c’t deckt auf

Dateien, IoT und Industrieanlagen ungeschützt im Netz

Dateifreigaben ungeschützt im Netz ..... **Seite 16**
Industrieanlagen und IoT ohne Schutz ..... **Seite 20**
Pager-Dienste unverschlüsselt ..... **Seite 24**
Feuerwehr-Alarmierung für alle ..... **Seite 26**
Wordpress zu gesprächig ..... **Seite 28**
Newsletter und Formulare missbrauchen ..... **Seite 32**

Angriffe auf die IT-Umgebungen von Unternehmen sind mitunter unglaublich einfach. Häufig kann man Daten abgreifen oder Industriesteuerungen übernehmen, ohne überhaupt Sicherheitsmechanismen umgehen zu müssen. Wir haben das Internet systematisch nach ungesicherten Servern durchsucht.

Von Jan Mahn und Merlin Schumacher

Paradiesische Zustände müssen das gewesen sein, als die Vorläufer des Internets erfunden wurden: Das gesamte Netzwerk bestand aus einer handvoll freundlich gesinnter Nutzer aus Forschungseinrichtungen und wer einen Dienst anbot, konnte mit Dankbarkeit und gutgemeinten Ratschlägen rechnen. Dass das im heutigen Internet anders aussieht, hat sich mittlerweile herumgesprochen – sollte man zumindest annehmen. Im Internet tummeln sich längst nicht nur freundliche Zeitgenossen und schon als gewöhnlicher Nutzer muss man ständig auf der Hut sein.

Ungleich aufmerksamer muss man sich aber verhalten, wenn man selbst einen Dienst im Internet veröffentlichen möchte. Immer dann, wenn man die Konfigurationsoberfläche des eigenen Routers öffnet und eine Portweiterleitung einrichtet, sollte man sich bewusst machen, welche Verantwortung man jetzt trägt. Ein handelsüblicher Router, der nebenbei als Firewall arbeitet, lehnt alle Anfragen von außen grundsätzlich ab und schützt die Geräte im Netz vor Anfragen aus dem Internet. Mit einer Portweiterleitung bohrt man gezielt ein Loch in diese Firewall und legt fest, welcher Port zu welchem Gerät im privaten Netz weitergeleitet werden soll. Das kann ein Webserver sein, die Steuerung des Smart-Homes oder ein Mailserver. Wichtig ist jetzt: Der veröffentlichte Dienst muss unbedingt mit einer Anmeldung versehen, verschlüsselt und die verwendete Software stets aktuell sein. Vor allem aber sollte man die Finger von Portweiterleitungen lassen, wenn man sich unsicher ist.

Planlos offen?

Wer unbedacht Ports aufreißt, der riskiert, dass ihm Daten gestohlen werden oder andere im privaten Netz umherspazieren und dort Schaden anrichten. Doch leider sind solche Fehlkonfigurationen keine Seltenheit. Immer wieder bekamen wir in der Vergangenheit Hinweise auf einzelne Fälle, die Hinweisgeber zufällig entdeckt haben. Besonders prominente Fälle waren eine Arztpraxis [1] und die Autovermietung Buchbinder [2], beiden wurden ungeschützte Dateifreigaben zum Verhängnis. Doch sind solche Probleme Einzelfälle oder eher die Regel? Um das herauszufinden, haben wir das Internet systematisch unter die Lupe genommen. In diesem und den folgenden Artikeln stellen wir eine Auswahl unserer Erkenntnisse vor. Die Fälle stehen exemplarisch für viele weitere Funde – gleichzeitig geben wir Ratschläge, wie Sie als Administrator solche Fehler vermeiden können.

In diesem Artikel beschreiben wir, wie wir vorgegangen sind, und zeigen beispielhaft am Protokoll SMB, welche Folgen eine Fehlkonfiguration haben kann. Ab Seite 20 befassen wir uns gezielt mit Industriesteuerungen und dem IoT-Protokoll MQTT – in Industrieanlagen können offene Systeme in kurzer Zeit besonders viel Schaden anrichten. Quasi nebenbei stießen wir bei unseren Recherchen auf weitere Konfigurationsfehler: Ab Seite 24 lesen Sie, wie unachtsame Admins Feuerwehr- und Rettungsdienstnachrichten im Internet veröffentlichten. Unschöne Probleme kann man sich auch als Betreiber von Newsletter-Formularen eintreten. Ab Seite 32 erfahren Sie, wie man durch Unachtsamkeit Spammern und Phishern einen erfolgreichen Arbeitstag garantiert. Allzu kommunikativ sind auch falsch konfigurierte Wordpress-Umgebungen – mehr ab Seite 28. Doch nicht nur im Internet wird gern unverschlüsselt und ungeschützt kommuniziert. Auch im Funkspektrum findet man mit einem günstigen Empfänger mehr offene Datenübertragung, als die DSGVO erlaubt. Ab Seite 24 lesen Sie die Details.

