RAPID7

NICER 2020:
DACH-Edition

Der National / Industry / Cloud Exposure Report (NICER) 2020 von Rapid7 ist die umfassendste Erhebung zum modernen Internet. In einer Zeit der globalen Pandemie und Rezession hat das Rapid7-Forschungsteam diese datengestützte Analyse der sich verändernden Internet-Risikolandschaft erstellt. Ziel war es, die Prävalenz und die geografische Verteilung allgemein bekannter Schwachstellen in den vernetzten Technologien zu ermitteln, die unsere Welt prägen. In dieser Ausgabe werden wir Details und bemerkenswerte Highlights speziell für die DACH-Region (Deutschland, Österreich, Schweiz) herausarbeiten.

Die wichtigsten Erkenntnisse:

- Die Gesamtexponierung reicht von niedrig (Schweiz, Platz 42 aller Länder) bis hoch (Deutschland, Platz 5), was vorhersehbar mit der Anzahl der Systeme korreliert, die im jeweiligen Land an das Internet angeschlossen sind.
- In allen drei DACH-Ländern gibt es eine beträchtliche Anzahl von SSH- (1.558.177), Telnet- (28.711) und Remote Desktop Protocol (RDP) -Diensten (197.682). Darüber hinaus gibt es eine recht große Anzahl von FTP-Servern (840.530) für die Übertragung von Klartextdateien.
- Schwachstellen mit hohem Schweregrad (CVSS 8.5+) konzentrieren sich auf eine kleine Anzahl sehr veralteter Versionen von Samba (Linux/Open-Source-Version von Microsoft SMB/CIFS-Filesharing-Diensten), DNS-Servern und Web/FTP-Servern, während Schwachstellen mit mittlerem Schweregrad (CVSS 4-8.4) in Hülle und Fülle vorhanden sind und sich auf eine Vielzahl von Versionen von Apache-HTTPD-Servern verteilen.

Zusammenfassung für DACH nach Ländern

Die nachstehende Tabelle zeigt den relativen Exponierungsrang der einzelnen Länder in der DACH-Region sowie die Vorherrschaft von IPv4-basierten Servern in diesen Ländern.

LAND	RANG	ALLOKIERTE IPV4-ADRESSEN	GEFUNDENE IPV4-ADRESSEN	NUTZUNG IN PROZENT
Deutschland	5	123,967,272	8,088,052	6.5%
Österreich	14	63,235,328	2,873,026	4.5%
Schweiz	42	20,921,768	777,258	3.7%
Summe DACH		208,124,368	11,738,336	14.8%

Gefundene Dienste in DACH-Ländern

Die nachstehende Tabelle bietet eine Übersicht der in Deutschland, Österreich und der Schweiz angebotenen Arten von Services.

SERVICE GRUPPE	SERVICE NAME	ANZAHL
Konsolenzugang	SSH (22)	1,558,177
Konsolenzugang	Telnet (23)	28,711
Datenbanken	memcached (11211)	1,344
Datenbanken	MS SQL (UDP/1434)	4,263
Datenbanken	MySQL (TCP/3306)	3
Datenbanken	Redis (6379)	4,116
File Sharing	FTP (21)	840,530
File Sharing	FTPS (990)	10,342
File Sharing	rsync (873)	17,937

SERVICE GRUPPE	SERVICE NAME	ANZAHL
File Sharing	SMB (445)	32,868
Infrastruktur	DNS (TCP/53)	247,032
Infrastruktur	DNS (UDP/53)	268,208
Infrastruktur	DoT (853)	340
Infrastruktur	NTP (123)	81,319
Mail	IMAP (143)	410,497
Mail	IMAPS (993)	402,247
Mail	POP3 (110)	389,964
Mail	POP3S (995)	355,822
Mail	SMTP (25)	711,898
Mail	SMTP (587)	412,257
Mail	SMTPS (465)	409,614
Remote Access	Citrix ADC/NetScaler	9,829
Remote Access	RDP (3389)	197,682
Remote Access	VNC (5900+5901)	21,244
Web	HTTP (80)	2,476,994
Web	HTTPS (443)	2,775,852

Schwachstellen nach Schweregrad und Land

Diese Tabelle zeigt die Anzahl aller erkannten Schwachstellen, die von Rapid7 durch Light-Touch-Scannen erkannt werden können, nach Schweregrad.

LAND	HOCH	MITTEL	NIEDRIG
Deutschland	47,579	6,659,446	238,343
Schweiz	3,566	496,202	18,208
Österreich	2,969	387,595	14,765
Summe DACH	**54,114**	**7,543,243**	**271,316**

DACH Dienste-Exponierung

Dieser Abschnitt konzentriert sich auf die wichtigsten Nicht-Web-Protokolle, die in DACH zu finden sind, insbesondere Telnet, SSH und RDP. SMB, MS SQL und all die anderen Protokolle sind in der DACH-Region zwar vorhanden, aber ihre Exponierungsraten liegen deutlich unter dem weltweiten Durchschnitt.

