Sicherheit im Heimnetzwerk: So werden Smart Homes zukunftsweisend sicher

Ein Leitfaden für Internetanbieter

Plume®

Einführung

Noch nie war die Sicherheit von Heimnetzwerken so wichtig wie heute. Die Kunden holen sich immer mehr Smart-Home-Geräte ins Haus. Viele davon bergen jedoch auch unbekannte Sicherheitsrisiken. Parallel dazu arbeiten immer mehr Menschen von zu Hause aus und die Arbeitswelt verändert sich gerade gravierend.

Ein Heimnetzwerk ist im Prinzip eine Vernetzung von mehreren Geräten. Diese muss natürlich gut geschützt werden. Doch anders als bei einem Unternehmensnetzwerk gibt es meist keine Fachleute, die sich um die Sicherheit des Heimnetzwerks kümmern. Solche Heimnetzwerke zu schützen ist nicht ganz einfach: Erstens gibt es sehr viele davon, zweitens sind sie eher klein, drittens haben wir es mit vielen verschiedenen Gerätetypen und Betriebssystemen zu tun und last but not least sind auch die Ressourcen und Fähigkeiten der Nutzer eher begrenzt.

Unsere Daten zeigen, dass in einem durchschnittlichen Plume-Haushalt zurzeit 21 Geräte mit dem Heimnetzwerk verbunden sind[1]. Auch wenn die Zusammenstellung immer etwas anders ausfällt, so können das in einer typische Familie mehrere Smartphones und Computer sein (dazu zählen auch Firmen- oder Schul-Laptops, die zum Arbeiten oder Lernen von zu Hause aus genutzt werden), dazu Tablets, Spielkonsolen und eine Box, ein Stick oder ein TV-Gerät zum Streamen von Videos.

Wenn sich diese Familie dann noch eine intelligente Türklingel, ein smartes Thermostat und einen Sprachassistenten anschafft (weltweit wird es davon bis 2024 schätzungsweise 8,4 Milliarden geben[2]), dazu vielleicht noch intelligente Lautsprecher, Lampen und ein Home Security System, dann schnellt diese Zahl rasant in die Höhe. Auch Gesundheits- und Fitnessgeräte werden immer beliebter und lasten das Netz zusätzlich aus. Dazu zählen nicht nur Hometrainer, sondern auch kleinere Geräte wie der Fitbit-Fitness-Tracker oder die Apple Watch.

Verbindet man all diese Geräte aus dem Internet of Things (IoT) mit dem heimischen WLAN, sind die Probleme fast schon vorprogrammiert[3]. Privatnutzer, von denen viele nicht über tiefgreifende technische Kenntnisse verfügen, machen sich Sorgen über die Sicherheit ihres Heimnetzwerks, wissen aber nicht immer, was zu tun ist. Eine aktuelle Umfrage zeigt, dass Hackerangriffe mit 75 % die Liste der Sicherheitsbedenken in Smart Homes anführen. Der Schutz ihrer Privatsphäre ist für viele Kunden wichtig, doch 40 % der Befragten geben an, dass sie sich mit dem Thema nicht wirklich auskennen[4].

Vor diesen möglichen Bedrohungen für ihr Smart Home haben Verbraucher am meisten Angst

Hackerangriffe

75 %

Spionageversuche der Regierung über intelligente Home-Kameras

53 %

Intelligente Lautsprecher

52 %

Quelle: ADT-Umfrage: Consumers want cyber protection for smart homes

[1] "Cyber intrusion protection for the smart home", Plume blog: https://blog.plume.com/cyber-intrusion-protection-for-the-smart-home
[2] "Report: Voice assistants in use to triple to 8 billion by 2023", Tech Crunch https://techcrunch.com/2019/02/12/report-voice-assistants-in-use-to-triple-to-8-billion-by-2023
[3] 10 IoT incidents that make you feel less secure" CISO MAG: https://cisomag.eccouncil.org/10-iot-security-incidents-that-make-you-feel-less-secure
[4] "ADT Survey: Consumers want cyber protection for smart homes https://www.securityinfowatch.com/residential-technologies/news/21126817/adt-survey-consumers-want-cyber-protection-for-smart-homes

