BERICHT (2021)

IoT im Unternehmen: Reges Treiben in menschenleeren Büros

Was passiert, wenn smarte Geräte monatelang allein am Arbeitsplatz zurückbleiben?

zscaler™

Seit Ausbruch der COVID-19-Pandemie kehrte an vielen Unternehmensstandorten monatelang gespenstische Ruhe ein. Im Innern der menschenleeren Gebäude herrschte jedoch rege Betriebsamkeit. Zahlreiche IoT-Geräte waren weiterhin mit dem Netzwerk verbunden: Smartwatches, digitale Beschilderung, vernetzte Drucker usw., die wie gehabt Daten aktualisierten, Funktionen ausführten und auf Befehle warteten.

Die Chancen, die sich inmitten der globalen Umstellung auf Remote-Arbeit erschlossen, ließen sich Cyberkriminelle natürlich nicht entgehen. Im Ergebnis wurden jede Stunde 833 IoT-Schadprogramme blockiert.

Von Smartwatches und IP-Kameras über Fahrzeuge bis hin zu Möbeln mit integrierten Musikkomponenten – das Spektrum der IoT-Geräte in Unternehmensnetzwerken wird immer breiter und bunter. Wenngleich alle Geräte zumindest teilweise SSL-Verschlüsselung für ihre Kommunikation verwenden, erfolgen ganze 76 Prozent der Transaktionen über unverschlüsselte Klartextkanäle. Um zu verhindern, dass Angreifer diese Geräte als Einfallsvektor ausnutzen, müssen Unternehmen ihre Netzwerke mithilfe von Zero-Trust-Richtlinien und -Architekturen schützen. In diesem Bericht analysieren die Bedrohungsexperten des ThreatLabz-Teams von Zscaler die Risiken durch zugelassene und inoffizielle IoT-Geräte sowie IoT-Malwaretrends anhand von Daten aus der Zscaler Cloud, die über einen zweiwöchigen Zeitraum erfasst wurden.

Im Bericht werden Ergebnisse aus zwei Studien präsentiert: einer Fingerprinting-Studie zur Analyse von IoT-Geräten und dem damit verbundenen Traffic sowie einer auf Daten aus der Zscaler Cloud basierenden Studie zur Untersuchung von IoT-Malware. Da IoT-Geräte – insbesondere inoffiziell genutzte Geräte – nicht mit Agents ausgestattet sind, stammen die erfassten Daten ausschließlich von Geräten und Angriffen auf Netzwerke an physischen Unternehmensstandorten. Die Daten für diesen Report wurden im Zeitraum vom 15. bis 31. Dezember 2020 erhoben, als die Mehrzahl aller nicht als systemrelevant eingestufter Unternehmensstandorte Covid-bedingt geschlossen war.

Anstieg der IoT-spezifischen Malware um 700 % im Vergleich zum Vorjahr.

Haupterkenntnisse

- IoT-Malware in Unternehmensnetzwerken hat seit 2019 um 700 Prozent zugenommen, obwohl weltweit ein Großteil der Belegschaft im Homeoffice arbeitet im Vergleich zu unserer Studie des Jahres 2019.

- Unterhaltungs- und Hausautomatisierungsgeräte stellten aufgrund ihrer Vielfalt, des geringen Anteils an verschlüsselter Kommunikation und der Verbindungen zu verdächtigen Zielen das größte Risiko dar.

- Gafgyt und Mirai – Malwarefamilien, die häufig in Botnetzen verwendet werden, waren für 97 Prozent der IoT-Malware-Payloads verantwortlich, die von der Zscaler Cloud blockiert wurden.

- 98 Prozent der blockierten IoT-Angriffe richteten sich gegen Unternehmen aus den Branchen Technologie, Fertigung, Einzel- und Großhandel sowie Gesundheitswesen.

- Die Mehrzahl der Angriffe ging von China, den USA und Indien aus.

- Überwiegend richteten sich die IoT-Angriffe gegen Ziele in Irland, den USA und China.

Fingerprinting von IoT-Geräten

Häufigste Geräte

Insgesamt untersuchten die Experten von ThreatLabz über eine halbe Milliarde IoT-Gerätetransaktionen. Dabei wurden 553 unterschiedliche IoT-Gerätetypen von 212 Herstellern identifiziert und in 21 Kategorien eingeteilt. Fast 65 Prozent aller Geräte fielen in die drei häufigsten Kategorien: Set-Top-Boxen (29 Prozent), Smart-TVs (20 Prozent) und Smartwatches (15 Prozent).