DACH-Dienst-Exponierung: Telnet

Es war nicht das erste Konsolenprotokoll, aber es ist das langlebigste.

ZUSAMMENFASSUNG

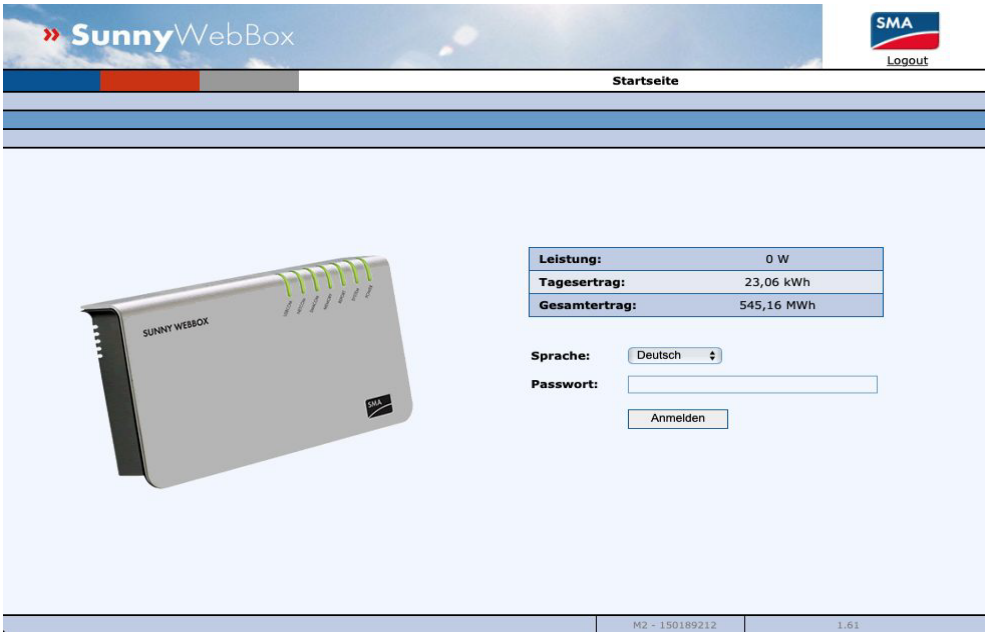
WAS ES IST:	Eine der ältesten Remote-Konsolen-Anwendungen, die heute im Internet verwendet werden.
WIE VIELE:	28,711 entdeckte Knoten
SCHWACHSTELLEN:	Seltsamerweise gibt es nur wenige Verwundbarkeiten im Sinne einer entfernten Codeausführung (obwohl einige wenige im Jahr 2020 aufgetaucht sind). Es gibt jedoch eine Fülle von Standard-Zugangsdaten, die Angreifer bei diesen unverschlüsselten Anmeldeaufforderungen verwenden können, und eine Fülle von Möglichkeiten, diese zu belauschen.
RATSCHLAG:	Setzen Sie Telnet nie und nimmer dem Internet aus.
ALTERNATIVEN:	SSH (Secure Shell) ist die einfachste Alternative zu Telnet, aber überlegen Sie, ob es klug ist, den Konsolenzugang über das Internet überhaupt erst freizugeben.

Die DACH-Sicht

Telnet kann ein Dienst sein, dessen Fingerabdrücke nur schwer zu erfassen sind, da die überwiegende Mehrheit der Anmeldeaufforderungen lediglich "Login:" oder "Benutzername:" sind. So ermöglichten nur 3.916 Geräte (14%) die Ermittlung des Geräteherstellers:

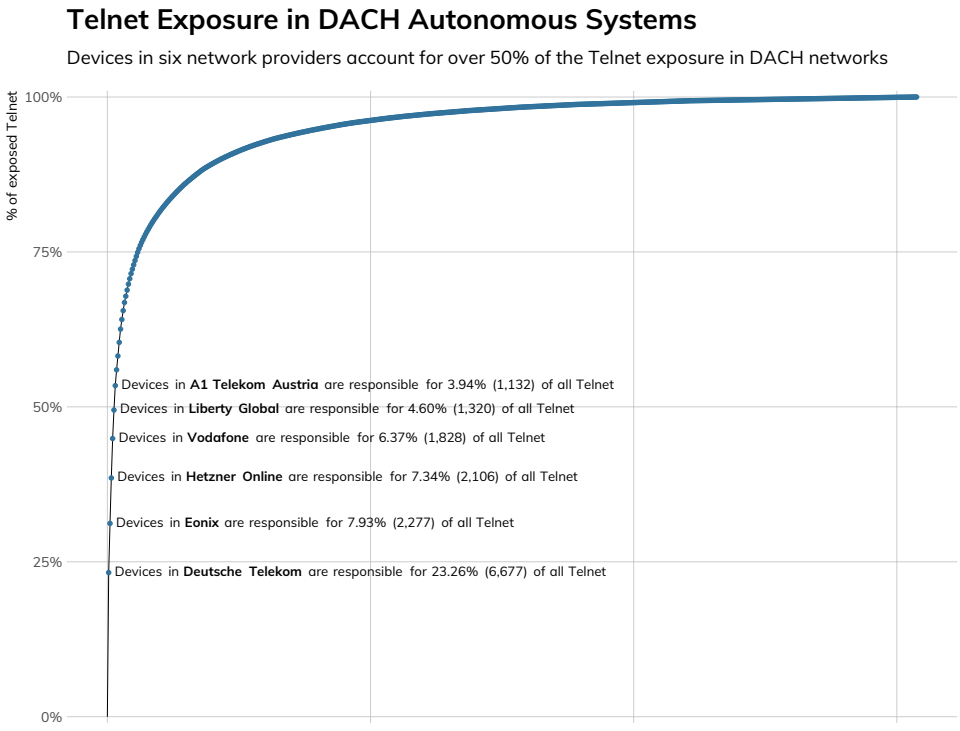
HERSTELLER	ANZAHL
Cisco	1,784
SMA Solar Technology	753
MikroTik	735
Microsoft	161
DD-WRT	101
Ubuntu	81
IBM	60
Debian	51
FreeBSD	38
CentOS	34
NetBSD	28
Hikvision	25
Fortinet	20
Allied Telesyn	13
Juniper	10
Polycom	9
Checkpoint	5
SCO	3
SUSE	3
Cobalt	1

Cisco und MikroTik sind Router der Unternehmens- oder Carrier-Klasse, d.h. Netzwerkanbieter oder Unternehmen haben sich versehentlich oder absichtlich dafür entschieden, Telnet zu aktivieren, wodurch ihr geschäftskritischer Datenverkehr gefährdet wird. Die Entdeckung von "SMA Solar Technology" war eine kleine Überraschung, da es sich dabei um "Sunny WebBox"-Geräte handelt, die zur Kommunikation mit Solarstrom-Wechselrichtern in Privathaushalten oder Unternehmen verwendet werden. Eine beunruhigende Anzahl von ihnen hat Telnet für den Fernzugriff aktiviert, zusammen mit einer unverschlüsselten HTTP-Port 80 Webadministrationsoberfläche:



Die Anwesenheit von "Microsoft" mag überraschend erscheinen, da Standard-Desktop-Windows normalerweise nicht mit Telnet ausgeliefert wird. Dabei handelt es sich jedoch meist um in Windows CE eingebettete Systeme, von denen viele administrative Schnittstellen zu Gebäudeautomatisierungs-Systemen aufweisen.

Über 50% der Telnet-Exponierungen in DACH stammen von nur sechs autonomen Systemen von Netzwerkanbietern: Deutsche Telekom, Eonix, Hetzner Online, Vodafone, Liberty Global und A1 Telekom Austria.



Leider stammt der größte Teil (65 %) der Telnet-Exponierung der Deutschen Telekom, wie bereits erwähnt, von SMA Solar Technology, wobei Cisco-Router/Firewall-Geräte mit 23 % der Exponierung an zweiter Stelle stehen. Die Telnet-Exponierung von Hetzner Online kommt hauptsächlich von MikroTik-Routern (58%), und sowohl Cisco- als auch SMA Solar-Geräte sind mit 43% bzw. 25% der Exponierung bei Vodafone am stärksten vertreten.

Unsere Empfehlung

Organisationen sollten überprüfen, was sie ins Internet gestellt haben, und sich bemühen, die Nutzung von Telnet so bald wie möglich zu unterbinden, indem sie regelmäßige Discovery-Scans durchführen und mit den Eigentümern von IT, Anwendungen und Geschäftsprozessen zusammenarbeiten, um umsetzbare Pläne für die Beendigung der Telnet-Nutzung zu erarbeiten.

ISPs sollten Telnet blockieren und auf keinen Fall selbst Telnet zur Verwaltung von Telekommunikationsdiensten nutzen. Dies gilt insbesondere für die DACH-Länder, in denen nur ein halbes Dutzend ISPs für den Großteil der Telnet-Exponierung verantwortlich sind.

Die Regulierungsbehörden in den DACH-Ländern sollten erwägen, die Nutzung von Telnet in öffentlichen Internet-Segmenten zu verbieten und Gerätehersteller daran zu hindern, Geräte zu vertreiben, die eine Konfiguration von Telnet ermöglichen.