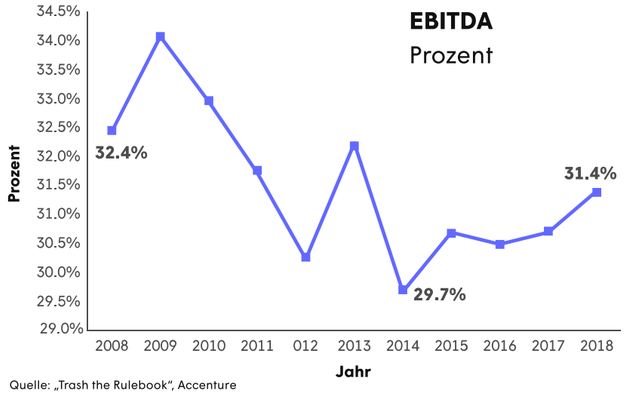
Warum das gesamte Heimnetzwerk für Internetanbieter von Bedeutung ist

Die Kunden von heute wünschen sich ein durchweg gutes WLAN-Erlebnis, bei dem alles mit minimalen Reibungsverlusten verfügbar ist. Eine Leitung und ein Modem oder einen Router bereitzustellen, reicht schon lange nicht mehr aus.

Kunden sind in der Regel keine Experten für IT-Sicherheit. Aber sie wissen, dass sie eine sichere digitale Umgebung brauchen, um sich und ihre Familien zu schützen. Da Heimnetzwerke so komplex sind, fühlen sich viele Benutzer nicht in der Lage, die Sicherheit ihres Netzwerks selbst einzurichten und zu überwachen. In diesem Bereich können sich Internetanbieter als zuverlässige Partner in einem wettbewerbsintensiven Markt etablieren, indem sie ihren Kunden einen sicheren und zuverlässigen WLAN-Zugang im gesamten Haus bieten. Anbieter, die nur eine Leitung in die Wohnung legen, werden auf diese eine Leistung reduziert. Für sie bleibt oft nur die Unterscheidung über den Preis. In einem Bericht aus dem Jahr 2019 stellt das Beratungsunternehmen Accenture treffend fest, dass in der erblühenden Smart Home Ära „das bloße Innehaben einer Position nicht länger als Wettbewerbsvorteil genügt“.[5]

Die Infrastruktur, auf der Internetanbieter traditionell ihre Serviceangebote aufgebaut haben, kann nicht mit den neuen Cloud-Technologien mithalten. Anbieter hingegen, die cloudbasierte Dienste vermarkten, können Updates sehr schnell ausrollen. So können alle Benutzer und alle Geräte stets auf die neuesten und besten Angebote zugreifen. Die Bereitstellung über die Cloud bedeutet auch geringere Kosten für die Überwachung und Wartung von Geräten im Netzwerk. Schließlich ermöglicht die Cloud Internetanbieter auch den Zugriff auf Ressourcen, deren Anschaffung im Alleingang zu teuer wäre. Allerdings sind Cloud-Dienste genau das, was große Technologieunternehmen wie Amazon, Apple und Google am besten können. Diese Unternehmen werden beim Eintritt in die Smart-Home-Ära von einem günstigen Rückenwind beflügelt, während traditionelle Internetanbieter mit zunehmendem Gegenwind zu kämpfen haben.

Geld ausgeben und trotzdem weniger verdienen? Das verursacht nur Kosten und ergibt keinen Sinn



Quelle: „Trash the Rulebook“, Accenture

Auch wenn das Investitionsniveau dank der Kosten pro Abonnent stabil geblieben ist, kämpfen Internetanbieter mit sinkenden Renditen

[5] “Trash the rulebook”, Accenture: https://www.slideshare.net/accenture/trash-the-rulebook-132815757

Internetanbieter befinden sich also an einem kritischen Punkt. Es genügt nicht, einfach nur nach Möglichkeiten zu suchen, wie sie Kosten sparen und bestehende Dienste optimieren können, um ihre heutige Marktposition zu halten. Vielmehr müssen sie in Strategien investieren, die ihnen auch in Zukunft Wachstum und Stabilität sichern. Dazu müssen sie ihr aktuelles Geschäftsmodell umgestalten und neue digitale Produkte und Cloud-Dienste anbieten, die für die Smart-Home-Ära gerüstet sind.

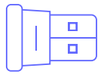
Doch zum Glück können Internetanbieter dabei auf ein starkes Fundament bauen: auf Ihre Kunden, ihre Netzwerke und ihre lokalen Marken. Und auf ihr Know-how. All das hilft ihnen, geschäftlich neue Wege zu beschreiten und ihren Kunden das zu bieten, was sie wollen. Die Sicherheit für Smart Homes steht auf der Wunschliste der Kunden ganz oben.

