MONTHLY SECURITY SUMMARY

AUSGABE OKTOBER 2022
MS CLOUD SECURITY UND WAFFENHANDEL

ABSICHERN VON MS CLOUD TENANTS

Durch unsere praktikablen Tipps wird es Ihnen möglich eine umfangreiche Absicherung Ihrer Microsoft Cloud-Umgebung vorzunehmen.

WAFFENHANDEL IM DARKNET

Konflikte wie in der Ukraine führen dazu, dass illegale Märkte im Darknet mit Waffen überschwemmt werden und so Kriminalität und Terrorismus befeuern können.

Oktober 2022: Wissensvermittlung

Johann Wolfgang von Goethe schrieb einmal: "Nichts ist schrecklicher als ein Lehrer, der nicht mehr weiss als das, was die Schüler wissen sollen." Viele Autoren, Dozenten und Lehrer begehen den Fehler, dass sie fortwährend ihre Überlegenheit demonstrieren wollen. Durch möglichst komplexe Gedankenkonstrukte soll in erster Linie der eigene Vorsprung aufgezeigt werden.

Das Vermitteln des Wissens und das Erweitern des Horizonts des Zuhörers tritt dabei in den Hintergrund. Aber nur weil eine Information verständlich ist, muss sie und deren Übermittler nicht von minderer Qualität sein. Die Schwierigkeit beim Lehren besteht nicht im Wissen von Details, sondern im Verständlichmachen von Ideen.

Was macht also eine gute Fachpublikation aus? Einerseits sind dies besonders neuartige, innovative und progressive Ideen. Albert Einsteins erste Aufsätze zur speziellen Relativitätstheorie gehören dazu. Aber gerade weil seine Sicht der Dinge so neu war, war sie nur wenigen Spezialisten zugänglich (teilweise nicht mal diesen; der Nobelpreis wurde ihm aus Unverständnis verwehrt).

Mit der Popularisierung des Neuen wird das Neue zum Alten, verliert aber dadurch nicht zwingend an Wert. Sigmund Freuds Schriften waren für damalige Verhältnisse besonders Populistisch. Ohne diesen Wesenszug hätten Worte wie Neurose oder Unbewusstsein keinen Einzug in den alltäglichen Sprachgebrauch halten können. Der moderne Mensch wäre sich den Hintergründen nicht in solchem Umfang bewusst, wie heute.

Marc Ruef
Head of Research

NEWS

WAS IST BEI UNS PASSIERT?

VORTRAG ZU VERTRAUEN IN AI AN SWISS CYBER STORM

Am 25. Oktober 2022 findet im Kursaal Bern die *Swiss Cyber Storm* statt, eine seit langem etablierte Sicherheitskonferenz, die die IT-Sicherheitsagenda für die Schweiz bestimmt. Unter dem Hauptthema *Digital Identities and How to Secure Them*, wird Marisa Tschopp einen Vortrag mit dem Titel *In AI We Trust?* halten. Tickets für den Event sind online erhältlich.

EXPERTENKOMMENTAR ZU RANSOMWARE-ANGRIFF AUF CHOCOLATIER

Ein bekannter Schokoladen- und Süssigkeitenhersteller in der Schweiz wurde Opfer eines Ransomware-Angriffs. Im Nachgang dessen wurden nun die Mitarbeiter darüber informiert, ebenfalls erweiterte Schutzmassnahmen im privaten Umfeld zu etablieren. Warum dieser Schritt erforderlich werden konnte, diskutieren die Journalisten Martin Schmidt und Patrik Berger mit Marc Ruef für den *Blick*.

VORTRAG ZU WINDOWS HARDENING AN BSIDES ZÜRICH

Die diesjährige BSides Zürich fand am 17. September statt. In der Morning Session wurde ein Vortrag von Mirjam Blumenstein und Michael Schneider mit dem Titel *Windows Hardening – How hard can it be?* gehalten. Michael Schneider leitet das Red Team bei scip AG und ist bekannt für seine Arbeiten in diesem Bereich, allen voran durch sein Toolkit *HardeningKitty*. Tickets zur Veranstaltung können online gekauft werden.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

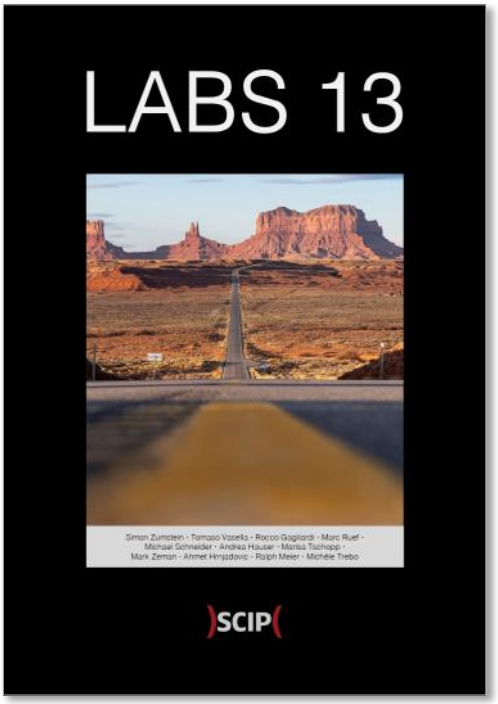
UNSER NEUES JAHRBUCH

Erneut veröffentlichen wir die aktuelle Ausgabe unseres Jahrbuchs. Bereits zum 13ten Mal fassen wir in diesem die Fachbeiträge von einem Jahr Forschung im Bereich Cybersecurity zusammen.

Das Buch ist wiederum sowohl in deutscher (ISBN 978-3-907109-30-4) als auch in englischer Sprache (ISBN 978-3-907109-31-1) verfügbar. Das Vorwort wurde von Dr. iur. David Vasella verfasst und setzt sich mit den rechtlichen Rahmenbedingungen der Informationssicherheit auseinander.

In unserem Katalog finden sich ebenfalls themenspezifische Bücher zu Künstlicher Intelligenz (ISBN 978-3-907109-14-4) und Sicherheit in der Hotellerie (978-3-907109-16-8).

Weitere Informationen auf unserer Webseite.



ISBN 978-3-907109-30-4 [de]
ISBN 978-3-907109-31-1 [en]

Bildquelle: https://pixabay.com/images/id-7465249/

MARIUS ELMIGER

MINIMIEREN DER ANGRIFFSFLÄCHE IHRES MICROSOFT CLOUD-TENANTS

Nachfolgend präsentieren wir die Top-10 risikoreichsten Microsoft-Cloud-Sicherheitskonfigurationen, welche wir während zahlreichen Security Assessment festgestellt haben. Microsoft hat Active Directory (AD) mit den Windows 2000 Server-Editionen im Jahr 2000 als Nachfolger des Windows-NT-Directory eingeführt. Und wie sich einige von Ihnen erinnern, war IT-Sicherheit zu diesem Zeitpunkt nicht immer das wichtigste Thema. Dies führte vor allem zu unsicheren Konfigurationen, wie z. B. zahlreiche Zuweisungen von Benutzerkonten zu privilegierten Gruppen wie zu den Domain Admins.

