
include:spfa.protection.outlook.com -all"
```

Abgesehen von include, erkennt das SPF zusätzlich die Direktiven *ip4*, *ip6*, *a*, *ptr*, *mx*, *exists* und *all*. Die *all* Direktive ist eine Sammelklausel, die immer erst am Ende eines Regelwerks verwendet werden sollte. Die Direktiven *ip4* und *ip6* erlauben die Angabe von IP-Adressen, deren zugehörige Hosts Email versenden dürfen. Die Direktiven a und mx geben an, dass der zugehörige DNS-Eintrag (*A* oder *MX*) mit der Quelladresse der überprüften Email übereinstimmen muss, ehe diese als gültige Email erkannt wird. Die Direktive *ptr* erfordert, dass eine zweistufige DNS-Abfrage (IP-Adresse → Domainname → IP-Adresse) dieselben IP-Adressen aufweist, ehe eine Email anerkannt wird. Die Direktive *exists* erfordert schlussendlich, dass der Angegebene DNS-Name (*A* Eintrag) existiert. Der grosse Vorteil dieser Direktive ist, dass *Makro-Erweiterungen* erlaubt sind.

Die eben genannten Direktiven können jeweils mit einem der *Qualifizierer* + "Pass", - "Fail", ~ "SoftFail" oder ? "Neutral" vorangestellt werden. Diese verändern die Art und Weise eines *Zutreffens* der genannten Direktive. Der Qualifizierer - führt zu einer gänzlichen Abweisung einer Email bei einem Zutreffen der Regel. Der Qualifizierer ~ stellt bei einem Zutreffen der Regel die Empfehlung aus, dass eine Email zwar akzeptiert, aber als SPAM behandelt wird. Der Qualifizierer ? enthält sich schlussendlich jeglicher Empfehlung gegenüber der verifizierenden Partei. Falls kein Qualifizierer angegeben ist, wird + angenommen.

Zusätzlich zu den Qualifizierer, können *Modifikatoren* verwendet werden, um eine SPF-Policy mittels *redirect* an eine andere Domäne verschoben werden oder um eine Ablehnung einer Email gegenüber der Endnutzerin zu erklären (*exp*). Letzterer erlaubt zusätzlich Makro-Erweiterungen.

DKIM – DOMAIN KEYS IDENTIFIED MAIL

Weil das SPF keine kryptographische Absicherung bzgl. der Authentizität von Email bereitstellt, sollte das Protokoll *DKIM* verwendet werden, um dies zu für legitime Emails zu tun. DKIM stellt dies sicher, indem jede von einer Domäne ausgehende Email von der Besitzerin der Domäne *kryptographisch signiert* wird. Damit DKIM funktioniert, bedarf es zweierlei Dinge. Einerseits muss die betrachtete Domäne in einem DNS *TXT* Eintrag des namens *{selector}._domainkey.example.com.* den Public Key der Besitzerin der Domäne enthalten.

```
"v=DKIM1; k=rsa; p=[Base64-encoded public key]"
```

Andererseits muss jede authentische Email den Header *Dkim-Signature* enthalten. Dessen Wert besteht aus mindestens 8 Parameter: Die DKIM Protokollversion, der Signaturalgorithmus, welche Teile der Email signiert wurden, der *Selector* zum Auslesen des Public Keys der Domäne und die Kryptographische Signatur der Email.

Somit erlaubt das DKIM-Protokoll die Validierung der *Authentizität und Integrität* der signierten Teile erhaltener Emails. Dabei ist zu beachten, dass der Email-Body nicht immer signiert wird. Weil aber das DKIM-Protokoll nicht für alle Email durchgesetzt werden kann, schützt es nicht vor gefälschten Nachrichten und sollte immer im Zusammenhang mit dem SPF verwendet werden.

DMARC – DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING AND CONFORMANCE

Das *DMARC* Protokoll vereint das SPF und DKIM dadurch, dass DMARC die Möglichkeit des *Monitoring* einführt. Dies bedeutet auch, dass sowohl das SPF wie auch DKIM bereits umgesetzt werden müssen, bevor DMARC funktionsfähig wird. DMARC baut auf einem DNS *TXT* Eintrag für den Namen *_dmarc.example.com.*, um dessen Policy zu spezifizieren:

```
"v=DMARC1;p=reject;pct=100;rua=mailto:aggrep@example.com"
```

Abgesehen vom Protokoll und Versionsparameter, kennt DMARC zehn Parameter. Der Parameter *p* spezifiziert, wie mit Emails umgegangen wird, wenn Sie entweder die SPF- oder DKIM-Validierung nicht bestehen. Dessen Werte *none*, *quarantine* oder *reject*, haben eine ähnliche Bedeutung wie die SPF-Qualifizierer ?, ~ und -. Die Angabe dieses Parameters ist notwendig für die sachgemässe Funktion von DMARC. Der Parameter *sp* erlaubt das Setzen von separaten Policies für Subdomänen. Die Parameter *adkim* und *aspf* bestimmen, wie Email von Subdomänen behandelt wird, wenn Regeln für SPF und DKIM nur für die Hauptdomäne existieren. Die Parameter *rua* und *ruf* bestimmen, wohin DMARC-Berichte gesendet werden sollen. Erstere Adresse erhält aggregierte Berichte über ausgewertete Emails, während letztere Adresse für jede Auswertung einen Bericht erhält. Die Parameter *pct*, *rf* und *ri* erlauben das feine Einstellen des Verhaltens der DMARC-Policy. Zu beachten ist, dass die Parameter *p* und *pct* dazu verwendet werden können, um DMARC graduell zu aktivieren.