WARUM ARBEITEN VON ZU HAUSE AUS ZIEMLICH RISKANT SEIN KANN

Arbeiten von zu Hause aus erfreut sich wachsender Beliebtheit, nicht nur in Notsituationen, die das Arbeiten im Betrieb gefährlich oder nahezu unmöglich machen. Auch bei normalem Betrieb genießen die Mitarbeiter die Flexibilität, die das Arbeiten im Homeoffice bietet. Leider versuchen auch Hacker davon zu profitieren und sind in Zeiten voller Angst, Unsicherheit und Zweifel oft besonders aktiv.

Das Arbeiten im Homeoffice birgt laut CISO Magazin eine ganze Reihe von Sicherheitsrisiken[6]:

30 % der Homeoffice-Nutzer greifen nicht über ein Firmen-VPN auf das Unternehmensnetzwerk zu.



40 % der Homeoffice-Nutzer verbinden sich über einen Firmen-Dongle. Der Rest loggt sich über das heimische WLAN oder Handy-Hotspots ein.

In einem durchschnittlichen Plume-Haushalt sind **21 Geräte** mit dem heimischen WLAN-Netzwerk verbunden. Jedes davon hat seine eigenen potenziellen Schwachstellen

Mit anderen Worten: Viele Anwender führen geschäftskritische Arbeiten mit sensiblen Kundendaten auf Rechnern aus, die über Netzwerke mit unbekannten Sicherheitsschwächen verbunden sind. Zusätzlich wimmelt es in diesen Netzwerken nur so vor ungeprüften Geräten. Aus einem gemeinsamen Gutachten der US Cybersecurity and Infrastructure Security Agency und des britischen National Cyber Security Centre geht hervor, dass die Zunahme der Heimarbeit während der COVID-19-Pandemie auch zu einem Anstieg der Angriffe bösartiger Akteure auf Einzelpersonen und Unternehmen geführt hat[7].

> „Mit dem weiteren Fortschreiten der COVID-19-Pandemie nutzen böswillige Akteure diese schwierige Zeit aus, um die Öffentlichkeit und Unternehmen zu schädigen. Dank unserer Zusammenarbeit mit dem NCSC und der gesamten Branche konnten wir diese Bedrohungen verfolgen und entsprechend darauf reagieren. Wir rufen alle auf, vor diesen Bedrohungen auf der Hut zu sein. Achten Sie auf verdächtige E-Mails und wenden Sie sich ausschließlich an vertrauenswürdige Quellen, um Informationen und Updates zu COVID-19 zu erhalten. Wir sitzen alle im selben Boot und können uns nur gemeinsam gegen diese Bedrohungen zur Wehr setzen."
>
> *—Bryan Ware, Assistant Director for Cybersecurity bei CISA*

[6] "1 in 3 Employees don't use VPN to connect to company network while working from home": CISO MAG survey: https://www.cisomag.com/ciso-mag-survey
[7] "UK and US security agencies issue COVID-19 cyber threat update", CISA.gov: https://www.cisa.gov/news/2020/04/08/uk-and-ussecurity-agencies-issue-covid-19-cyber-threat-update

Mit Sicherheitsangeboten können Internet-anbieter mehr Wertschöpfung erreichen

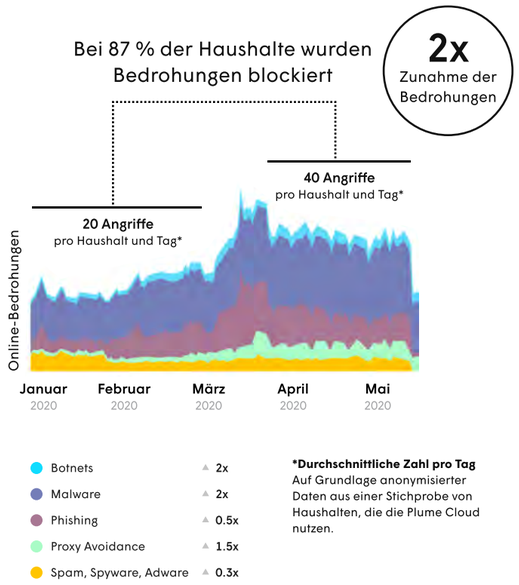
In einer immer vernetzteren Welt stehen Internetanbieter vor einer großen Herausforderung: Sie müssen weiterhin schnelle und tadellos funktionierende Verbindungen anbieten, aber auch einen Weg finden, sich von anderen abzuheben. Erreichen können sie das, indem sie eine sicherere IT-Umgebung für ihre Kunden und deren Familien schaffen, die mehr Kontrolle und Transparenz über die persönliche IT-Sicherheit bietet. Plume hat es sich zur Aufgabe gemacht, das Portfolio der Internetanbieter um modernste Sicherheitslösungen zu ergänzen – auf der Grundlage von hochmoderner KI und maschinellem Lernen.