DACH-Dienst-Exponierung: Secure Shell (SSH)

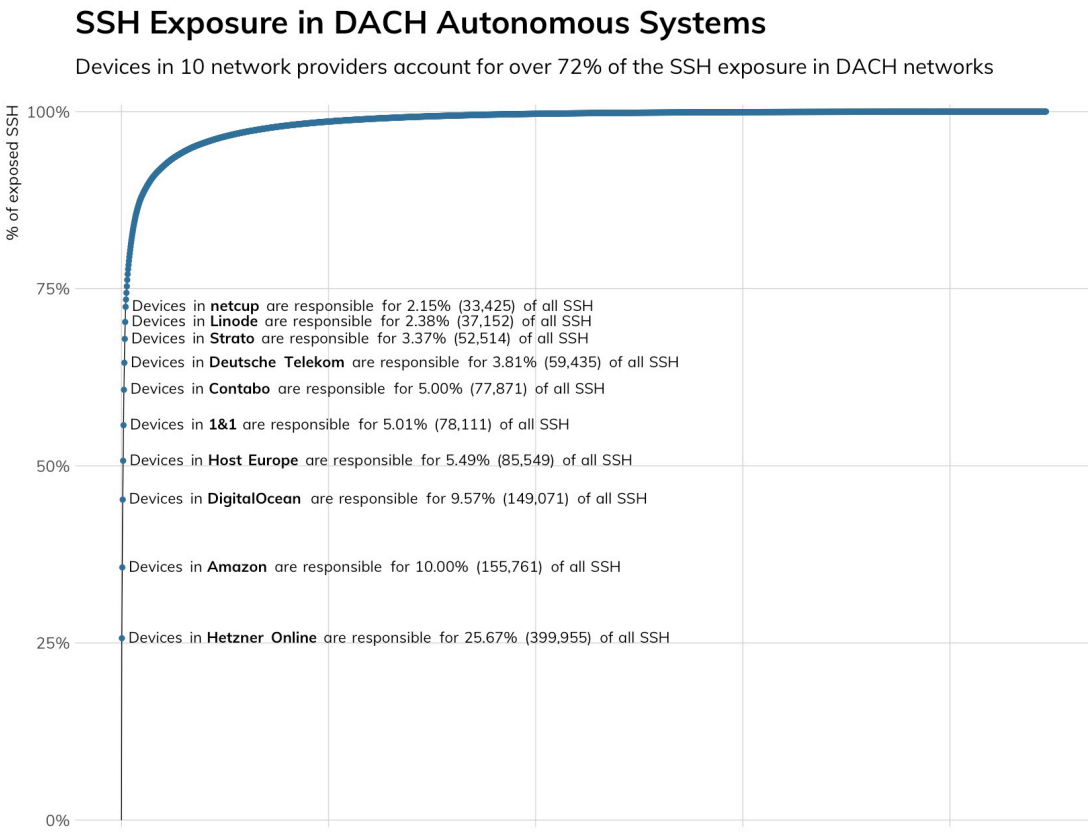
Dieser Dienst trägt Sicherheit schon im Namen!

ZUSAMMENFASSUNG

WAS ES IST:	SSH ist normalerweise eine sichere Alternative zu Telnet, aber es kann auch praktisch jedes Protokoll in eine warme, beruhigende Decke kryptographischer Sicherheit hüllen.
WIE VIELE:	1,558,177 entdeckte Knoten
SCHWACHSTELLEN:	Wie bei Telnet stammen die üblichen Gefährdungen im Zusammenhang mit SSH von Standardpass-wörtern und der Wiederverwendung von Passwörtern. Außerdem neigt SSH dazu, Schwachstellen in den kryptographischen Bibliotheken von Betriebssystemen aufzudecken.
RATSCHLAG:	Setzen Sie SSH mit Bedacht ein und bauen Sie auf ein System zur Generierung und Verwaltung sicherer Passwörter oder privater Schlüssel.
ALTERNATIVEN:	Es gibt sicherlich Alternativen zu SSH, aber es ist frei, quelloffen und wird von einem Netzwerk akademischer und kommerzieller Softwareentwickler gut gepflegt. Es ist schwer vorstellbar, eine vernünftige Alternative zu SSH zu finden, insbesondere angesichts der Tatsache, dass SSH ansonsten unsichere Protokolle transportieren kann.

Die DACH-Sicht

Während die Telnet-Exponierung vor allem in ISP-Netzwerken zurückging, ist die SSH-Exponierung über ISPs, Cloud-Provider und andere Hosting-Provider verteilt. Dennoch sticht die Hetzner-Online-Exponierung hervor, da über ein Viertel der Systeme nur auf SSH-Verbindungen warten.



Wie in der Zusammenfassung angemerkt, kann SSH eine großartige Möglichkeit sein, sicheren Fernzugriff auf ein System bereitzustellen, vorausgesetzt, Sie verwenden zertifikatsbasierten Zugriff und/oder verlangen eine Mehrfaktor-Authentifizierung. Außerdem müssen Sie die Versionen aktuell halten - was viele Benutzer eindeutig nicht tun, da wir über 140 verschiedene OpenSSH-Versionen in DACH-Ländern entdeckt haben.