Im Laufe der Jahre wurden jedoch schlechte AD-Sicherheitspraktiken reduziert, da es zum Standard wurde, dass AD besser geschützt werden muss. So wurde es beispielsweise zur gängigen Praxis, eine minimale Anzahl dedizierter Domain-Admin-Konten einzurichten, die nur innerhalb ihrer zulässigen Security-Boundary arbeiten dürfen. Warum erzählen wir Ihnen das? Weil es sich bei Cloud-Assessments manchmal so anfühlt, als ob man mit einer Zeitmaschine ins Jahr 2000 zurückreist, um dieselben Fehler zu sehen, die in dieser Zeit gemacht wurden.

DIE TOP-10 RISIKOREICHSTEN KONFIGURATIONEN

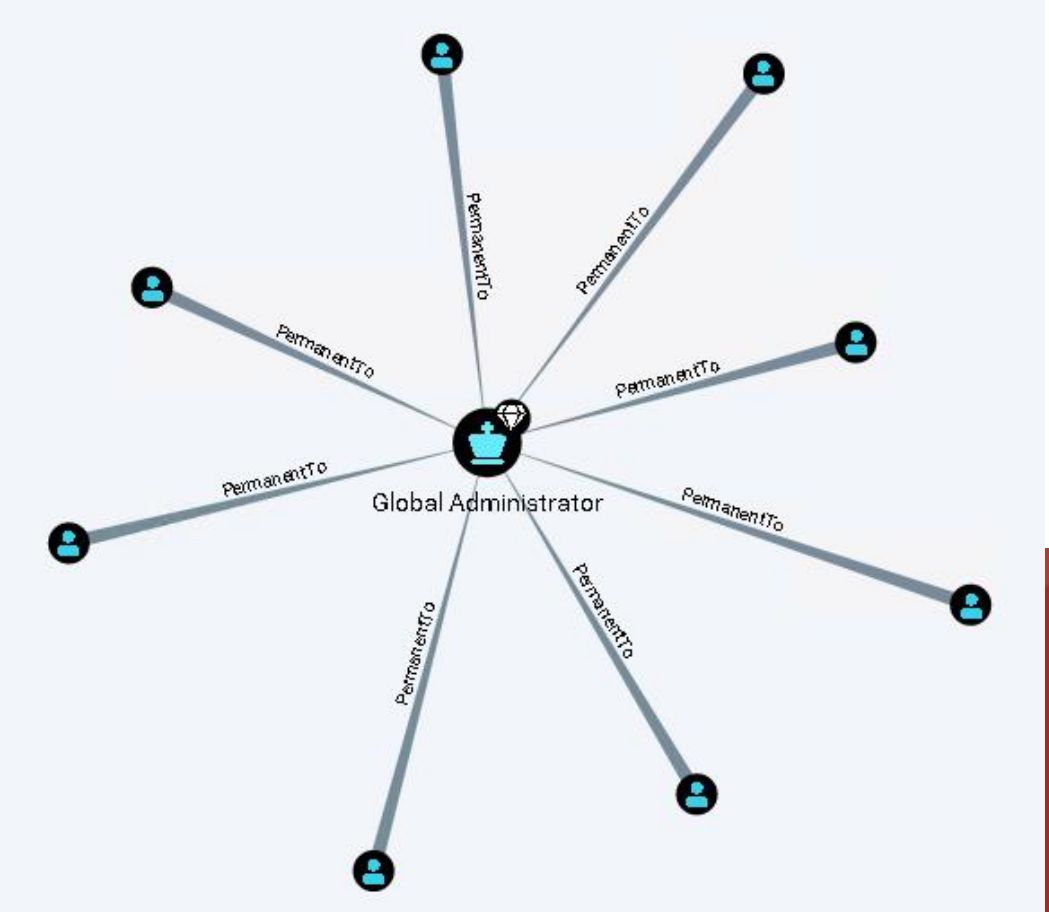
Die folgende Top-10-Liste bringt Sie "zurück in die Zukunft", indem diese grundlegende riskante Konfigurationen oder Praktiken beschreibt, die vermieden werden sollten. Ausserdem finden Sie eine Liste mit Links und Quellen für weiterführende Informationen. Die identifizierten Risiken basieren auf unseren Erfahrungen aus verschiedenen Microsoft Cloud Assessments.

Risk 1 – Reguläre Benutzerkonten, welche der Global Administratoren Rolle zugewiesen sind

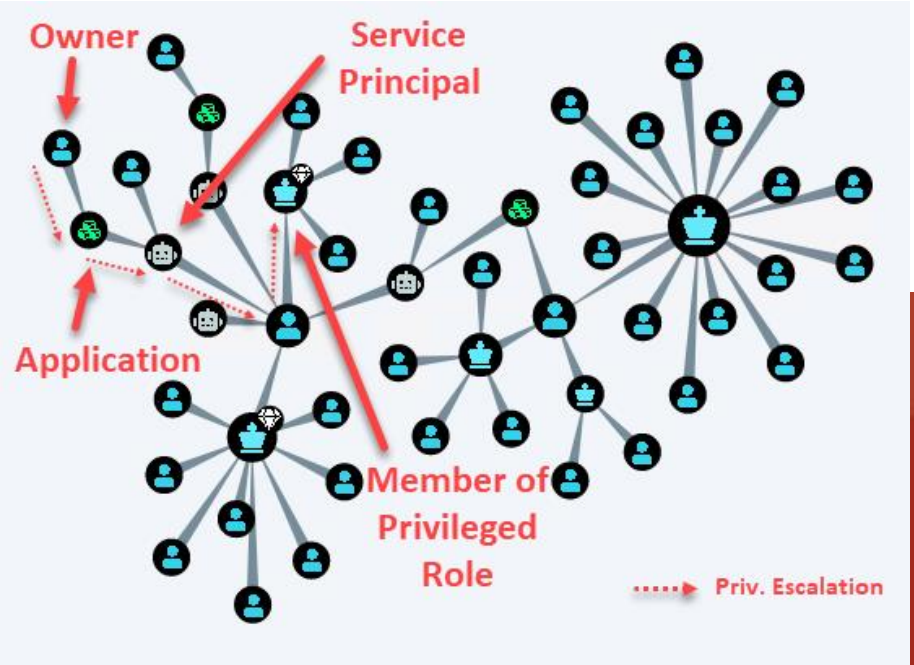
Vergleicht man alle unsere Microsoft Cloud-Assessment der letzten Jahre, so hatten 8 von 10 ein oder mehrere reguläre Benutzerkonten, die permanent an Tier-0 Rollen in Azure AD zugewiesen waren. Tier-0-Rollen in der Cloud können als alle Rollen oder Entitäten interpretiert werden, die direkt oder indirekt zu Global Adminstrators werden können, wie zum Beispiel Mitglieder der Privilege Role Administrators oder Identitäten mit der AppRole RoleManagement.ReadWrite.Directory. Bei den entdeckten regulären Benutzerkonten handelte es sich hauptsächlich um Hybrid Identities, die aus dem Active

Directory synchronisiert wurden. Der Grund für die Zuordnung war oft Bequemlichkeit, Unwissenheit oder die Angst, aus dem Azure AD ausgesperrt zu werden. Überraschenderweise versuchen die Unternehmen üblicherweise, dem Active Directory-Least-Privilege-Konzept zu folgen, indem sie beispielsweise ein dediziertes Konto verwenden oder sogar das Microsoft-Tiering-Modell zur Verwaltung Ihres Active Directory's anwenden. Für die Microsoft-Cloud wurde dieses Prinzip jedoch nicht mehr angewandt.