Bill McFarland, CTO von Plume, prognostiziert, dass die Zahl der vernetzten Geräte in einem durchschnittlichen Plume-Haushalt von derzeit ca. 21 auf über 38 anwachsen wird – und zwar in allen Kategorien: Computer, Mobiltelefone, Tablets, Set-Top-Boxen, Sprachassistenten, Smart-TVs, Drucker, Überwachungskameras, Spielkonsolen und mehr[8].

Und jedes dieser Geräte ist ein potenzieller Angriffspunkt. Ausgehen können diese Angriffe von bestimmten Websites und den Servern, mit denen sie verbunden sind. Die Angreifer nutzen dafür unter anderem schwache oder mehrfach verwendete Passwörter oder ungepatchte Software. Ihre Angriffe erfolgen zum Beispiel in Form von gezieltem Phishing, Spam, Betrugsangriffen und anderen bösartigen Attacken.

In der Zeit von März bis Mai 2020 stieg die Nutzung von Heimnetzwerken um 120 %. Im selben Zeitraum wurden in 87 % der Häuser, die mit Plume-Systemen ausgestattet sind, Bedrohungen abgewehrt. Die Zahl der Angriffe auf diese Haushalte hat sich im selben Zeitraum gegenüber den Vormonaten verdoppelt und stieg von 20 auf 40 pro Tag. Malware führte dabei die unrühmliche Liste an[9]. Schützen wir diese Haushalte vor solchen Bedrohungen, profitieren die Kunden von einem echten Mehrwert. Der Internetanbieter wird zum vertrauenswürdigen Partner, mit dem sie anderen immer einen Schritt voraus sind. Das verstehen wir unter einem verbesserten Kundenerlebnis.

Zunahme von Cyber-Angriffen in der Quarantäne-Zeit



INTERNETANBIETER MÜSSEN SICH DEN HERAUSFORDERUNGEN DES IOT STELLEN

Moderne Sicherheitslösungen für die Nutzer von Home-WLAN-Netzen anzubieten bedeutet eine Menge Arbeit für Internetanbieter – und das hat verschiedenste Gründe:

- Weltweit gibt es schätzungsweise mehr als 20 Milliarden IoT-Geräte[10]
- Verbraucher gehen davon aus, dass die Anbieter von Smart-Home-Geräten wie Amazon, Apple, Google etc. auch für die entsprechende Sicherheit sorgen. Internetanbieter werden dadurch an den Rand gedrängt
- IoT-Geräte stellen aus verschiedenen Gründen eine neue Bedrohungsstufe für Heimnetzwerke dar[11]:
  - *Die Geräte laufen nicht über Browser, sondern verbinden sich direkt mit dem Netzwerk*
  - *Viele Hersteller bringen nicht oft Patches für ihre Geräte heraus*
  - *Viele Verbraucher aktualisieren ihre Software nicht, selbst wenn Patches verfügbar sind*
  - *Die Verbraucher legen keine sicheren Passwörter fest oder ändern die Standard-Passwörter nicht*

Wenn Internetanbieter auf diese Dinge eingehen, können sie sich diese Bedürfnisse zum strategischen Vorteil machen. Je mehr Menschen von zu Hause aus arbeiten, Kurse belegen und Entertainment-Videos streamen, umso beliebter und notwendiger wird das Internet der Dinge und die damit verbundenen Geräte.

Nun können Internetanbieter entweder jede Menge Personal und Ressourcen dafür aufwenden, jedes heute und in Zukunft auf dem Markt verfügbare IoT-Gerät zu schützen – oder aber sie entscheiden sich für eine Partnerschaft mit Plume und bieten ihren Kunden genau den vielschichtigen Schutz, den diese brauchen[12].