Während es in Ordnung ist, SSH auf Servern freizugeben, ist es viel weniger in Ordnung, es für die Verwaltung von Internet-basierten Routern freizugeben, da wir wissen, dass diese Geräte gerne mit Standardpasswörtern und leicht zu erratenden Passwörtern ausgeliefert werden. Zudem kann es schwierig sein, sie für eine sicherere zertifikatsbasierte Authentifizierung zu konfigurieren. Über 560 Cisco Adaptive Security Appliances (Cisco ASA) und fast 360 MikroTik-Router haben SSH für den administrativen Fernzugriff aktiviert.

Unsere Empfehlung

Organisationen sollten bestrebt sein, einen möglichst minimalen SSH-Fußabdruck zu haben, die Aktualität der Version zu gewährleisten und für die Sitzungen Zertifikate und/oder Mehrfaktor-Authentifizierung zu verlangen. Um sich ein klareres Bild davon zu machen, warum dies so wichtig ist, lesen Sie den SSH-Abschnitt im globalen NICER-Bericht.

Cloud-Provider sollten es nahezu unmöglich machen, Instanzen mit veralteten SSH-Versionen zu betreiben, und den Kunden einen Überwachungs- und Benachrichtigungsdienst zur Verfügung stellen, wenn veraltete Versionen oder unsichere Konfigurationen entdeckt werden. Geschieht dies nicht, riskiert der Cloud-Anbieter seinen Ruf und stellt Angreifern möglicherweise indirekte (kostenlose) Rechenzyklen und Bandbreite zur Verfügung.

Die Regulierungsbehörden in DACH sollten die Verwendung von SSH über Telnet fördern und Leitlinien für sichere Betriebspraktiken für dieses kritische Protokoll bereitstellen.

DACH-Dienst-Exponierung: Remote Desktop Protocol (RDP)

Es ist wie VNC, aber mit Microsoft-Touch.