Die Verwendung regulärer Benutzerkonten für die Verwaltung von Tier-0 vergrössert die Angriffsfläche unnötig und kann zu einer Kompromittierung des Microsoft-Cloud-Tenants führen. Angreifer werden versuchen, die Sicherheitsausnahmen zu missbrauchen, die meist für reguläre Benutzerkonten gelten, z. B. unlimitierter Internetzugang, Passwortrücksetzfunktionen, Social Engineering, laxe Härtungsmassnahmen, MFA-Fatigue Attack und weitere. Daher empfehlen wir, sich an das Least Privilege Modell zu halten, indem Sie dedizierte Cloud-only-Benutzerkonten für die Verwaltung der Microsoft Cloud verwenden. Die Tier-0 Cloud-Only-Benutzerkonten müssen Teil eines Joiner-Mover-Leaver (JML)-Prozesses sein. Ein manueller JML-Prozess, z. B. in Form eines Tickets, reicht aus, um zu vermeiden, dass ein IAM-System zu Tier-0 hochgestuft werden muss, da die Anzahl der Tier-0 -Benutzerkonten gering gehalten werden sollte. Das



Argument, dass Hybrid Identities bereits in den JML-Prozess einbezogen sind, ist nicht immer stichhaltig. Es kann zu dem oben beschriebenen Szenario führen, bei welchem reguläre Benutzerkonten Tier-0 Entitäten zugewiesen werden, da Active Directory Tier-0-Benutzer meist nicht in die Cloud synchronisiert werden. Angenommen, Azure AD Hybrid Identities müssen zwingend aus einem Grund für Tier-0 Cloud Berechtigungen verwendet werden. In diesem Fall empfehlen wir, ein dediziertes Active Directory-Identitätsmuster für die Hybrid Idenities zu erstellen und dieses wiederum in einen JML-Prozess einzubinden. Auf diese Weise können für diese Hybrid Identities restriktive Zugriffsrichtlinien im AD und in der Cloud festgelegt werden. Zusätzlich empfehlen wir die Verwendung von der Microsoft Cloud Lösung Privilege Identity Management (PIM) für privilegierte Konten. Um die Rolle zu aktivieren, sollte Multifaktor-Authentifizierung (MFA) verwendet werden.



Reguläre Benutzerkonten, welche dauerhaft der Global Administrator Rolle zugeordnet sind

Risk 2 – Schwaches Azure AD Service Principal und Cloud Application Management

Service Principals repräsentieren die Identität einer Microsoft Cloud Application. Ein neu angelegter Azure AD-Tenant mit entsprechenden Lizenzen hat etwa 390 vorkonfigurierte Service Principals, welche die Cloud-Application wie Microsoft Teams, SharePoint Online, Exchange Online oder Microsoft Graph repräsentieren. Wenn beispielsweise eine benutzerdefinierte Microsoft-Cloud-Anwendung im Azure AD-Portal oder über die API erstellt wird, werden zwei Entitäten erstellt: eine Application und ein Service Principal. Die Application Objekt ist die globale Repräsentation der Unternehmens-Applikation für alle Tenants, während der Service Principal die lokale Repräsentation eines bestimmten Tenants ist. Service Principals oder Managed Identities in Azure ARM werden auch für die IaaS- und PaaS -Dienste von Azure genutzt, um beispielsweise für neue Dienste, bestehende Dienste oder allge-

mein für Automatisierungsaufgaben. Die Kompromittierung von Service Principals ist ein interessantes Ziel für Angreifer. Service Principals können mit einer Vielzahl von Berechtigungen ausgestattet werden und sind ideal für Privilege Escalation Szenarios oder Backdooring von Azure AD oder Azure ARM.

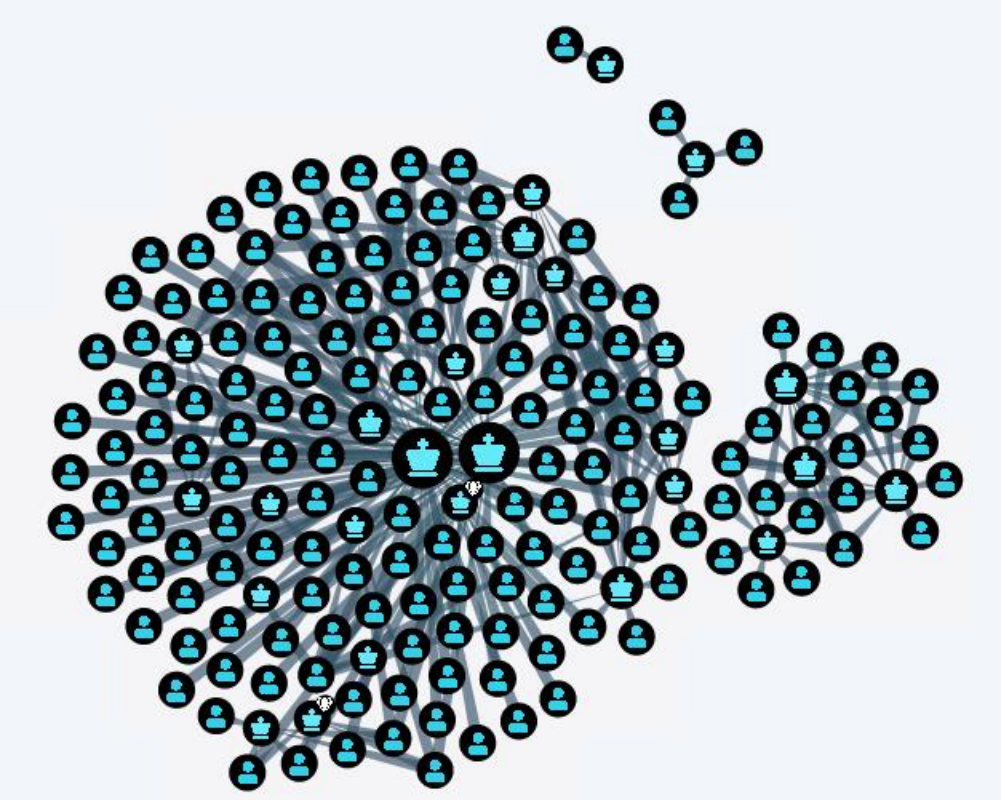
Cloud-Application werden durch die Zusammenstellung verschiedener IaaS- und PaaS-Services erstellt. Ein Application in der Microsoft Cloud ist in der Regel ein Service Principal zugewiesen. Wenn eine Application beispielsweise Zugriff auf eine Datenbank benötigt, wird dem Service Principal der Anwendung der Zugriff auf die Datenbank gewährt. Anwendungsnutzer greifen in der Regel über OAuth 2.0 Authorisation Flows auf Cloud-Applications zu. Die Erteilung von Berechtigungen für Applications kann kritisch werden, da einige Applications hoch privilegierte Zugriffsrechte haben können.