Eleanore Young

NUR WER BEREIT IST RISIKEN EINZUGEHEN

KANN DEN WEG ZUM ERFOLG FINDEN

Bildquelle: https://pixabay.com/photo-2671825/

VULNERABILITY SUMMARY

AUSGEWÄHLTE SCHWACHSTELLEN DES AKTUELLEN MONATS

1

CISCO WEB SECURITY APPLIANCE MALWARE PROTECTION ATTACHMENT BYPASS

Eine Schwachstelle wurde in Cisco Web Security Appliance ausgemacht. Sie wurde als kritisch eingestuft. Dies betrifft eine unbekannte Funktion der Komponente Advanced Malware Protection. Durch das Manipulieren durch Attachment kann eine erweiterte Rechte-Schwachstelle (Bypass) ausgenutzt werden. Technische Details oder ein Exploit zur Schwachstelle sind nicht verfügbar. Ein Exploit zur Schwachstelle wird momentan etwa USD $25k-$50k kosten.

https://vuldb.com/de/?id.109457

2

MICROSOFT WINDOWS 10/SERVER 2016 DEVICE GUARD ERWEITERTE RECHTE

Eine Schwachstelle wurde in Microsoft Windows 10/Server 2016 ausgemacht und betrifft das Device Guard Security Feature. Mittels dem Manipulieren mit einer unbekannten Eingabe kann eine erweiterte Rechte-Schwachstelle (Signature) ausgenutzt werden. Die Beschaffenheit der Schwachstelle lässt vermuten, dass ein Exploit momentan zu etwa USD $25k-$50k gehandelt werden wird. Sie lässt sich durch das Einspielen des Patches KB4048956 lösen.

https://vuldb.com/de/?id.109367

3

MICROSOFT EXCEL SECURITY FEATURE MACRO ERWEITERTE RECHTE

Eine Schwachstelle wurde in Microsoft Excel 2007 SP3/2010 SP2/2013 SP1/2013 RT SP1/2016 ausgemacht. Durch Makros kan sie ausgenutzt werden. Technische Details oder ein Exploit zur Schwachstelle sind nicht verfügbar. Ein Exploit zur Schwachstelle wird momentan etwa USD $5k-$10k kosten. Sie lässt sich durch das Einspielen des Patches KB4011197 lösen. Dieser kann von catalog.update.microsoft.com bezogen werden.

https://vuldb.com/de/?id.109385

4

AMAZON KEY CLOUD CAM 802.11 DEAUTHENTICATION FRAME DENIAL OF SERVICE

Es wurde eine problematische Schwachstelle in Amazon Key gefunden. Betroffen hiervon ist die Komponente Cloud Cam 802.11 Deauthentication Frame Handler. Dadurch kann eine Denial of Service-Schwachstelle ausgenutzt werden. Technische Details oder ein Exploit zur Schwachstelle sind nicht verfügbar. Die spezielle Ausprägung dieser Schwachstelle führt dazu, dass ihr ein historisches Interesse beigemessen werden kann.

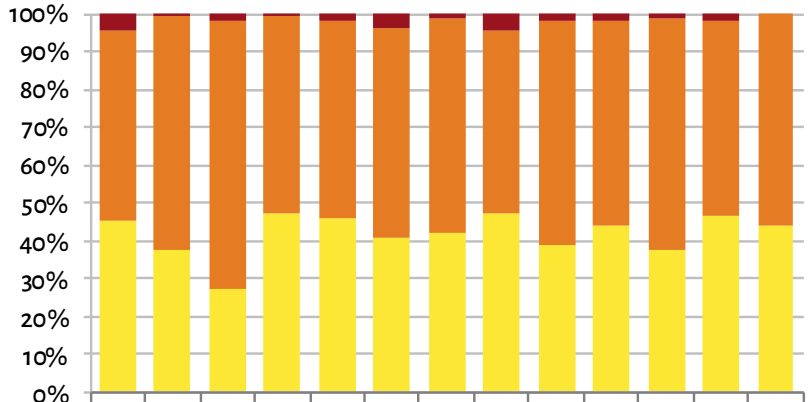
https://vuldb.com/de/?id.109569

VULNERABILITY LANDSCAPE

AKTUELLE STATISTIKEN AUS UNSERER VULDB

MEISTEXPONIERTE PRODUKTE IM VERGANGENEN MONAT

VERLAUF DER RISIKEN DER VERGANGENEN 12 MONATE



	Nov 16	Dec 16	Jan 17	Feb 17	Mar 17	Apr 17	May 17	Jun 17	Jul 17	Aug 17	Sep 17	Oct 17	Nov 17
sehr kritisch	28	2	23	5	28	56	9	48	32	26	15	28	0
kritisch	346	517	1056	499	934	895	646	525	1027	726	847	825	301
problematisch	313	312	406	454	830	658	472	512	678	591	527	737	238

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

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 DIE 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