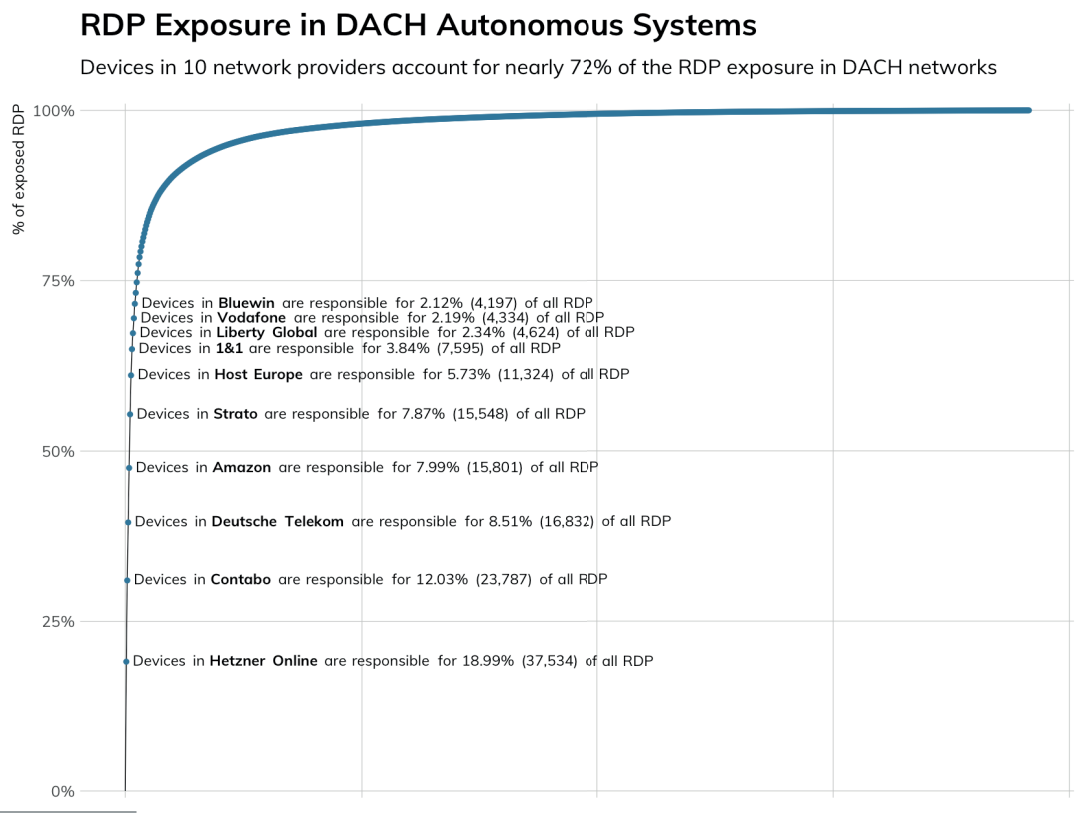
ZUSAMMENFASSUNG

WAS ES IST:	Ein proprietäres Protokoll, das von Microsoft entwickelt wurde, um Verbindungen über die grafische Benutzeroberfläche (GUI) von einem System zum anderen herzustellen. Der Standardport ist TCP/3389, aber es kann auf jedem offenen Port gehostet werden.
WIE VIELE:	197,682 entdeckte Knoten
SCHWACHSTELLEN:	Zahlreiche Probleme bei der Remote-Code-Ausführung, einschließlich CVE-2019-0708[1] (BlueKeep), das von Microsoft im Frühjahr 2019 bekannt gegeben wurde.
RATSCHLAG:	Platzieren Sie RDP hinter einer VPN-Verbindung, wenn es "always on" sein muss. Wenn RDP intermittierend zur Verfügung gestellt werden kann, stellen Sie sicher, dass alle Knoten, die RDP bereitstellen, vollständig gepatcht und gemäß den empfohlenen Spezifikationen gehärtet sind und eine Mehrfaktor-Authentifizierung verwenden.
ALTERNATIVEN:	Dies ist die von Microsoft empfohlene Lösung für den Fernzugriff auf entfernte Systeme. Sie macht das, was sie verspricht, ziemlich gut, so dass es keine wirklichen Alternativen gibt. Wenn Sie diese Art des Zugriffs benötigen, befolgen Sie die Hinweise im Abschnitt "Ratschläge".

Die DACH-Sicht

Obwohl Microsoft Remote Desktop einen schnellen und effizienten Zugriff auf Windows-Server innerhalb Ihres Unternehmensnetzwerks ermöglicht, wurde es nie wirklich für den direkten Zugriff auf das Internet konzipiert und ist zu einem der am meisten angegriffenen Dienste im Internet geworden. Fast 95 % der exponierten RDP in DACH verwenden eine Authentifizierung[2] auf Netzwerkebene - was dazu beiträgt, den Erfolg einfacher Angriffe zu verhindern. Das Exponieren von RDP kann aber gefährlich sein, wenn man bedenkt, wie einfach es ist, Brute-Force- oder Credential-Stuffing-Attacken gegen diese Systeme durchzuführen.

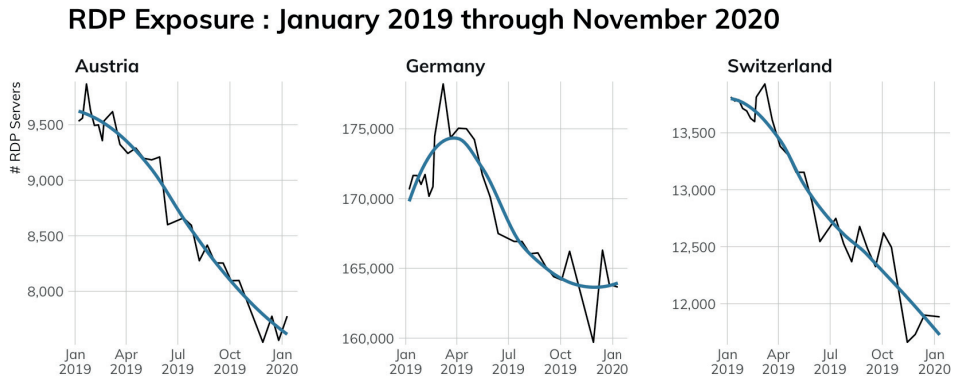
RDP wird in fast 960 autonomen Systemen eingesetzt, da viele Organisationen und Einzelpersonen es aus Bequemlichkeit nutzen. Es gibt dabei einige Cluster bei wenigen ISPs für Geschäfts- und Privatkunden sowie bei Hosting- und Cloud-Providern:



[1] BlueKeep/CVE-2019-0708 <https://attackerkb.com/topics/huQasjoVMS/windows-remote-desktop-rdp-use-after-free-vulnerablility-bluekeep?>

[2] NLA <https://en.wikipedia.org/wiki/Network_Level_Authentication>

Ein gutes Zeichen ist, dass sich die RDP-Nutzung in den DACH-Ländern auf einem soliden Abwärtstrend befindet. Wir haben die NICER-Daten für diesen DACH-Bericht aktualisiert und die Trends seit 2019 bis November 2020 untersucht. In Österreich, Deutschland und der Schweiz gibt es Anzeichen dafür, dass Individuen und Organisationen die Nutzung von RDP für den direkten Fernzugriff auf Server langsam auslaufen lassen.[3]



Unsere Empfehlung

Organisationen sollten dringend erwägen, RDP-Systeme hinter ein gut konfiguriertes und gut gewartetes virtuelles privates Netzwerk (VPN) zu verlagern. Zum Zeitpunkt der Veröffentlichung stehen Angreifern über 15 Milliarden Zugangsdaten[4] zur Verfügung, von denen viele aus Phishing-Angriffen und der Exfiltration von Credential-Speichern stammen, so dass Sie sich nicht auf eine einfache Kombination aus Benutzername und Passwort verlassen können, um Angreifer erfolgreich abzuwehren.