[8] "The smart home report 2019: how optimization, security, and personalization are shaping smart home 2.0", Plume: https://www.popsci.com/smart-home-fix-guide
[9] "Cyber threats climb during COVID-19", Plume IQ May 2020: https://blog.plume.com/resources/newsletters/cyber-threats-climb-during-covid
[10] "The Wired guide to the Internet of things", Wired: https://www.wired.com/story/wired-guide-internet-of-things
[11] Inside the smart home: Device threats and attack scenarios" Trend Micro: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/inside-the-smart-home-iot-device-threatsand-attack-scenarios
[12] "Plume Advanced IoT Protection™: Defending your network", Plume blog: https://blog.plume.com/advanced-iot-protection

So bekommen Sie Sicherheitsprobleme mit Plume in den Griff

In Sachen Sicherheit setzt Plume auf Layering: Verteidigung aus der Tiefe. Der Plume Guard™-Service als Bestandteil der HomePass™-Suite adressiert alle wichtigen Fragen rund um die „KI-Nahrungskette“, um es mit den Worten von Plume-Mitbegründer und Vice President für Produktentwicklung Adam Hotchkiss zu sagen. Hierbei bildet jedes Layer die Grundlage für das nächste Kompetenz-Niveau[13]. Diese Layer sind:

- **Datenerfassung:** Was ist passiert?
- **Datenanalyse:** Warum ist es passiert?
- **KI-Prognosemodell:** Was wird als Nächstes passieren?
- **Änderungen durch KI vorwegnehmen:** Ändern, was als Nächstes passiert

Auf diese Weise kann Guard Bedrohungen im ganzen Haus neutralisieren. Unterstützt wird das System durch cloudbasierte Echtzeit-Schutzalgorithmen und intelligentes maschinelles Lernen. Die Bereitstellung des Systems erfolgt ganz einfach über Plume Pods oder Ihr OpenSync™-fähiges Gateway. Verwaltet wird es mit der nutzerfreundlichen HomePass-App.

Was ist OpenSync?

OpenSync ist ein Open-Source-Framework, das die Bereitstellung und Verwaltung von Smart Home Services aus der Cloud ermöglicht – schnell und einfach auf verschiedene Größenordnungen skalierbar[14]. Es erleichtert die Kommunikation zwischen der Cloud und der CPE-Hardware. Als gemeinsame Middle-Layer-Lösung ermöglicht OpenSync die Bereitstellung von Angeboten wie von adaptivem WLAN und KI-gestützten Sicherheitsmaßnahmen über alle kompatiblen Geräte. Die Software wurde ursprünglich von Samsung, Comcast, Bell Canada, Liberty Global und Plume gemeinsam entwickelt und 2018 als Open Source veröffentlicht. Die Initiative wird von großen Internetanbietern, Geräteherstellern und Branchenorganisationen unterstützt, darunter auch Charter Communications und das Telecom Infra Project (TIP)[15].

[13] “Plume at ANGA COM 2019 – International keynote: The AI advantage”: https://www.youtube.com/watch?time_continue=190&v=adPaYplLjBU&feature=emb_logo

[14] “Open Sync”: https://www.opensync.io/about

[15] “Plume at Broadband World Forum 2018 - Fahri Diner talks OpenSync with Light Reading”: https://www.youtube.com/watch?v=_iJGw6gTYqk&feature=youtu.be&t=167

[16] “Cyber-intrusion protection for the smart home”, Plume blog: https://blog.plume.com/cyber-intrusion-protection-for-the-smart-home

KI-GESTÜTZTE SICHERHEITSLÖSUNGEN WIE GUARD BIETEN EINE REIHE VON FUNKTIONEN, DIE IN IHRER SUMME EINEN UMFASSENDEN SCHUTZ BIETEN:

Advanced Device Typing: Die ADT-Technologie klassifiziert 95 % der Geräte innerhalb weniger Minuten und passt die Aussteuerung über die Cloud an die Anforderungen des jeweiligen Gerätes an. Die Informationen werden den Internetanbietern zur Verfügung gestellt, die diese zur Verwaltung der Smart Home Services nutzen können.