Häufig bei unseren Assessments finden wir privilegierte Service Principals oder Cloud-Application mit einem alltäglichen Benutzerkonto als Owner. Ein Owner kann den Service Principal verwalten oder sich als solcher ausgeben. Wenn also ein Benutzer eine Anwendung mit höheren Privilegien als der Benutzer selbst steuern kann, ist eine Privilege Escalation über den Service Principal möglich. Neben der Ownership stellen wir auch häufig fest, dass zugewiesene Berechtigungen nicht aktiv überwacht werden. Häufig finden wir über privilegierte Service Principals mit Anwendungsrollenrechten wie *.ReadWrite.All, *.ReadWrite.Directory oder direkte Zuweisungen zu den Rollen Global Administrator oder Exchange Administrator. Die Überprüfung, wer Applications verwalten kann, einschliesslich Applications- und Delegationsberechtigungen, ist in einer Microsoft-Cloud-Umgebung von entscheidender Bedeutung, um unerwünschte Credential-Pivoting-Pfade zu verhindern. Beispielsweise sollte der Besitzer von privilegierten Service Principals oder Applications niemals ein reguläres Benutzerkonto sein.

Risk 3 – Zu viele Administratoren

Allzu oft ist ein Ergebnis eines Microsoft Cloud Assessment, dass der Microsoft Cloud Tenant zu viele Administratoren hat. Sei es in Azure AD, Azure ARM, Azure DevOps oder M365. Die Gründe dafür sind vielfältig, aber einer der Gründe für diese Praxis ist meistens, dass verschiedene IT-Teams mit unabhängigen Projekten und engen Zeitplänen die Microsoft

Cloud administrieren. Das Ergebnis sind viele Administratoren, die beispielsweise Conditional Access, Azure AD-Berechtigungen, Service Principals, Azure ARM-Ressourcen und so weiter konfigurieren müssen. Silos sollten in der Cloud keinen Platz haben, da alles viel stärker miteinander verbunden ist als bei On-Premises IT Lösungen. Fehlkonfigurationen können schwerwiegende Folgen haben. Daher ist es wichtig, einen Plan zu haben, um zu vermeiden, dass projektbezogene Benutzerkonten zufälligen Rollen zugewiesen werden, ohne die Auswirkungen der Berechtigungen oder die daraus resultierenden Zugriffsrechte zu verstehen. Ähnlich wie bei Active Directory sollte die Anzahl der Administratoren auf ein Minimum beschränkt werden.



Risk 4 – Riskante Ausnahmen für Global Administrators oder andere privilegierte Rollen

Wir haben in jedem Microsoft-Cloud-Assessment Ausnahmen gefunden, insbesondere für Global Administrator in Conditional Access Regeln. Leider ist die Begründung allzu oft die Umgehung von Sicherheitskontrollen oder ein Shortcut, um Zeit zu sparen. Insbesondere für privilegierte Rollen wie Global Administrator sollten keine Ausnahmen gemacht werden, mit einer Ausnahme: Breakglass-Konten.

Manchmal werden für reguläre Benutzerkonten Ausnahmen benötigt. In diesem Fall empfehlen wir die Verwendung der Microsoft Cloud-Funktion Access Review, sobald eine Ausnahme erforderlich ist. Zugriffsüberprüfungen können für eine bestimmte Azure AD-Gruppe festgelegt werden, die beispielsweise eine monatliche Überprüfung aller Gruppenmitglieder, die Teil der Ausnahme sind, erzwingt. Das Ziel sollte

Base protection - All apps: Require MFA and Compliant Device

Applies to	**Including**: All users **Excluding**: Users in groups: _m365-CondAccessExclude Users in roles: Global Administrator
Applications	**Including**: All applications
Controls	**Requirements (all)**: Mfa, RequireCompliantDevice

sein, die Ausnahme in naher Zukunft durch eine sicherere Lösung zu ersetzen.

Risk 5 – Fehlende Management Einschränkungen für privilegierte Rollen

Die sichere Cloud-Verwaltung wurde häufig in unseren Assessments als nicht vorhanden eingestuft. Wir kamen häufig zum Schluss, dass die Anmeldung mit dem Global Administrator oder anderen privilegierten Rollen von jedem Gerät aus möglich war. So wurde beispielsweise nur das M365-Portal durch Conditional Access eingeschränkt, nicht aber das Azure AD Portal oder der alte Azure AD Graph Explorer. Warum? Weil häufig das Projektteam Conditional Access einrichtete z.B. nur für M365, nicht aber für Azure ARM zuständig war (Silo Mentalität, welche vermieden werden sollte). In der Vergangenheit gab es nur wenige Möglichkeiten, der Management Zugriff auf die Microsoft Cloud zu beschränken. Wir empfahlen meistens, die Verwaltung nur von einem bestimmten Unternehmens-Admin-Proxy mit einer dedizierten öffentlichen IP-Adresse aus zuzulassen. Heutzutage lässt sich mit Conditional Access jedoch festlegen, auf welchem Gerät sich ein Benutzer mit einer bestimmten Rolle anmelden darf. Daher empfehlen wir dringend Privileged Access Workstations (PAW) in Kombination mit Conditional Access zu verwenden, zumindest für Tier-0-Administratoren.