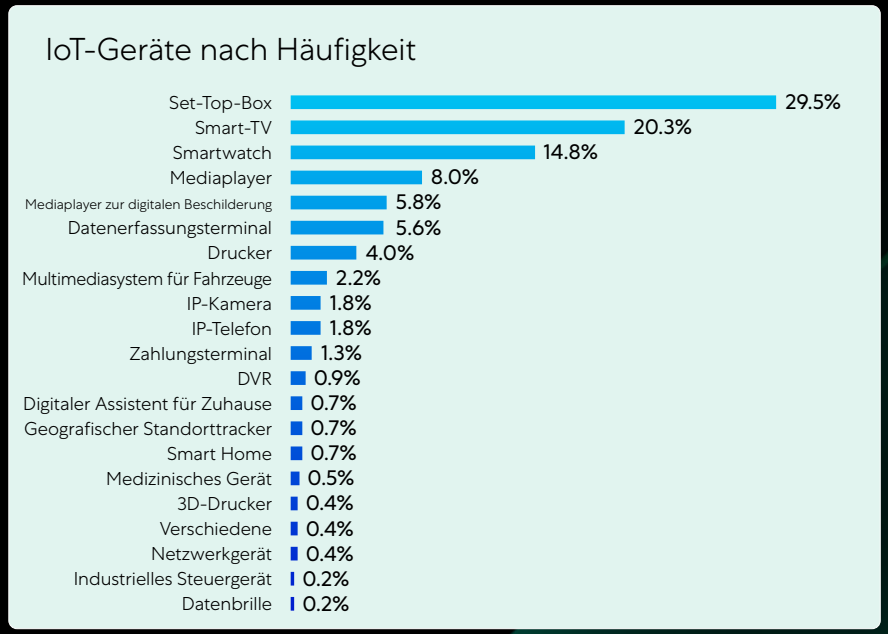
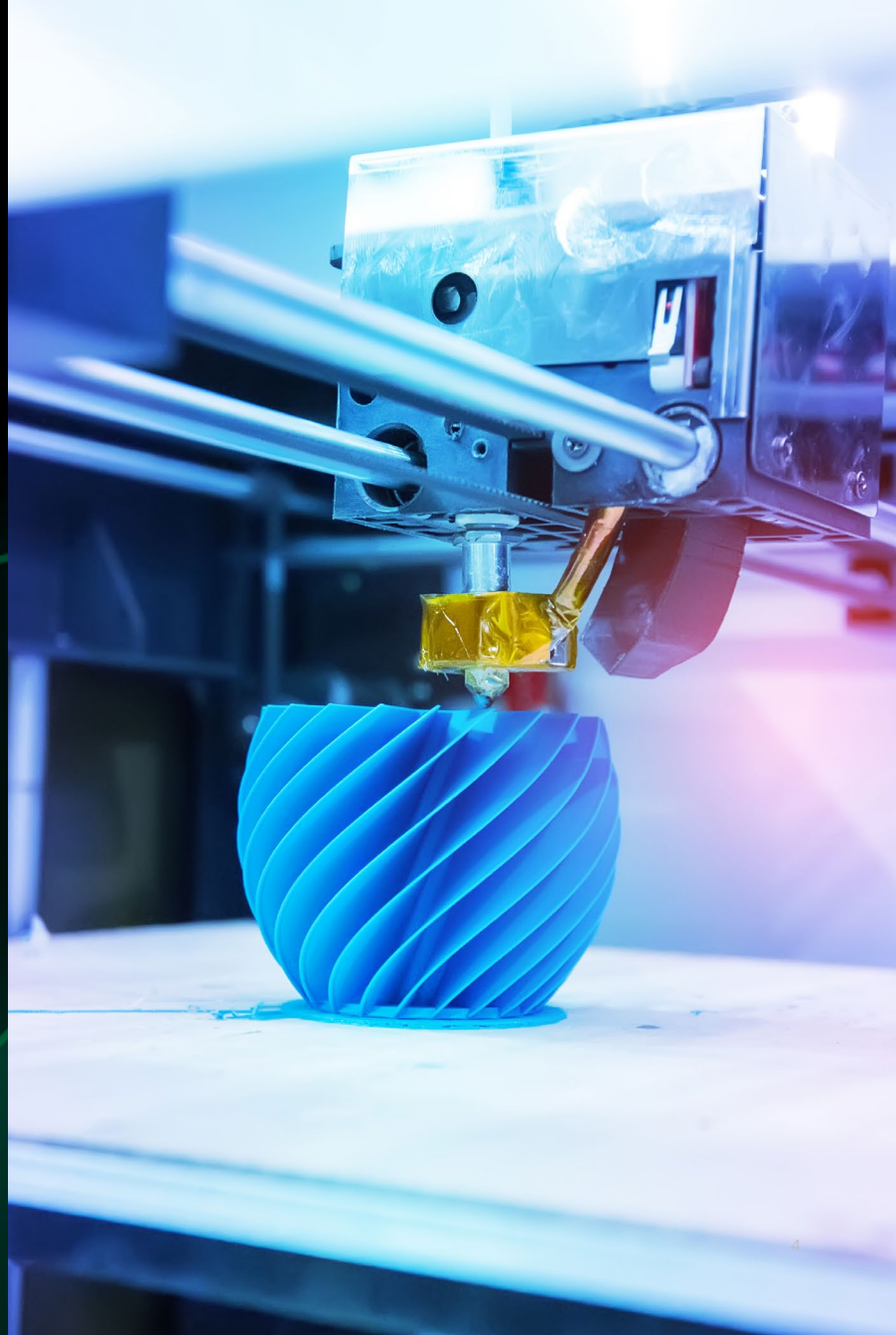