Geräteschutz im ganzen Haus: Mithilfe KI-basierter Analysen wird verhindert, dass Geräte sich mit bedrohlichen Servern verbinden und möglicherweise mit Malware, Spyware oder Ransomware infiziert werden oder Phishing-Angriffen zum Opfer fallen.

Erkennung und Blockierung von Eindringlingen: Der IP-basierte Online-Schutz verhindert, dass Angreifer von außen Zugriff auf Heimnetzwerke erlangen, und benachrichtigt Benutzer über Attacken auf ungeschützte Geräte[16].

Verhaltensanalyse und Erkennung von Anomalien: Die Guard Anomalieerkennung nutzt Machine Learning, um die normale IoT-Geräteaktivität zu verstehen und zu dokumentieren. Abweichungen vom gewohnten Verhalten werden umgehend geprüft und können bei schwerwiegenden Anomalien sogar zu automatischen Gerätesperrungen führen.

Behebung und Isolation: Werden starke Abweichungen erkannt, sperrt Plume automatisch die betroffenen Verbindungen und schottet bestimmte Geräte des Kunden ab, um die Verbreitung von schädlicher Software zu verhindern.

Netzwerkweites Sicherheits-Dashboard: Verfolgen Sie die Geschehnisse in Ihrem Netz aus verschiedenen Perspektiven wie z. B. nach Aktivitäten, Zeiträumen oder geografischer Verteilung. So können Sie schnell auf Infrastruktur-Bedrohungen reagieren.

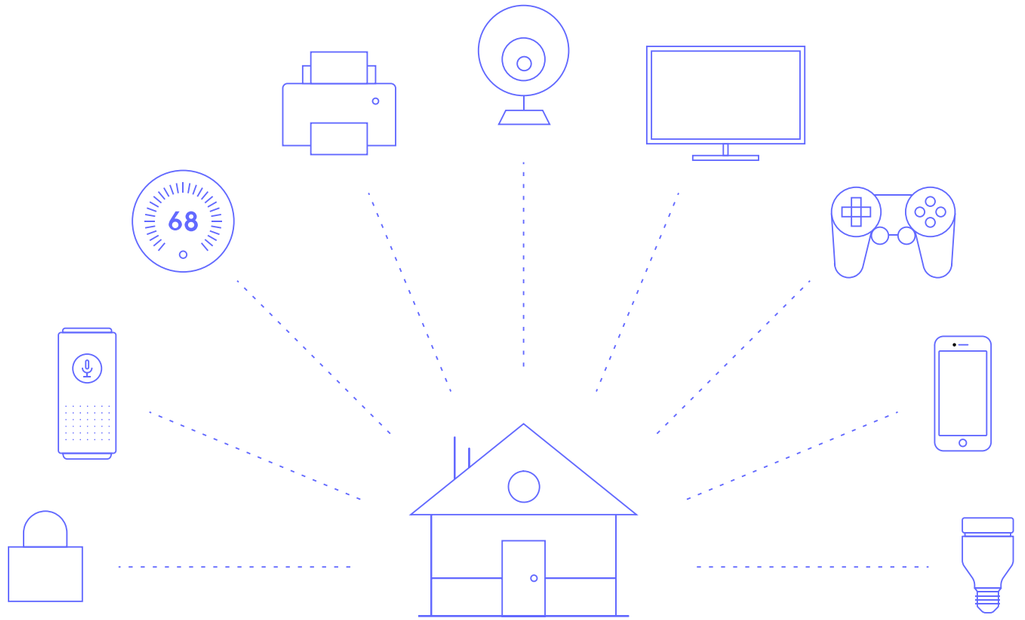
Über die Plume-Daten-Dashboards können Kundendiensttechniker Netzwerkbedrohungen überwachen und Benutzerprobleme bis auf Geräteebene beheben. Im Gegensatz zu vielen anderen Lösungen bietet Guard technologie- unabhängige Sicherheit: Dank der erweiterten IoT-Schutzfunktionen können Kunden IoT-Hardware ihrer Wahl verwenden und sogar verschiedene Marken miteinander kombinieren. Die optimalen IoT-Schutzmechanismen von Guard sorgen jederzeit für maximale Sicherheit.

Diese Funktionen zielen speziell auf Bedrohungen für IoT-Geräte ab. Über Verhaltensanalysen und Anomalieschutz werden Verhaltensweisen erkannt, die für die einzelnen Geräte in diesem Netzwerk untypisch sind[17]. Bis das ungewöhnliche Verhalten genauer untersucht worden ist, kann das Gerät sogar unter Quarantäne gestellt werden.