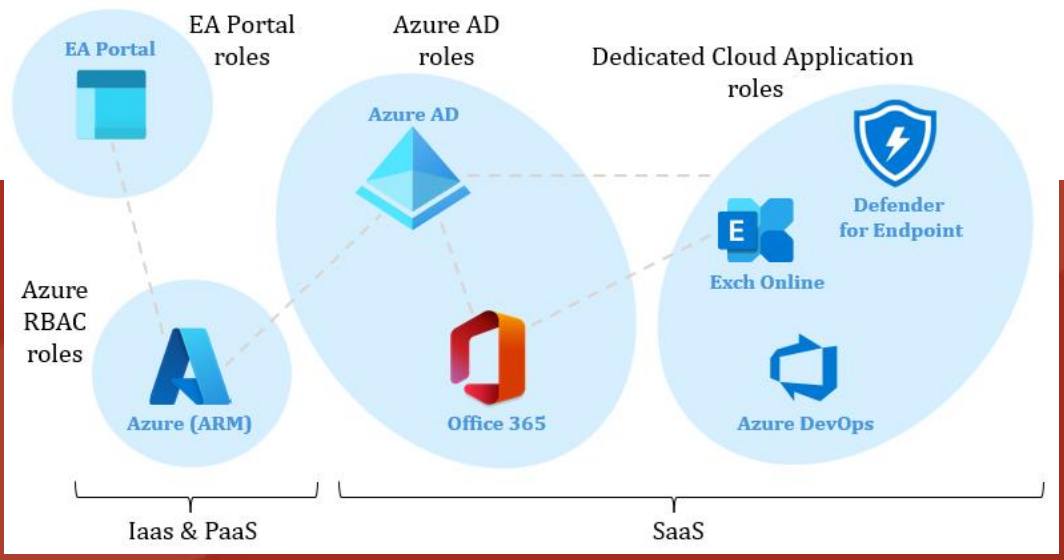
Risk 6 – Wissenslücken

Bei Assessments stellen wir oft fest, dass das zuständige IT-Personal Wissenslücken in Bezug auf die Funktionsweise der Microsoft Cloud hat. Das geht Hand in Hand mit der Silo-Mentalität, die unserer Meinung nach in einem Cloud-Setup nicht förderlich ist. Ein häufig missverstandenes Beispiel sind die verschiedenen Rollentypen in der Microsoft-Cloud. Zusammengefasst kennt die Microsoft-Cloud-Architektur vier Hauptorte, an denen Rollen zu finden sind. Der erste Ort ist der Azure Resource Manager (ARM), der IaaS- und PaaS-Workloads hostet. Die Rollen an diesem Ort werden als Azure RBAC-Rollen bezeichnet und gewähren Zugriff auf verschiedene Dienste wie Virtual Machines, Storage Accounts, Key Vaults und mehr. Der zweite Standort ist Azure AD. Azure AD verwaltet übergeordnete Rollen, welche direkten und indirekten Zugriff auf ARM- und SaaS-Anwendungen haben. Die mächtigste Rolle in der Microsoft-Cloud, der Global Administrator, ist hier zu finden. Diese Rolle kann alle Entitä-

ten in einem Tenant kontrollieren. Die meisten Rollen in Azure AD haben den Zweck, M365 zu verwalten. Der dritte Standort sind Rollen innerhalb von Cloud-Anwendungen. Als Beispiel in Cloud Applications wie Microsoft Graph, Exchange Online, Defender for Endpoint oder Azure DevOps. In solchen Rollen können manchmal Azure AD-Rollen, Gruppen, Service Principals oder Benutzer als Mitglieder gefunden werden. Der letzte Ort ist das Azure EA-Portal, in dem die Subscriptions für ARM verwaltet werden, wenn Ihr Unternehmen eine Enterprise Agreement hat. Der Enterprise Administrator und der Account Owner im EA-Portal haben vollen indirekten Zugriff auf alle Subscriptions, welche vom EA-Portal verwaltet werden. Die Rollen in Cloud Applications und des EA-Portals werden oft übersehen und fehlen daher in den Prozessen vom Identity & Access Management (IAM). Angreifer können solche Rollen nutzen, um unbemerkt zu bleiben, und können so weitreichenden Zugang zu verschiedenen Cloud-Diensten erhalten. Wir empfehlen daher, solche Rollen in die IAM-Prozesse aufzunehmen. Für das EA-Portal sollten nur dedizierte Microsoft Cloud Work Accounts verwendet werden, und es sollte sichergestellt werden, dass ähnliche organisatorische und sicherheitstechnische Massnahmen wie bei anderen privilegierten Konten, z. B. Global Administrators, angewendet werden.

Risk 7 – AAD Connect Missverständnisse

AAD Connect ist eine lokale Lösung, die Identitäten aus Active Directory mit der Microsoft Cloud synchronisieren kann. Die synchronisierten Objekte in der Cloud werden als Hybrid Identity bezeichnet. Der JML-Prozess, der bereits in der bestehenden lokalen IAM-Lösung implementiert ist, ist somit angeblich gewährleistet. Leider ist dies nicht wirklich der Fall, da AAD Connect nicht alle Cloud-Entitäten wie Cloud -Only-Benutzer, Gastkonten und Service Principals verwalten kann. Diese Entitäten werden meist vergessen und erfordern ebenfalls einen JML-Prozess. Daher sollte ein Konnektor, vorzugsweise über die Microsoft Graph API, eingerichtet werden, um nicht synchronisierte Entitäten abzudecken. Ausserdem muss die AAD Connect-Lösung



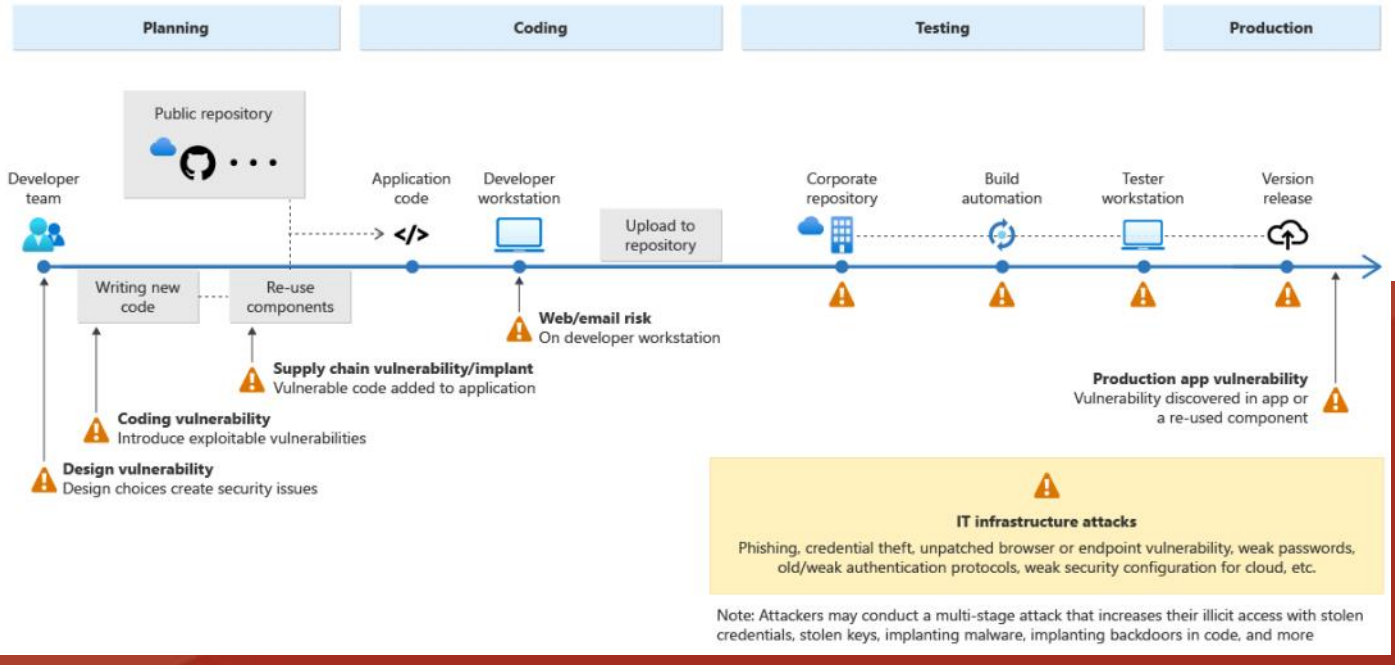
als Tier-0-Lösung behandelt und sollte daher nur von Tier-0-Administratoren des Active Directory verwaltet werden.