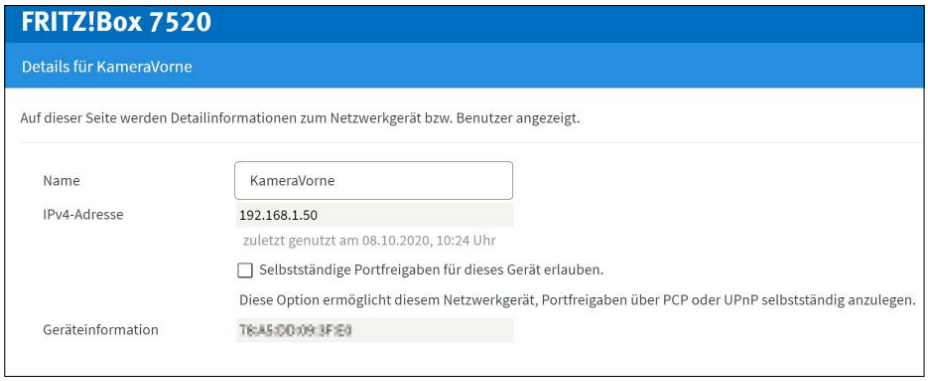
IPs sind nicht geheim

Viele unfreiwillige Dienstanbieter sitzen einem gewaltigen Irrtum auf, den man auch immer wieder in Foren und Blogs als gut gemeinten Ratschlag liest: Solange man keine Domain einrichte, die per DNS auf die Adresse auflöst, sei eine IP-Adresse in den Weiten des Internets quasi geheim. Es gebe schließlich über 4 Milliarden Adressen, daher sei es unmöglich, einen veröffentlichten Dienst unter einer beliebigen Adresse zu erraten.

Diese Erzählungen gehören definitiv ins Reich der Mythen. Schon die vermeintlichen 4,2 Milliarden IP-Adressen existieren nur in der Theorie. Abziehen kann man zunächst alle Broadcast-Adressen sowie sämtliche reservierten Adressbereiche, zusammen rund 600 Millionen. Die verbliebenen rund 3,6 Milliarden IPv4-Adressen reichen keinesfalls aus, damit ein Dienst anonym bleiben kann.

Möchte man offene Ports im Internet finden, muss man nur systematisch danach suchen. Ein bewährtes Werkzeug unter Sicherheitsforschern ist die Suchmaschine shodan.io. Deren Betreiber haben Server mit Portscannern eingerichtet – ein solcher Portscanner probiert nacheinander die Ports an einer Adresse durch und protokolliert, auf welchen Ports er eine Antwort bekommen hat. Will man das gesamte Internet durchsuchen, muss man das 3,6 Milliarden mal wiederholen. Shodan geht dann noch einen Schritt weiter und stellt für zahlreiche Protokolle eine Verbindung her und speichert die Antworten in seiner Datenbank. Über eine Weboberfläche kann man gezielt nach Protokollen oder

Über 63.000 SMB-Server fanden wir weltweit im Internet. Auf viele konnte man ohne Zugangsdaten zugreifen.



Möchte man verhindern, dass das NAS per UPnP ein Loch in die Firewall bohrt und Daten ungewollt mit der Welt teilt, muss man die Funktion im Router deaktivieren.

Antworten suchen. Einen ähnlichen Dienst gibt es bei censys.io. Ganz einfache Suchen sind kostenlos, für kommerzielle Nutzung und Filter muss man zahlen.

Gezieltes Vorgehen

Für unseren Sicherheitsreport wollten wir uns aber nicht auf gefilterte und aufbereitete Datensätze von anderen verlassen. Solche Suchmaschinen bringen die Funde in eine eigene Reihenfolge und finden einige Adressen gar nicht. Stattdessen entschieden wir uns, selbst ein System zum systematischen Scannen des gesamten IPv4-Internets vorzubereiten. Dafür mussten wir das Rad nicht neu erfinden. Grundlage für unseren automatischen Scanner ist das Open-Source-Kommandozeilenwerkzeug ZMap. Das scannt das gesamte Internet und schreibt alle IP-Adressen mit einem offenen Port in eine Datei. Bemerkenswert ist die Geschwindigkeit, die ZMap an den Tag legt: Ein Scan für einen Port über alle Adressen dauert nach Angaben der Entwickler nur 5 Minuten, wenn man eine 10-GBit/s-Leitung nutzen würde. Wir entschieden uns, die Scans auf angemieteter Hardware bei einem Hoster zu starten, und drosselten ZMap auf unter 25 MBit/s. So mussten wir teilweise einige Tage auf einen kompletten Scan des Internets warten.

Netzlaufwerke für alle

Den ersten Scan starteten wir auf SMB-Port 445. Windows-Nutzer kennen das Protokoll von den Windows-Dateifreigaben, aber auch Linux-Maschinen und NAS können SMB anbieten. Die Liste der Ergebnisse war lang. Bei etwa 63.000 IPs meldete sich ein SMB-Dienst. Auf diese Liste ließen wir ein Skript los, das einen SMB-Verbindungsaufbau ohne Zugangsdaten probierte.