Die Überwachung von IoT-Geräten im Netzwerk, kombiniert mit Intrusion Protection und Outbound-IP-Protection, blockiert automatisch riskante IP-basierte Interaktionen mit verbundenen Geräten im Haus. Diese Daten fließen in ihrer Gesamtheit in die intelligenten Lösungen ein und machen diese dadurch für alle Nutzer, die den Plume HomePass installiert haben, noch intelligenter. Anhand dieser Daten kann die Technologie sowohl das Benutzerverhalten als auch die online existierenden Bedrohungen besser verstehen, ebenso wie ihre Verbreitung, ihre Prävalenz und ihre Ziele. Und ein tieferes Verständnis ermöglicht bessere und schnellere Reaktionen auf Bedrohungen. So wird der Schutz, den HomePass-Mitglieder in ihrem Netzwerk genießen, Tag für Tag besser und besser.

Die Benutzer müssen das Gefühl haben, dass ihr Netzwerk ihre Anforderungen erfüllt und sie schützt – und nicht andersherum. Internetanbieter kommen nicht umher, ihren Kunden personalisierte Erfahrungen, Produkte und Dienstleistungen anzubieten. Die HomePass-App schafft genau diese persönliche Note: Sie warnt Benutzer vor Problemen und gibt ihnen die Möglichkeit, Optionen so anzupassen, dass diese Probleme behoben werden. Und sobald Internetanbieter die Wünsche und Bedürfnisse ihrer Kunden verstanden haben, können sie ihnen immer mehr anbieten und einen noch höheren Mehrwert schaffen.

So können Nutzer beispielsweise mit Sense™ ihre vorhandenen WLAN-Geräte zu einem Bewegungserkennungsnetzwerk kombinieren, so dass sie sich in ihrem Haus noch sicherer fühlen[18]. Access™ bietet sicheren WLAN-Gastzugriff ohne separates Gastnetzwerk und ermöglicht es den Benutzern, sowohl die Nutzung als auch die abgerufenen Inhalte in ihrem Haushalt zu steuern. Derselbe Dienst lässt Eltern Regeln für ihre Kinder festlegen und den Inhalt bestimmen, auf den diese zugreifen können. Einfache Optionen zur Netzwerkverwaltung stellen sicher, dass der Kunde die volle Kontrolle über die Nutzung seines Netzwerks behält – zum Schutz seines Netzwerks und seiner Familie.



[17] "Plume Advanced IoT Protection™: Defending your network", Plume blog: https://blog.plume.com/advanced-iot-protection
[18] "Give your home a sixth sense with Plum Motion", Plume blog: https://blog.plume.com/give-your-home-a-sixth-sense-with-plume-motion

Vorteile für Unternehmen

Die Services, die Sie über Plume anbieten, klingen völlig anders als das, was Internetanbieter bisher zu bieten hatten. Und schließlich wollen Sie ja auch kein x-beliebiger Anbieter mehr sein. Hat der Internet- anbieter die Grundlagen für die Verbindung geschaffen, muss er in der Lage sein, die Privatsphäre und die Daten seiner Kunden sowie das Netzwerk vor bösartigen Angriffen zu schützen. Plume macht genau das möglich und verbessert die Sicherheit in den Netzwerken der Nutzer[19]. Statistiken belegen eindeutig: Dienstleister, die mehr – und vor allem Besseres – zu bieten haben als andere, sind wettbewerbsfähiger und weitaus beweglicher in dynamischen Märkten.

Internetanbieter, die Plume Services im Portfolio haben, profitieren von zahlreichen Vorteilen:

- Höhere Kundenzufriedenheit und höhere Net Promoter Scores
- Weniger Kundenabwanderung
- Chancen für neue Produkte, Services und Umsatzquellen
- Echtzeit-Daten-Insights in die Performance von Technologie und Netzwerk
- Bessere Dateneinblicke in die Gewohnheiten und Bedürfnisse der Kunden
- Neue KI-Funktionen für den Kundenservice und vieles andere

Mit Plume können Internetanbieter ihr Geschäft strategisch weiterentwickeln, indem sie sich auf einem immer härter umkämpften Markt von anderen abheben und mit neuen Wegen mehr Abonnenten gewinnen. Und dank des hohen Mehrwerts, die das innovative Smart Home Portfolio bietet, werden diese neuen Abonnenten zu treuen und langlebigen Kunden.