Abb. 1: IoT-Geräte nach Häufigkeit



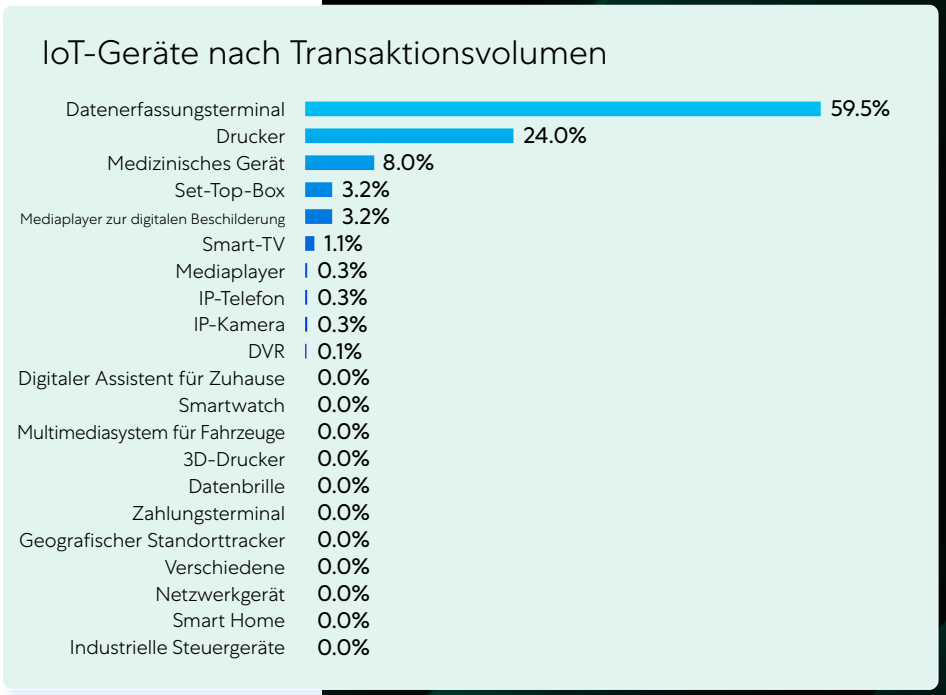
Internet der technischen Kuriositäten?

Das „Internet der Dinge“ expandiert stetig und umfasst mittlerweile Kategorien, die viele IT-Teams womöglich gar nicht auf dem Schirm haben. Bei der Analyse der mit der Cloud vernetzten Geräte stießen die ThreatLabz-Experten auf einige unerwartete Kandidaten:

- **Smarte Kühlschränke:** Ein smarter Kühlschrank von Samsung kann Musik, Videos und Inhalte vom Mobiltelefon des Besitzers auf einen Bildschirm an der Kühlschranktür streamen.
- **Lampe mit Musik:** Ikea und Sonos haben eine Tischleuchte namens „Symfonisk“ mit integriertem Mediaplayer auf den Markt gebracht.
- **Autos:** Fahrzeug-Mediaplayer von Tesla und Honda stellten Verbindungen zu Unternehmensnetzwerken her.
- **WLAN-Speicherkarten:** WLAN-Speicherkarten von Eye Fi, die normalerweise in Kameras zum Speichern und Weiterleiten von Fotos verwendet werden, schickten Daten durch die Zscaler Cloud.

Gesprächigste Geräte

Auf IoT-Geräte entfielen in dem zweiwöchigen Beobachtungszeitraum 0,038 Prozent aller Transaktionen in der Zscaler Cloud. Bestimmte Gerätetypen hatten einen sehr viel höheren Anteil am gesamten Transaktionsvolumen als andere. Datenerfassungsterminals und Drucker machten allein über 80 Prozent des gesamten IoT-Traffics aus (siehe Abb. 2).



Datenbasis: 575.091.158 Transaktionen von IoT-Geräten
Abb. 2: Transaktionen von IoT-Geräten

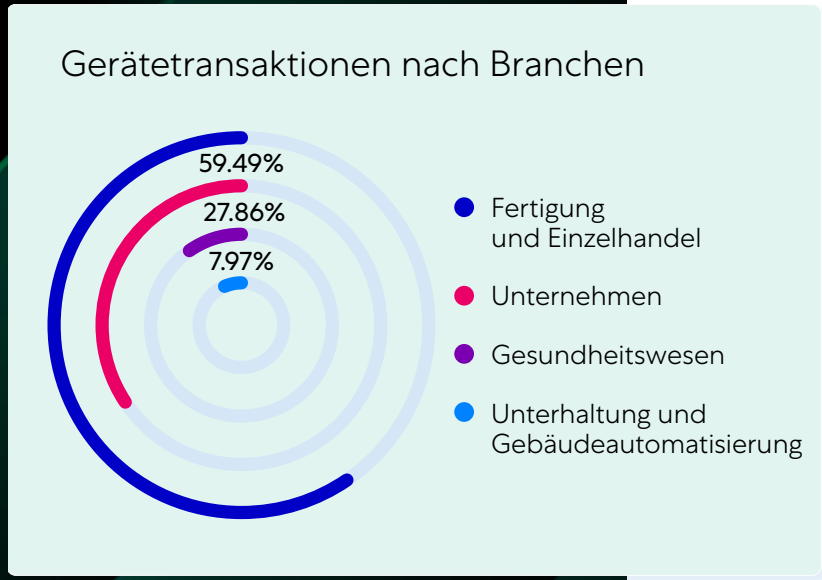


Abb. 3: IoT-Geräte nach Typ

Traffic nach Geräten – branchenbezogene Klassifizierung

IoT-Geräte wurden weiter nach Branchen in vier Kategorien eingeteilt:

- **Geräte für Fertigung und Einzelhandel** hatten einen Anteil von 59 Prozent am gesamten Transaktionsvolumen. Das Spektrum umfasste 57 verschiedene Gerätetypen von 20 Herstellern, darunter 3D-Drucker, Geolokalisierungs-Tracker, industrielle Steuergeräte, Multimediasysteme für Fahrzeuge, Datenerfassungsterminals und Zahlungsterminals.
- **Unternehmensgeräte** wie Mediaplayer zur digitalen Beschilderung, digitale Videorekorder, IP-Kameras und -Telefone, Drucker sowie Netzwerkgeräte hatten einen Anteil von 28 Prozent am gesamten Transaktionsvolumen.
- **Geräte für das Gesundheitswesen** hatten einen Anteil von acht Prozent am gesamten Transaktionsvolumen. Insbesondere handelte es sich dabei um Medizinprodukte, die größtenteils von drei Herstellern stammten: GE Healthcare, Abbott Laboratories und HOLOGIC.
- **Unterhaltungs- und Gebäudeautomatisierungsgeräte** hatten einen Anteil von fünf Prozent am gesamten Transaktionsvolumen, der von einer Vielzahl von Geräten wie digitalen Assistenten für Zuhause, Mediaplayern, Set-Top-Boxen, Datenbrillen, Smart-Home-Geräten, Smart-TVs und Smartwatches generiert wurde. Diese machten zwar den geringsten Prozentsatz der Transaktionen aus, wiesen aber die größte Vielfalt auf und umfassten eine Reihe von Verbrauchergeräten – insgesamt 420 Geräte von 150 verschiedenen Herstellern.

IoT-Geräte nutzen meistens Klartext zur Kommunikation

Die ThreatLabz-Experten stellten fest, dass 76 Prozent aller Transaktionen von IoT-Geräten über Klartextkanäle und nur 24 Prozent der Transaktionen über sichere verschlüsselte Kanäle erfolgten. Dieser Anteil erscheint zwar inakzeptabel niedrig, stellt aber eine fast dreifache Verbesserung gegenüber den Ergebnissen unserer Studie von 2019 war, als nur 8,5 Prozent der IoT-Kommunikation verschlüsselt waren. Dennoch besteht weiterhin einSicherheitsrisiko: Für Angreifer ist es viel einfacher, Klartextkommunikation auszuspähen oder, schlimmer noch, abzufangen und zu modifizieren, was dem Missbrauch von IoT-Geräten zu bösartigen Zwecken Vorschub leistet.

Alle 553 in der Studie analysierten Geräte verwendeten SSL-Verschlüsselung in gewissem Umfang, wobei der Prozentsatz der tatsächlich verschlüsselten Kommunikation jedoch stark nach Gerätetyp variierte. Unternehmens- und Gebäudeautomatisierungsgeräte kommunizierten fast ausschließlich in Klartext, während Geräte für das Gesundheitswesen ungefähr die Hälfte ihrer Transaktionen verschlüsselten.