Risk 8 – DevOps Lösungen und ihre versteckten Risiken

Im Artikel Attack Path Analysis – Vorteil gegenüber Angreifern verschaffen haben wir einen möglichen Attack Path beschrieben, welcher ein reguläres Benutzerkonto in Azure DevOps missbraucht, um Zugriff auf einen privilegierten Service Principal zu erhalten. Um solche Attack Paths zu verringern, empfehlen wir sicherzustellen, dass ähnliche organisatorische und sicherheitstechnische Massnahmen wie bei anderen privilegierten Konten, z. B. Global Administrators, angewendet werden. Überdies sollte die verwendete DevOps-Lösung gemäss den verfügbaren Sicherheitsempfehlungen gehärtet werden.

Risk 9 – Fehlende Anwedungen vom Clean Source Principal

"Beim Clean Source Principle müssen alle Sicherheitsabhängigkeiten genauso vertrauenswürdig sein wie das zu sichernde Objekt." (Microsoft – Clean source principle). In On-Premises-Umgebungen und erst recht in der Cloud wird dieses grundlegende Prinzip oft vergessen/ignoriert. Eine häufig vorgebrachte Begründung bei unseren Assessments lautet: "Unser Microsoft Cloud Tenant ist noch nicht produktiv", was offensichtlich gegen das eben genannte Prinzip verstösst. Ein Azure AD Tenant ist unserer Meinung nach produktiv, sobald der Azure AD Tenant auf der Microsoft Website angefordert wird. Daher sollten die Prinzipien wie Least Privilege und Clean Source von Anfang an beachtet werden. Wer kann sonst garantieren, dass der Tenant nicht während des Einrichtungsprozesses oder der Pilotphase kompromittiert wurde?



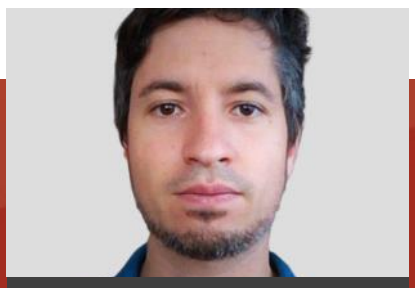
Risk 10 – Fehlende Cloud-Verteidiger/Angreifer Denkweise

Die alte Sicherheitsarchitektur vor dem Cloud Computing ähnelt der Struktur einer mittelalterlichen Burg. Alles befand sich in einem vertrauenswürdigen internen Netz, und alle Sicherheitskonfigurationen waren um den Burgrand herum angeordnet. Mit Cloud Computing ist diese Architektur mehr und mehr obsolet geworden. Ausserdem ist das Konzept der Perimetersicherheit nicht praktikabel, wenn die Dienste auf einer gemeinsam genutzten, mit dem Internet verbundenen Infrastruktur laufen. Um diese neuen Herausforderungen zu bewältigen, sind innovative Modelle für die Sicherheitsarchitektur und eine Änderung der Denkweise erforderlich. Ein Beispiel für eine fragwürdige Denkweise ist, wenn die Begründung für eine Sicherheitsfeststellung lautet: “Aber Microsoft kümmert sich schon darum”. Leider ist mit einer solchen Denkweise die Wahrscheinlichkeit einer Kompromittierung hoch. Vereinfacht ausgedrückt bedeutet die Kultivierung der Denkweise eines Verteidigers, dass man versteht, wer für was in einer Cloud-Umgebung verantwortlich ist. Laut Microsoft sind “Cloud-Dienste eine geteilte Verantwortung”. Aus der Sicht von Microsoft bedeutet “gemeinsam”, dass Microsoft die Plattform und die Tools zur Verfügung stellen, die Konfiguration, Überwachung und Sicherung des Tenants obliegt, aber Ihnen. Daher ist es von entscheidender Bedeutung, ein umfassendes Verständnis dafür zu haben, wie ein Microsoft Cloud Tenant gesichert, überwacht und verwaltet werden muss. Regelmässige Konfigurationsüberprüfungen und -anpassungen mit der Unterstützung von Microsoft-Sicherheitstools wie Microsoft Secure Score, Defender for Cloud Recommendations, Azure Monitor Workbooks und anderen werden empfohlen. Auch die Verwendung von Assessmenttools von Drittanbietern wie AzureHound, ROADtools, AzureADAssessment oder AAD Internals, um nur einige zu nennen, kann bei einem Assessment der Sicherheitslage eines Azure AD Tenant von Nutzen sein.

Der Grundsatz des Clean Source Principal sollte beachtet werden. Verwendete Tools sollten zuerst überprüft und möglichst mit den geringsten benötigten Privilegien verwendet werden.

FAZIT

Die präsentierten Top-Ten-Risiken sind nicht als abschliessend zu betrachten, da die Liste um weitere risikoreiche Aspekte ergänzt werden könnte, z. B. fehlende Sicherheitsüberwachung, Unkenntnis über Credential Pivoting und Extraktion von Access- oder Refresh-Tokens aus Browser-Sitzungen. Nichtsdestotrotz wollten wir Ihr Bewusstsein für bewährte Sicherheitspraktiken schärfen, denn in der Cloud ist die Einhaltung dieser Praktiken noch wichtiger als im On-Premises Umfeld. Die Befolgung von Sicherheitsstandards ist ein guter Ratschlag für den Betrieb von Cloud-Plattformen, da diese ohne Härtungsmassnahmen und kontinuierliche Sicherheitsanpassungen standardmässig nicht sicher sind. Alles in allem unterscheiden sich die Grundlagen der Sicherung einer Cloud-Umgebung nicht wesentlich von der Sicherung einer On-Premises Umgebung. Daher ist es wichtig, die Fehler der Vergangenheit nicht zu wiederholen und in ein solides Fundament zu investieren, bevor die umfangreichen und lukrativen Möglichkeiten einer Cloud-Plattform genutzt werden.



Marius Elmiger

Next Level Cyber Threat Intelligence

Cyber Threat Intelligence ist darum bemüht, Trends bei Angriffen auf Computersysteme zu erkennen und vorauszusagen. Dadurch können Attacken antizipiert und frühzeitig abgewehrt werden.

)SCIP(

https://www.scip.ch

MICHÈLE TREBO

WAFFEN AUF DEM ILLEGALEN MARKT

Wie die Neue Zürcher Zeitung anfangs Mai 2022 in einem ihrer Artikel erklärt, lieferte der Westen bereits vor Kriegsbeginn tragbare Systeme wie Pistolen, Sturmgewehre, Granatwerfer, Panzer- und Flugabwehrraketen an die ukrainische Grenze. Dazu kamen schwere Waffen mit komplexen und personalintensiven Systemen wie Panzer, Kampfhelikopter oder Artilleriesysteme.

Die nachfolgende Liste von Waffensystemen, die im Russland-Ukraine-Konflikt auf beiden Seiten zum Einsatz kommen, ist nicht abschliessend.