Auch aus finanzieller Sicht ist Plume für Internetanbieter sehr attraktiv. Der Service erhöht den ARPU und senkt die Kosten für Kundendienstanrufe und Technikereinsätze. Aus technischer Sicht hilft eine gründlichere Analyse des Kundenverhaltens den Internetanbietern, die Anforderungen an ihr Netzwerk besser zu verstehen. Die Techniker haben einen besseren Einblick in potenzielle Probleme und können so ihren Service immer optimal am Rollen halten.

Churn reduziert um bis zu:

30 % ↓

ARPU erhöht um bis zu:

13 € ↑

Support-Anrufe reduziert um bis zu:

51 % ↓

Technikereinsätze reduziert um:

67 % ↓

WENN DAS AUSERGEWÖHNLICHE ZUR NORMALITÄT WIRD

Die COVID-19-Krise hat mit ihrer schnellen Ausbreitung Netzwerke rund um den Globus auf eine harte Probe gestellt[20]. Ganze Familien mussten über längere Zeit von zu Hause aus arbeiten und lernen, was ihre Netzwerke bis aufs Äußerste belastete.

Kurz nach den ersten Lockdowns Anfang 2020 lag die Spitzenauslastung an Wochentagen 45 % über dem normalen Wert[21]. In Europa stieg der durchschnittliche Upstream-Traffic um rund 55 %. Dies ist vor allem auf die Zunahme von Videokonferenzen und Arbeiten aus dem Homeoffice zurückzuführen. Auch andere Auswirkungen waren zu beobachten:

- Erhöhte Bandbreitennutzung mehrerer Geräte im Netzwerk
- Verstärkter Einsatz neuer Software (Streaming, Videokonferenzen, Fernzugriffssoftware usw.) durch neue Benutzer
- Mehr Angriffe[22], auch durch DDoS[23], Ransomware und Whaling
- Immer mehr junge Nutzer im Homeschooling, die sich mit IT-Sicherheit noch nicht so gut auskennen[24]

[19] "Plume AI Security" https://discover.plume.com/ai-security-data-sheet
[20] "Redoing the math: the impact of COVID-19 on broadband networks", Nokia blog: https://www.nokia.com/blog/redoing-the-math-the-impact-of-covid-19-on-broadband-networks
[21] "Network traffic insights in the time of COVID-19: April 9 update", Nokia blog: https://www.nokia.com/blog/network-traffic-insights-time-covid-19-april-9-update
[22] "4,000% increase in ransomware emails during COVID-19", Canada's National Observer: https://www.nationalobserver.com/2020/04/14/news/4000-increase-ransomware-emails-during-covid-19
[23] "Network traffic insights in the time of COVID-19: April 9 update", Nokia blog: https://www.nokia.com/blog/network-traffic-insights-time-covid-19-april-9-update
[24] The COVID-19 pandemic has changed education forever. This is how", https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning

Zeit zum Handeln

In einer Zeit, in der Geräte ständig im Netz sind, nehmen die Sicherheitsbedenken der Nutzer weiter zu – zu Recht. Internetanbieter, die ihren Kunden eine sichere, bequeme und intelligente All-in-One-Lösung zum ganzheitlichen Schutz ihres Heimnetzwerks bieten, stechen positiv aus der Masse der Anbieter heraus.

Jetzt ist genau die richtige Zeit für Internetanbieter, einen strategischen Wandel in ihrem Unternehmen voranzutreiben und Smart Home Services in ihr Portfolio aufzunehmen. Der beste Weg dahin führt über eine Partnerschaft mit einem Anbieter, der diesen Wandel schnell, nahtlos und kosteneffizient begleiten kann. Plume macht genau das möglich: mit einer cloudbasierten Bereitstellungsplattform, der passenden Hardware, der HomePass-App, erstklassigem Support und vielen anderen Tools. So können Internetanbieter ihre Kunden noch besser und umfassender bedienen und gleichzeitig ihr Geschäft zukunftsträchtig ausbauen.

Sie möchten mehr über HomePass, die Smart Home Services Suite von Plume, erfahren oder einen Termin zur Produktdemonstration vereinbaren? Besuchen Sie unsere Website oder setzen Sie sich gleich heute noch mit uns in Verbindung.