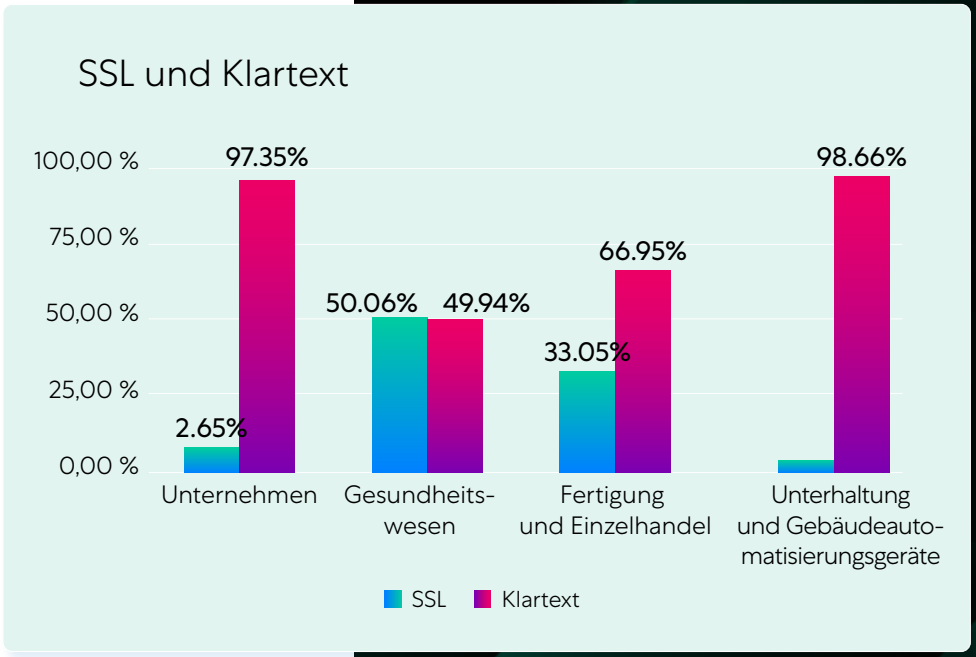


Abb. 4: Prozentualer Anteil verschlüsselter Kommunikationen nach Gerätetyp

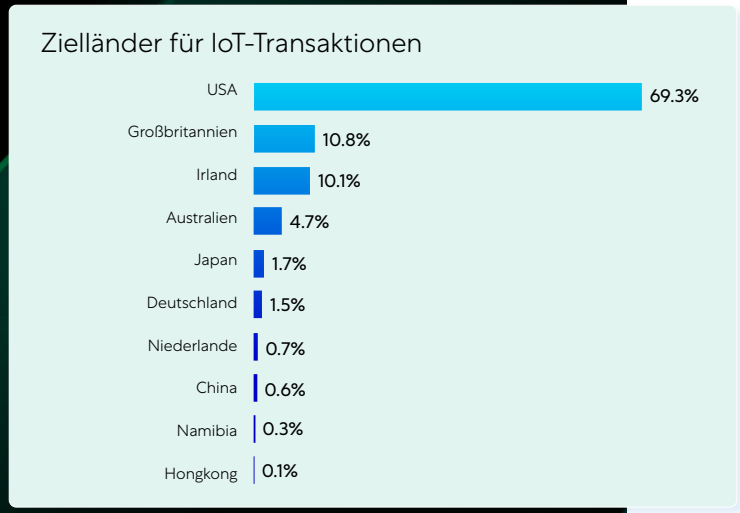


Abb. 5: Häufigste Zielländer für IoT-Kommunikation

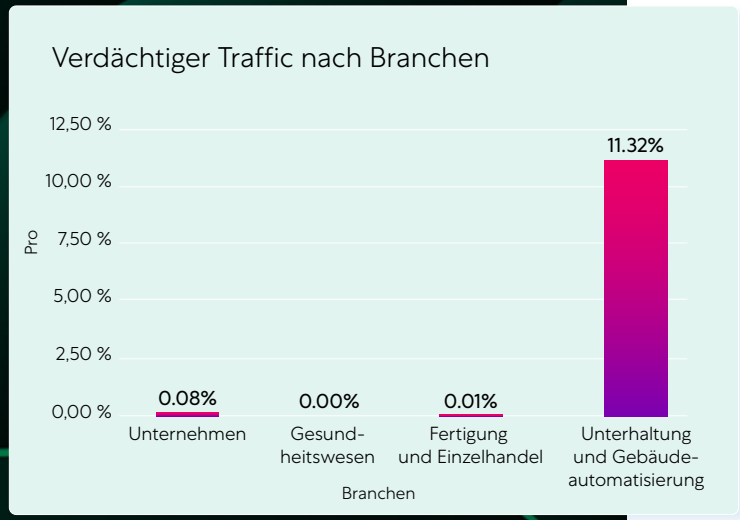


Abb. 4: Prozentualer Anteil verdächtigen Traffics nach Gerätetyp

Mit welchen Ländern kommunizieren die IoT-Geräte?

Die ThreatLabz-Experten analysierten, in welche Zielländer IoT-Geräte Daten weiterleiteten. Dabei handelt es sich mehrheitlich um legitime Kommunikation, die dem Verwendungszweck von IoT-Geräten, nämlich dem Senden und Empfangen von Daten, entspricht. 69 Prozent des Traffics floss in die USA als bei Weitem beliebtestes Zielland, gefolgt von Großbritannien (11 Prozent) und Irland (10 Prozent). Die zehn häufigsten Zielländer werden nachstehend aufgeführt.

Unterhaltungs- und Gebäudeautomatisierungsgeräte schicken Daten am wesentlich wahrscheinlicher nach China und Russland

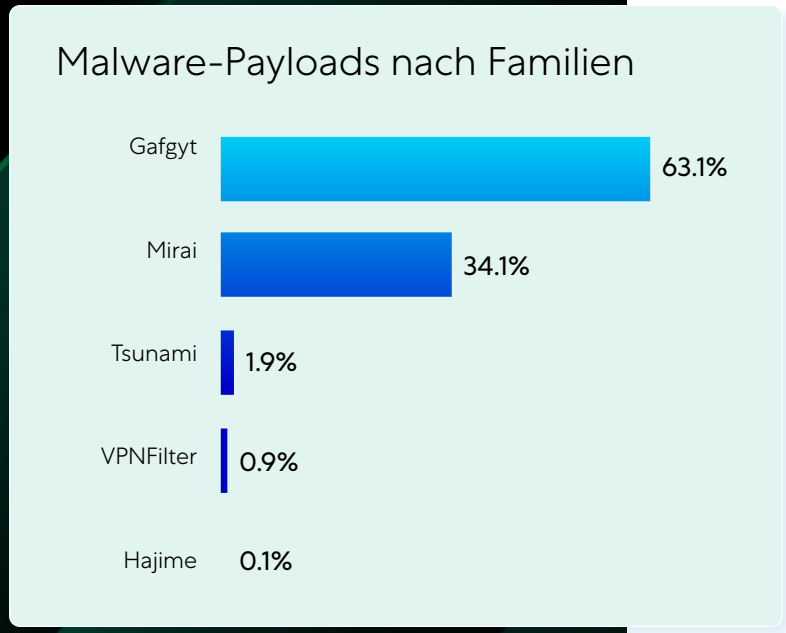
Elf Prozent des Traffics von Unterhaltungs- und Gebäudeautomatisierungsgeräten gingen nach China und Russland. Obwohl es sich dabei größtenteils um legitimen, harmlosen Traffic handelt, stuft ThreatLabz diese Zielländer aufgrund des Risikos von Staatsspionage und weiteren Gefährdungen als verdächtig ein. Dieser verdächtige Traffic kam fast ausschließlich (99,9 Prozent) von Smart-TVs und Set-Top-Boxen.

Umgekehrt verhielt es sich mit Geräten, die für Anwendungsfälle in Unternehmen, Gesundheitswesen, Fertigung und Einzelhandel entwickelt wurden – insgesamt ging weniger als 0,1 Prozent ihres Traffics in verdächtige Zielländer.