ISPs und Hosting-Provider sollten Kunden davon abhalten, RDP-Dienste aufrechtzuerhalten, und dabei helfen, alternative Möglichkeiten zur Fernadministration von Systemen oder zum Zugriff auf kritische Anwendungen anzubieten. Die Regulierungsbehörden in DACH sollten nachdrücklich von der Nutzung direkter Internet-RDP-Verbindungen abraten und alternative Ansätze für den grafischen Fernzugriff auf Systeme aufzeigen.

DACH Angreifbare Schwachstellen

In diesem konzentrierten Blick auf die DACH-Region wollten wir speziell die Arten von Schwachstellen mit hoher und mittlerer Schwere untersuchen, die heute über das Internet ausnutzbar zu sein scheinen. Wie bei NICER beschränken sich diese Schwachstellen auf diejenigen, die wir mehr oder weniger offensichtlich erkennen können: dass Anbieter und Version einer anfälligen Software (anonym, ohne Anmeldedaten) per Fingerabdruck gefunden werden können; dass die Software in dieser Version mindestens eine öffentlich bekannte Schwachstelle aufweist, die im CVE Dictionary aufgeführt ist, und dass der CVE-Eintrag einen zugehörigen CVSS-Wert hat.

Schwachstellen mit hohem Schweregrad

Während die CVSS-Methode zur Bewertung von Schwachstellen ihre Herausforderungen hat[5], ist sie die bequemste Methode, die wir haben, um die Gefährlichkeit einer öffentlich bekannten Schwachstelle auszudrücken. Für unsere Zwecke ist eine "hochgradige" Schwachstelle eine Schwachstelle, die mit 8,5 oder höher bewertet wird, und diese Schwachstellen haben fast alle eine Art von RCE-Komponente (Remote Code Execution) - ein Angreifer, der diese Schwachstellen ausnutzt, neigt dazu, sich ungehinderten Zugang zu der betroffenen Komponente zu verschaffen.

[3] Wie im NICER 2020 angemerkt, haben individuelle Scans eine Fehlermarge von ~4%, da das Internet schockierend instabil sein kann. Versuchen Sie also zu vermeiden, sich auf die einzelnen Punkt-für-Punkt-Werte zu konzentrieren. Wir haben eine geglättete Trendlinie hinzugefügt, um leichter erkennen zu können, wohin sich jedes Land mit der Exponierung von RDP bewegt.

[4] https://resources.digitalshadows.com/whitepapers-and-reports/from-exposure-to-takeover

[5] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=635185

HERSTELLER	PRODUKT	ANZAHL VON SYSTEMEN MIT SCHWERWIEGENDEN SCHWACHSTELLEN
proftpd	proftpd	18,640
samba	samba	16,638
isc	bind	7,658
apache	http_server	4,196
openbsd	openssh	2,794
microsoft	iis	1,663
exim	exim	360
apache	couchdb	78
powerdns	recursor	10

Die Samba-Schwächen, wie z. B. CVE-2012-1182[6], weisen funktionierende Exploits auf, die zur Ausführung von Code mit Root-Privilegien führen können. Zwar sind die Netze in DACH nicht mit solchen Systemen durchsetzt, aber es gibt genug, um ein großes Botnet zu erstellen, und jeder Einstiegspunkt kann tieferen Zugang zu Backend-Netzwerken bieten.

In ähnlicher Weise ermöglichen große Schwachstellen in ProFTPD, wie z.B. CVE-2015-3306[7], eine praktisch vollständige, nicht authentifizierte Kontrolle über das entfernte System, insbesondere wenn es mit einem PHP-fähigen Webserver gepaart ist.

Die Gesamtzahlen mögen zwar gering sein, aber sie werden durch die Telnet-, SSH- und RDP-Exponierungen wettgemacht.

Schwachstellen mit mittlerem Schweregrad

Verwundbarkeiten mit hohem Schweregrad stehen immer im Mittelpunkt der Berichterstattung, da sie in der Regel "leicht" zu nutzen sind, um die Kontrolle über ein bestimmtes System zu erlangen, aber Schwachstellen mit mittlerem Schweregrad sind nichts, was man vernachlässigen sollte. Diese Schwachstellen sind in der Regel keine direkten Einfalltore für RCE, aber sie bieten Angreifern das Nächstbeste, nämlich Passwörter oder andere vertrauliche Informationen. Zum Beispiel ist die Cisco-ASA-Schwachstelle CVE-2020-3259[8] nur eine 7,5, aber sie beinhaltet das Durchsickern von ziemlich kritischem SSL-Schlüsselmaterial, was zu einer Kompromittierung einer gesamten VPN-Umgebung führen kann.