Die meisten Server brachen die Verbindung ab oder verlangten ein Login. Etwa 1500 Server antworteten bereitwillig auf unsere Anfragen und listeten die verfügbaren Freigaben. Einige Server boten sogar noch SMB 1 an, für das seit Jahren Exploits bekannt sind. Uns interessierten – schon um jeden rechtlichen Ärger zu vermeiden – aber nur die Freigaben, die ohne jede Anmeldung les- und oder beschreibbar waren. Davon gab es viele: So fanden wir die gesamte Buchhaltung zweier südamerikanischer Baufirmen und eines mittelamerikanischen Urlaubsclubs, Verträge, Rechnungen und Beschlüsse einer asiatischen Regionalverwaltung und viele NAS-Geräte.

Bei den NAS handelt es sich um ein systematisches Problem und nicht immer hat der Nutzer die Portweiterleitung per Hand im Router aktiviert. Viele Router gestatten es Geräten im Netzwerk, per UPnP eine solche Weiterleitung selbst einzurichten. Öffnet das NAS Port 445 in der Firewall, ist die Katastrophe perfekt. Deaktivieren Sie daher UPnP-Freigaben in Ihrem Router. Die Fritzbox listet unter „Internet / Freigaben / Portfreigaben“ alle Geräte mit offenen Ports auf. Entfernen Sie hier alle Haken in der Spalte „Selbstständige Portfreigabe“ und klicken Sie auf „Übernehmen“.

Manche NAS bieten Freigaben für Apples Backup-System Time Machine an, die grundsätzlich ohne Anmeldung erreichbar sind. Im lokalen Netz mag das praktisch sein, um den Mac zu sichern, in Kombination mit einer Portfreigabe ist das verheerend. Wir fanden zahlreiche Komplett-Backups von Apple-Nutzern weltweit. Bei vielen NAS waren wir auch nicht die ersten Besucher. Hier hatten schon Verschlüsselungstrojaner zugeschlagen.

Auch ein grober Schnitzer aus Deutschland war dabei, zur Abwechslung mal kein NAS. Ein nordrhein-westfälischer Büromöbelhändler hatte seinen Windows-Server ins Netz gestellt, damit die Mitarbeiter bequem auf die Daten zugreifen können – leider konnte das auch jeder nicht angemeldete Besucher. Die gesamte Unternehmenskommunikation war per SMB für jedermann zugänglich, darunter Rechnungen der letzten Jahre, Kundenlisten, Umsatzauswertungen, Kostenvoranschläge. Wir haben den Anbieter darauf aufmerksam gemacht und er hat die Lücke zügig geschlossen und zugesichert, den zuständigen Landesdatenschutzbeauftragten zu informieren. Die Freigaben lagen auch nicht auf einer Maschine im eigenen Netz, sondern auf einer virtuellen Maschine bei einem Hoster. Die haben oft keine separate Firewall, sodass man sich unbedingt darum kümmern muss, die Firewall des Betriebssystems einzurichten. Im Gespräch war der IT-Verantwortliche des kleinen Unternehmens überrascht, dass die Freigabe in den Weiten des Netzes gefunden werden konnte. Den Vorfall nahm er zum Anlass, eine VPN-Lösung bei einem Dienstleister in Auftrag zu geben.

Was tun?

All diese Freigaben fanden wir mit einem oberflächlichen Scan, wir mussten keine Zugangssicherungen überwinden. Eine Absicherung der Freigaben per Authentifikation ist zwar schon ein Schritt mehr, reicht gegen Angreifer aber nicht aus. SMB gehört zu den sehr geschwätzigen Protokollen. Auch wenn man von außen nicht auf die Freigaben selbst, sondern nur auf die Übersicht zugreifen kann oder Details zur verwendeten Software sieht, ist das schon zu viel. Aus unserer Sicht gehört SMB ins lokale Netz, nicht ins Internet! Wer Netzwerkfreigaben braucht, muss ein VPN einrichten.

Alternativ können Sie über eine selbstgehostete Nextcloud-Instanz nachdenken (sofern Sie Admin-Erfahrungen mitbringen). Und selbst Server von Google, Amazon und Microsoft sind immer noch ein datenschutzfreundlicherer Ort als eine laienhaft ins Internet gehängte SMB-Freigabe. *(jam@ct.de)* c't

Literatur

[1] Ronald Eikenberg, Dr. Datenleck, Warum eine komplette Arztpraxis offen im Netz stand, c't 25/2019, S. 16

[2] Hartmut Gieselmann, Ronald Eikenberg, Christian Wölbert, Joerg Heidrich, Daten-GAU bei Buchbinder, Persönliche Informationen von 3 Millionen Kunden der Autovermietung Buchbinder offen im Netz, c't 4/2020, S. 12