IoT-Malwarestudie

Während des zweiwöchigen Zeitraums der ThreatLabz-Studie zu IoT-spezifischen Malwareaktivitäten in der Zscaler Cloud wurden Daten aus demselben Zeitraum ausgewertet, der für die IoT-Gerätefingerabdruckstudie maßgeblich war.

Insgesamt wurden 300.000 Transaktionen in Verbindung mit IoT-Malware, Exploits und Command-and-Control-Kommunikationen blockiert. Das bedeutet einen Anstieg um fast 700 Prozent gegenüber dem Vergleichszeitraum im Vorjahr. Innerhalb des zweiwöchigen Beobachtungszeitraums wurden 900 verschiedene Malware-Payloads von 18.000 unterschiedlichen Hosts abgefangen.



Datenbasis: 900 Payloads
Abb. 7: Malware-Payloads nach Familien

Häufigste IoT-Bedrohungen

Die überwältigende Mehrheit der 900 verschiedenen Payloads (97 Prozent) war zwei Malwarefamilien zuzurechnen: Gafgyt und Mirai. Daneben wurde auch Malware aus den Familien Tsunami, VPNFilter und Hajime beobachtet.

Obwohl die größte Anzahl unterschiedlicher Payloads auf Gafgyt entfiel, kamen Mirai-Payloads im Studienzeitraum häufiger bei Malwareangriffen zum Einsatz. Bei 76 Prozent aller blockierten Angriffe handelte es sich um Malware aus der Mirai-Familie, weitere 5 Prozent waren der Gafgyt-Familie zuzurechnen und 19 % anderen.

IoT-Botnets
Erfolgreiche Exploits von IoT-Geräten verschaffen Angreifern Zugriff sowohl auf das Gerät selbst als auch auf die Netzwerke, mit denen es verbunden ist, und können potenziell großen Schaden anrichten. Insbesondere Malware aus den Familien Mirai und Gafgyt sind dafür bekannt, dass sie Geräte zum Erstellen von Botnets missbrauchen. Dabei handelt es sich um Netzwerke, die sich in der Kontrolle des Angreifers befinden und weitreichende koordinierte Angriffe ermöglichen. Bisher wurden Botnets u. a. für DDoS-Angriffe (Distributed Denial of Service), Diebstahl von Finanzdaten, Kryptowährungs-Mining und gezielte unbefugte Zugriffe verwendet. Der bislang schwerste DDoS-Angriff, der 2016 weitreichende Internetausfälle verursachte, ging von einem Botnet der Mirai-Familie aus. ThreatLabz wertete im Rahmen dieser Malwarestudie versuchte Botnets-Callbacks aus und kam zu dem Ergebnis, dass Angreifer dabei nicht nur IoT-Geräte, sondern auch eine Reihe gängiger Router und anderer Netzwerkgeräte ins Visier nahmen:

Geräte, die am häufigsten für Botnet-Callbacks missbraucht wurden	
Videoüberwachungsanlagen (CCTV) und DVRs von über 70 Anbietern	MVPower DVRs
Verschiedene Geräte, die Realtek SDK mit miniigd daemon verwenden	Linksys-Geräte
Huawei HG532	Netgear-Geräte der Reihen R7000/R6400
ZyXEL-Router	Netgear-Router der Reihe DGN1000
GPON-Router von Dasan	D-Link-Geräte
Eir-D1000-Router	NVR-Geräte von Vacron
D-Link-Geräte	

Am häufigsten betroffene Branchen

Mit 40 Prozent der Infektionen durch IoT-Malware verzeichneten Technologieunternehmen die höchste Angriffsrate. Die Fertigungsbranche (28 Prozent) sowie Einzel- und Großhandel (24 Prozent) waren ebenfalls beliebte Angriffsziele.

Länder, von denen die meisten Malware-Angriffe ausgehen

In unserer Studie wurde festgestellt, dass 88,5 Prozent der kompromittierten IoT-Geräte Daten an Server in den Malwarezielländern China (56 Prozent), den USA (19 Prozent) oder Indien (14 Prozent) weiterleiteten. In allen beobachteten Fällen sollte die Malware entweder direkt ausgeliefert oder das System zunächst infiziert werden, um anschließend eine Verbindung zur betreffenden Malware aufzubauen. Dabei ist zu beachten, dass einige Angreifer Command-and-Control-Server innerhalb des Landes einrichten, in dem der Angriff stattfindet. Daher gibt der Serverstandort nicht unbedingt Aufschluss über den tatsächlichen Standort des Angreifers.