HAUBITZE M777

Das gezogene 155-Millimeter-Schleppartilleriegeschütz wird von der Global Combat Systems Division von BAE Systems im Vereinigten Königreich hergestellt und ist seit 2005 in Verwendung. Ob zu Lande, zu Wasser oder in der Luft, es zeichnet sich besonders durch seine Zuverlässigkeit und Mobilität aus. Je nach Munition beträgt die Reichweite 24 – 40 Kilometer und benötigt ein Begleitfahrzeug. Wird ein M107-Projektil eingesetzt, kommt das Geschütz 24 Kilometer weit, mit einem ERFB-Geschoss 30 Kilometer. Das M795-Projektil ist als die tödlichere Version des M107-Projektils mit grösserer Reichweite konzipiert und erreicht 28.7 – 37 Kilometer. Am weitesten kommt das M982 Excalibur mit 40 Kilometern. Mittels Feuerkontrollsystem kann die M777 unabhängig von einer Feuerleitstelle schiessen. Da bei der Konstruktion der M777 Titan verwendet wurde, weisst sie lediglich ein Gewicht von 4,2 Tonnen auf und kann so einfach und schnell transportiert werden. Dies und auch die Risiken, keinen Sprengfallen ausgesetzt zu sein, maximiert die Überlebenschancen. Für die Haubitze M777 spielt das Gelände oder Hindernisse keine Rolle, weshalb sie über grosse Entfernungen eingesetzt werden kann. Das Geschütz wird von den Bodentruppen Australiens, Kanadas, Indiens, Saudi-Arabiens, der Vereinigten Staaten und auch Ukrainens eingesetzt. Ukrainische Militärangehörige müssen allerdings erst auf dem amerikanischen Truppenübungsplatz Grafenwöhr in der Oberpfalz (Deutschland) in deren Handhabung geschult werden, bevor sie die Haubitze bedienen können.

ISKANDER-M

Den ballistischen Raketen russischer Bauart mit Kurzstreckenraketensystem gelingt es, 400 Kilome-

ter entfernte Ziele zu treffen. Die Reichweite ist auf 500 Kilometer erweiterbar. Ihre Flughöhe beträgt 6 bis 50 Kilometer. Russische Streitkräfte konnten so zu Beginn des Russland-Ukraine-Konflikts von heimischem Boden aus die Ukraine angreifen. Die Raketen können von einem Lastwagen aus schnell befestigt werden. Wurden sie einmal gestartet, können sie ihre Flugbahn so schnell anpassen, dass ihr Ziel schwer berechenbar ist und somit auch gegnerische Flugabwehrsysteme sie nicht stoppen können. Sie manövrieren während des Fluges ständig. Die Iskander-M wurde ausschliesslich für das russische Militär entwickelt. Neben dem Modell Iskander-M gibt es auch die Modelle Iskander-E und Iskander-K. Bei der Iskander-E handelt es sich um eine Exportversion mit einer Reichweite von 280 Kilometern. Die Iskander-K ist eine neue Version mit neuen Marschflugkörpern R-500 und ebenfalls einer Reichweite von 280 Kilometern.

JAVELIN-FGM-148

Die hochwirksame, handliche, infrarotgelenkte Panzerabwehrlenkwaffe gilt als das meistgelieferte System im Russland-Ukraine-Konflikt. Durch ihr geringes Gewicht von nur 20 Kilogramm kann sie von der Schulter aus abgefeuert werden und so Ziele in bis zu 2,5 Kilometern Entfernung bekämpfen. Neben Kampfpanzern und Militärfahrzeugen können die Raketen auch gegen Bunker oder Hubschrauber eingesetzt werden. Die Javelin kommt hauptsächlich aus Amerika, wird aber auch von Frankreich, Polen oder Grossbritannien geliefert.

KAMOW KA-52

Der russische Hochleistungskampfhelikopter zeichnet sich besonders durch seine zwei Doppelrotoren mit je drei Rotorblättern, die in entgegengesetzter Richtung drehen, aus. Dank dieser Rotoren braucht der Kampfhelikopter keinen Heckrotor, ist sehr beweglich und schnell und kann vertikal bis zu 4 Kilometer steigen. Ausserdem kann er bei Tag und Nacht operieren. Der Zweiplätzer ist die weiterentwickelte Version des einsitzigen Ka-50. Besonders eignet sich der Ka-52 für Aufklärungsmissionen, Zielbezeichnung und Luftangriffe im Gruppenverband. Das Cockpit ist gegen Flak-Geschosse bis zum Kaliber 20 Millimeter gepanzert. Allerdings ist der Helikopter gegen schultergestützten Flugabwehrraketen machtlos und kann somit leicht abgeschossen werden. Er ist mit dem Datenlink-System Breeze ausge-

rüstet und kann damit Video-, Bild- und Radardaten in Echtzeit zu anderen Kampfhelikoptern übermitteln. Weiter verfügt er über ein Gyrostabilised-Optical-Electronic-System mit verschiedenen TV-, RLV- und WBG-Kameras, Laserzielbeleuchtung und Entfernungsmesser. Mit dem Multifunktionsradar FH01 Arbalet können Luft-, Boden- und Seeziele bis zu 15 Kilometern geortet und Lenkwaffen ins Ziel geführt werden.

T-72

Der sowjetische Kampfpanzer ist klein und mit 40 Tonnen Gefechtsgewicht leicht. Um ihn zu bedienen, braucht es drei Personen. Der Panzer ist mit einer 125-Millimeter-Kanone ausgestattet. Die Ladeautomatik des Panzers lädt die Geschosse in weniger als drei Sekunden nach. Die Beladung besteht aus 44 Schuss, wobei 22 davon in einem Ladekarussell im Wannenboden unter dem Turm und der Rest an verschiedenen Plätze im Innenraum aufbewahrt werden. Wird der Panzer getroffen, so gibt es kaum ein Entkommen für die Besatzung, denn diese sitzt in unmittelbarer Nähe zur Munition. Ursprünglich wurde der T-72 von der Sowjetarmee eingesetzt. Die Ukraine bekam von Tschechien, Polen und der Slowakei Lieferungen, aber auch auf seitens der Russen wird der Kampfpanzer eingesetzt. Aufgrund der vielen Exporte kommt der Panzer häufig zum Einsatz, darunter auch in vielen Nahost-Staaten.

BM-21 GRAD

Der sowjetische Mehrfachraketenwerfer, der auf einem Lastwagen montiert ist, kann 40 Raketen ohne Nachladen von 2.87 Metern Länge verschiessen und ist in drei Sekunden schussbereit. Die Raketen können einzeln in kleinen Gruppen in Intervallen oder alle 40 innerhalb von zwanzig Sekunden verschossen werden. Danach dauert das Nachladen etwa zehn Minuten. Da der BM-21 Grad maximal zwei Minuten braucht, um seine Stellung zu verlassen, können in weniger als sechs Minuten alle 40 Raketen abgeschossen werden. Dies macht es den Feinden schwierig, ihn anzugreifen. Weiter benötigt man wegen der Streuung der Einschläge eine grosse Zahl Raketen, um sein Ziel zu treffen. Haubitzen sind somit genauer als der Grad. Seinen ersten Kampfeinsatz war 1969 im sino-sowjetischen Grenzkonflikt. 2003 wurde in Russland dann eine neue Version mit verbessertem Kampfwert präsentiert. D. h. Satellitennavigation, automatisches Feuerkon-

trollsystem und neuer Raketentyp, der bis zu 40 Kilometer weit schiesst. Was aber im Vergleich zu neueren Raketenwerfern immer noch gering ist. Der BM-21 Grad wird in über sechzig Ländern eingesetzt, darunter auch Russland und die Ukraine.