HERSTELLER	PRODUKT	ANZAHL VON SYSTEMEN MIT MITTELSCHWEREN SCHWACHSTELLEN
apache	http_server	753,452
openbsd	openssh	101,651
isc	bind	71,179
squid-cache	squid	29,639
nginx	nginx	19,121
proftpd	proftpd	18,664
exim	exim	17,154
samba	samba	16,821
apache	tomcat	4,038
thekelleys	dnsmasq	3,958
microsoft	iis	1,663
mailenable	mailenable	624
mortbay	jetty	411

[6] https://attackerkb.com/topics/u6DlzoLbwe/cve-2012-1182-samba-rce-via-rpc

[7] https://attackerkb.com/topics/1Qhi2ndx91/cve-2015-3306-proftpd-unauthenticated-remote-read-write

[8] https://attackerkb.com/topics/g0etAbGFCv/cve-2020-3259

HERSTELLER	PRODUKT	ANZAHL VON SYSTEMEN MIT MITTELSCHWEREN SCHWACHSTELLEN
apple	cups	30
microsoft	personal_web_server	24
libssh	libssh	18
powerdns	recursor	13
tornadoweb	tornado	12
sun	java_system_web_server	8
ipswitch	imail_server	6
novell	groupwise	5
altn	mdaemon	4

Der Großteil dieser mittelschweren Schwachstellen ermöglicht triviale Denial-of-Service-Angriffe, wobei eine Handvoll, wie z.B. CVE-2013-2249[9], je nach Konfiguration auch andere Remote-Aktionen ermöglichen.

Noch beunruhigender an diesem Arsenal von Schwachstellen (aller Schweregrade) ist die Versionsvielfalt in Komponenten, deren Aktualisierung ziemlich trivial wäre. Unsere Scans ergaben nicht weniger als 147 verschiedene Versionen von Apache Tomcat[10], einer Java-Anwendungsumgebung, die viele verschiedene Webanwendungen unterstützt, und 129 verschiedene Versionen von Apache HTTPD.

HERSTELLER	PRODUKT	ANZAHL ENTDECKTER VERSIONEN
apache	tomcat	147
nginx	nginx	129
apache	http_server	115
samba	samba	114
isc	bind	57
squid-cache	squid	54
openbsd	openssh	53
mortbay	jetty	39
exim	exim	28
caucho	resin	19
thekelleys	dnsmasq	19
ibm	lotus_domino	16
proftpd	proftpd	13

Wenn diese alten Versionen dem Internet ausgesetzt werden, ist das ein Signal an Angreifer, dass der Rest Ihrer Infrastruktur ebenso ungepflegt sein könnte, und erhöht die Wahrscheinlichkeit, dass Sie Ziel von Angriffen werden.

[9] https://attackerkb.com/topics/Ox3QTCWuJI/cve-2013-2249
[10] https://tomcat.apache.org/

Schlussfolgerungen

Die Exponierung der DACH-Region (kombiniert) ist im Vergleich zu anderen Ländern auf einem erhöhten Niveau. Deutschland ist das Land mit der höchsten Internet-Exponierung in der Region und liegt an fünfter Stelle, Österreich an 14. Die Schweiz liegt auf Platz 42 der am stärksten exponierten Länder der Region.

Dennoch gibt die Anzahl von fast 900.000 Klartext-FTP-Servern zusammen mit fast 200.000 RDP-Servern, weit über 1,5 Millionen SSH-Servern und Zehntausenden von exponierten Telnet-Servern in der Region Anlass zu einer gewissen Besorgnis. Um die lokale Online-Exponierungssituation zu verbessern, sollten Leser aus DACH sicherstellen, dass ein exponiertes System:

- **absichtlich exponiert wird.** Sie wollten es exponieren und haben es nicht versehentlich exponiert.
- **kompetent konfiguriert wird.** Die Konfiguration ist sicher und darauf ausgelegt, nur die notwendigen Aufgaben auszuführen.
- **regelmäßig gepatched wird.** Sie müssen sich wirklich bemühen, mit den aktuellen Versionsständen Schritt zu halten, insbesondere wenn kritische Schwachstellen identifiziert wurden. Sie müssen auch alles daran setzen, dass Sie gepatchte Versionen auch dann abrufen können, wenn Ihre Standard-Paket-Repositorys die Aktualisierung einstellen.
- **sorgfältig gepatched wird.** Sie haben soeben die Angriffsfläche sowohl für sich selbst/ihre Organisation als auch für das Internet als Ganzes vergrößert; als solche sind Sie von Natur aus dafür verantwortlich, Ihren Teil zur Verteidigung dieser Ressourcen beizutragen.
- **im Bewusstsein exponiert wurden, dass sie angegriffen werden können.** Forscher sind nicht die einzigen, die nach Diensten suchen, und Angreifer haben nicht die ethischen und rechtlichen Einschränkungen, die wir haben, also werden sie härter suchen und nach Belieben angreifen. Sie können nicht davon ausgehen, dass Ihre Dienste nur den gutartigen Interaktionen und Methoden ausgesetzt werden, die Sie in Ihren Anwendungsfällen skizziert haben.

Lesen Sie den kompletten Bericht:

https://www.rapid7.com/research/report/nicer-2020/