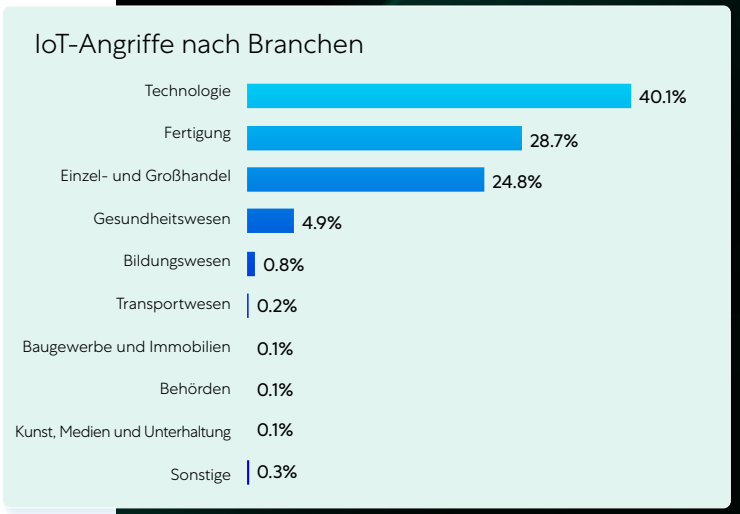


Abb. 8: IoT-Angriffe nach Branchen

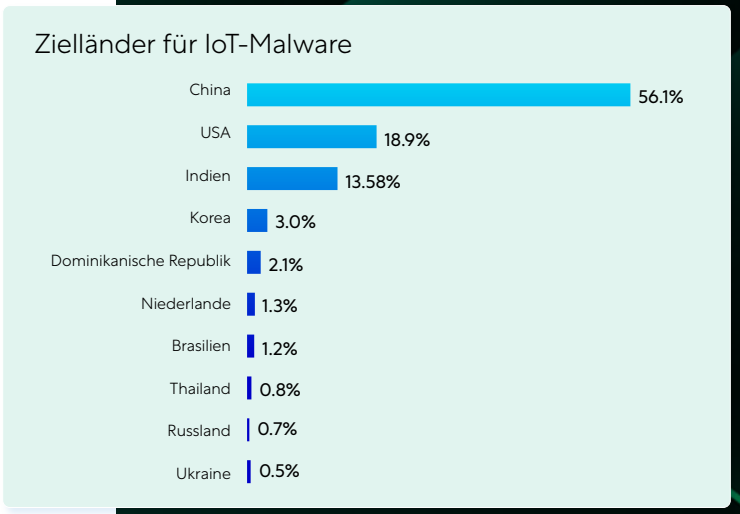


Abb. 9: Häufigste Zielländer (IoT-Malware-Angreifer)

Häufigste ASNs von Malwareangreifern

Nachfolgend werden die Malwareziele detaillierter aufgeschlüsselt. Die Tabelle enthält Angaben zu den wichtigsten autonomen Systemnummern (ASNs) und IP-Adressen, die im Beobachtungszeitraum Verbindungen zu IoT-Malware herstellten:

ASN	IP	AS-Name
16276	158.69.0.77	OVH, FR
398468	193.42.137.107	VMSNETWORKS, US
213035	193.239.147.144	SERVERION-AS Serverion B.V., NL
36352	107.173.125.167	AS-COLOCROSSING, US
202448	86.105.252.203	MVPS https://www.mvps.net, CY
46606	162.241.126.53	UNIFIEDLAYER-AS-1, US
53667	198.251.81.249	PONYNET, US
212953	46.102.106.25	MRS-BILISIM, TR
35913	45.15.143.175	DEDIPATH-LLC, US
213371	37.49.230.52	SQUITTER-NETWORKS, NL
35913	45.15.143.140	DEDIPATH-LLC, US
42864	45.95.169.218	GIGANET-HU GigaNet Internet Service Provider Co, HU
63916	103.42.214.181	IPTELECOM-AS-AP IPTELECOM Global, HK
134520	103.42.214.181	GIGSGIGSCLOUD-AS-AP GigsGigs Network Services, HK
3462	111.248.163.38	HINET Data Communication Business Group, TW
36352	107.173.181.189	AS-COLOCROSSING, US
36352	192.227.147.157	AS-COLOCROSSING, US
212369	45.155.125.116	TRDESERVER, TR
206898	185.172.110.205	BLADESERVERS, AU
213035	193.239.147.245	SERVERION-AS Serverion B.V., NL

Abb. 10: Häufigste ASNs von Malwareangreifern

Häufigste Opfer von IoT-Malwareangriffen

Die Herkunftsländer der Malwareopfer wurden anhand der jeweiligen Client-IP-Adresse von ThreatLabz ebenfalls erfasst. Hier führten Irland (48 Prozent), die USA (32 Prozent) und China (14 Prozent) die Rangliste der häufigsten Zielscheiben für IoT-Angriffe an.

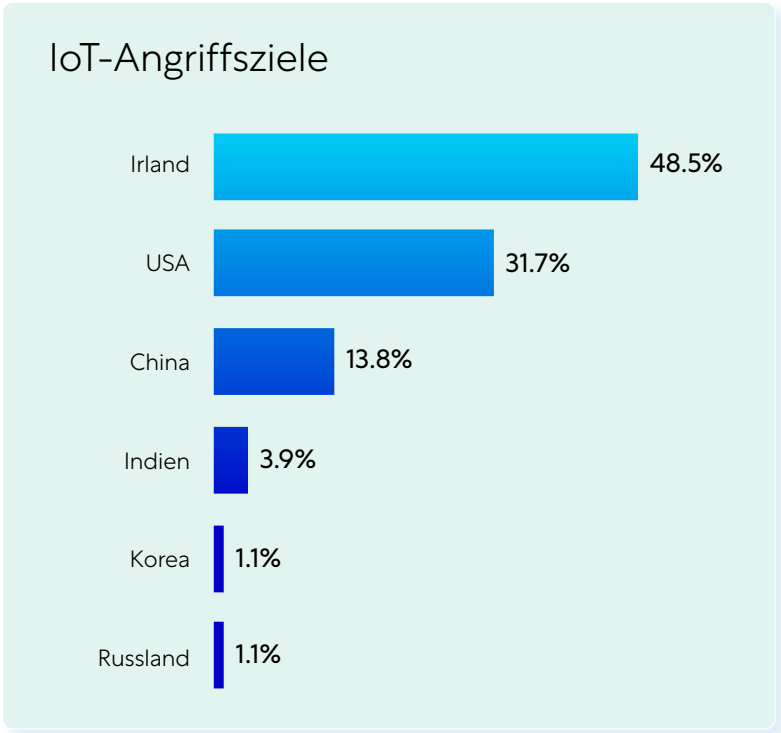


Abb. 12: Häufigste Herkunftsländer (IoT-Malwareopfer)