HAUBITZE 2000

Die Panzerhaubitze 2000 gilt als das modernste Artilleriegeschütz und wird in Deutschland hergestellt. Sie muss von fünf Personen bedient werden, ausser bei automatisiertem Munitionsfluss, wobei drei Personen reichen. Das selbstfahrende Geschütz ist auf einer Panzerwanne mit Kettenantrieb gebaut und kommt je nach Munition 30 bis 40 Kilometer weit. Es können bis zu sechs Granaten so abgefeuert werden, dass sie fast zeitgleich im Ziel einschlagen. Das Ziel wird digital von einem Leitstand übermittelt. Die Ukraine bekam von Deutschland insgesamt sieben Haubitzen und von den Niederlanden fünf.

STINGER

Die Boden-Luft-Rakete Stinger wurde in Amerika gebaut und für die Bekämpfung von tief fliegenden Flugzeugen und Helikoptern konzipiert. Um das Ziel erfassen und die Rakete von der Schulter abfeuern zu können, braucht es zwei Personen. Nach dem Abfeuern navigiert sich die Rakete selbstständig zu ihrem Ziel. Sie orientiert sich an dem Infrarotlicht, das von Triebwerken erzeugt wird und verfolgt so den Flugkörper. Die Stinger kann Ziele in bis zu 6 Kilometern Entfernung und 3 Kilometern Höhe treffen. Seit Beginn des Russland-Ukraine-Konflikts wurde die Flugabwehrrakete von den USA, Deutschland, Lettland und den Niederlanden an die Ukraine geliefert.

SWITCHBLADE-DROHNE

Die sogenannte Kamikaze-Drohne zerstört sich selbst, sobald sie ihr Ziel trifft und ist somit selbst die Waffe. Sie kann ohne Besatzung bis zu zehn Minuten in der Luft verweilen, bis sie ihr Ziel im Sturzflug ansteuert und explodiert. Die amerikanische Drohne kann vom Boden aus manuell gesteuert oder so programmiert werden, dass sie ihr Ziel selbst detektiert. Kurz vor der Detonation kann die Drohne noch gestoppt werden. Die amerikanische Drohne gibt es in zwei verschiedenen Ausführungen. Die Switchblade 300 hat eine Reichweite von 10 Kilometern und kann sich fünfzehn Minuten in der Luft halten. Die Switch-

blade 600 hat eine Reichweite von 40 Kilometern, kann vierzig Minuten fliegen und ist im Gegensatz zur Switchblade 300 auch zur Bekämpfung von gepanzerten Objekten geeignet. Es wurden über 700 Switchblade-Drohnen in die Ukraine geliefert.

CAESAR-HAUBITZE

Die französische, selbstfahrende, ungepanzerte Haubitze hat ein Kaliber von 155 Millimetern mit 52 Kaliberlängen. Je nach Geschoss erreicht sie eine Reichweite von 30 bis 50 Kilometern. Mit der halb automatischen Ladehilfe kann sie 6 bis 8 Schuss pro Minute abfeuern, wobei die ersten drei Projektile innerhalb von 15 Sekunden verschossen werden können. Das Fahrzeug kann 18 Geschosse Bereitschaftsmunition und die dazugehörigen Treibladungen transportieren und ist innerhalb von einer Minute einsatzbereit. Die 8×8-Ausführung kann sogar 30 Geschosse Bereitschaftsmunition mitführen. Dieses Jahr wurde ein neues Modell präsentiert, das ein 6×6 -Fahrgestell hat und deren Führerhaus gepanzert ist. Ausserdem besitzt sie neu ein Feuerleutsystem. Neben dem Russland-Ukraine-Konflikt kam die CAESAR-Haubitze auch in Afghanistan, Thailand, dem islamistischen Staat und in Saudi-Arabien zum Einsatz.

WAFFEN DES RUSSLAND-UKRAINE-KONFLIKTS AUF DEM ILLEGALEN MARKT

Nachforschungen im Darknet deuten darauf hin, dass die Flut von westlichen Waffen an die Ukraine den Verkauf dieser Waffen auf dem illegalen Markt bzw. an radikale terroristische Gruppen fördert. Auch Russland gehöre zu den Käufern. Denn je mehr Waffen sie kaufen, desto weniger müssen sie letztendlich bekämpfen. Beispielsweise wurde kürzlich aufgedeckt, dass das ukrainische Militär die von Frankreich geschenkten CAESAR-Haubitzen über den illegalen Markt an Russland verkauft hat. Weil amerikanische Waffenlieferungen nicht durch amerikanische Truppen überwacht werden, besteht auch da der Verdacht, dass diese Lieferungen abgezweigt werden und das Material nie auf ukrainischem Boden landet. Vielmehr tauchen sie auf dem illegalen Markt auf und geraten so in die Hände von Betäubungsmittelhändlern, terroristischer Organisationen, extremistischer Milizen oder paramilitärischer Gruppen auf der ganzen Welt.

Es ist zu beachten, dass die beiden genannten Beispiele von Quellen stammen, die Nähe zu russischen Staatskanälen wie RT und SputnikNews haben und entsprechend befangen sein können. Verlässliche Quellen in diesen Zeiten und zu diesem Thema zu finden gestaltet sich schwierig. Ob die Informationen tatsächlich der Wahrheit entsprechen, oder ob diese zu politischen Zwecken gestreut werden, ist gegenwärtig schwierig einzuschätzen.Die Quintessenz ist, dass die NATO und ihre von westlichen Steuerzahlern finanzierten Waffenoperationen nun eine Quelle einer massiven internationalen Lieferkette für den Waffenhandel ist.

ZUSAMMENFASSUNG

Die vom Westen gelieferten Waffensysteme an die ukrainische Grenze, darunter Kriegswaffen wie die Haubitze M777, die Iskander-M, die Javelin-FGM-148, der Kamow Ka-52, der T-72, der BM-21 Grad, die Haubitze 2000, die Stinger, die Switchblade-Drohne und die CAESAR-Haubitze erreichen nicht alle ihr Ziel. Sie werden vorher umgeleitet oder auf dem illegalen Markt verkauft. Weshalb die NATO nun die Hauptquelle des Waffenhandels geworden ist, finanziert durch die westlichen Steuerzahler. Der Waffenhandel bleibt nach wie vor aktiv und wird besonders durch Kriege und Konflikte gefüttert. Den illegalen Waffenmarkt zu unterbinden, scheint ein unmögliches Unterfangen zu sein.

Michèle Trebo


)SCIP(
WAHRE SCHÖNHEIT
IST OFT VOR UNS
VERBORGEN

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:
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 fremden Produkten zu Werbezwecken. Werbung wird explizit als solche gekennzeichnet.

scip AG
Badenerstrasse 623
8048 Zürich
Schweiz

+41 44 404 13 13
www.scip.ch