Grundlagen zum Schutz vor IoT-Malware

Angesichts der ständig zunehmenden Bandbreite „intelligenter“ Geräte wäre der Versuch, sie aus Unternehmensnetzwerken auszuschließen, quasi aussichtslos. Umso wichtiger ist es, durch entsprechende Zugriffsrichtlinien zu verhindern, dass IoT-Geräte als Einfallsvektor für den unbefugten Zugriff auf vertrauliche Daten und Anwendungen missbraucht werden.

Im Folgenden werden Best Practices zur Minderung des Malwarerisikos erläutert, das sowohl von zugelassenen als auch inoffiziell genutzten IoT-Geräten ausgeht:

- **Verfolgen und Verwalten von Netzwerkgeräten.** Da IoT-Geräte häufig nicht verwaltet werden, geben die von Endpunkt-Agents gelieferten Daten keinen zuverlässigen und transparenten Aufschluss darüber, welche Geräte in den Räumlichkeiten eines Unternehmens im Einsatz sind. Um jederzeit den Überblick über die aktuellen Aktivitäten sämtlicher Geräte im Unternehmensnetzwerk zu behalten, empfiehlt sich der Einsatz einer Lösung, die Netzwerkprotokolle untersucht. Zusätzlich sollten Architekturen implementiert werden, die eine Überprüfung des gesamten verschlüsselten und unverschlüsselten Traffics ermöglichen, damit auch Kommunikationen von unbekannten Geräten erkannt werden. Dann sind geeignete Sicherheitsvorkehrungen einzusetzen.

- **Ändern von voreingestellten Passwörtern.** Diese Leier ist schon so alt wie die Geschichte der IT: Wenn voreingestellte Standardpasswörter nicht geändert werden, haben Angreifer leichtes Spiel. Die Passwörter für inoffiziell benutzte IoT-Geräte entziehen sich zumeist der Kontrolle des Unternehmens – bei der Bereitstellung unternehmenseigener IoT-Geräte sollte das Einrichten neuer Passwörter jedoch zur selbstverständlichen Gewohnheit werden. Auch Mitarbeiter, die eigene Geräte für ihre Arbeit verwenden, müssen entsprechend geschult werden.

- **Schließen von Sicherheitslücken durch Patches und Updates.** In vielen Branchen – insbesondere Fertigung und Gesundheitswesen – werden IoT-Geräte zur Abwicklung alltäglicher Arbeitsabläufe eingesetzt. Bei diesen offiziell zugelassenen Geräten ist unbedingt darauf zu achten, dass neu entdeckte Sicherheitslücken umgehend durch entsprechende Patches geschlossen werden.

- **Implementieren einer Zero-Trust-Sicherheitsarchitektur.** Für unternehmenseigene Assets sind strenge Richtlinien durchzusetzen, damit Benutzer und Geräte nur im unbedingt erforderlichen Umfang und nach erfolgter Authentifizierung auf Ressourcen zugreifen können. Die Kommunikation ist auf die jeweils relevanten IP-Adressen, ASNs und Ports zu beschränken, die für den externen Zugriff benötigt werden. Ist eine Internetverbindung für IoT-Geräte erforderlich, die nicht offiziell zugelassen sind, muss der gesamte Traffic überprüft sowie der Zugriff auf Unternehmensdaten blockiert werden, am besten durch einen Proxy. Die Bedrohung durch ungesicherte IoT-„Schattengeräte“ lässt sich nur durch vollständigen Verzicht auf Richtlinien abwehren, die auf einem impliziten Vertrauensverhältnis basieren. Stattdessen muss der Zugriff auf vertrauliche Daten durch dynamische identitätsbasierte Authentifizierung nach dem Zero-Trust-Prinzip kontrolliert werden.

Über ThreatLabz

ThreatLabz ist als Forschungsabteilung von Zscaler für die Früherkennung neuer Bedrohungen zuständig. Dadurch lässt sich sicherstellen, dass die Tausenden Unternehmen, die weltweit mit der Plattform Zscaler Zero Trust Exchange™ arbeiten, jederzeit geschützt sind. Neben der Erforschung und Verhaltensanalyse von Malware-Bedrohungen tragen die ThreatLabz-Experten auch zur Entwicklung neuer Prototypen für einen erweiterten Bedrohungsschutz auf der Zscaler-Plattform bei und führen regelmäßig interne Sicherheitsüberwachungen durch, um sicherzustellen, dass Zscaler-Produkte und -Infrastrukturen die geltenden Sicherheitsstandards erfüllen. Detaillierte Analysen neuer und sich ausbreitender Bedrohungen werden regelmäßig unter research.zscaler.com veröffentlicht.

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Benutzern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlust. Die SASE-basierte Zero Trust Exchange ist auf über 150 Rechenzentren weltweit verteilt und die weltweit größte Inline-Cloud-Sicherheitsplattform. Informieren Sie sich auf **zscaler.com** oder folgen Sie uns auf Twitter **@zscaler**.