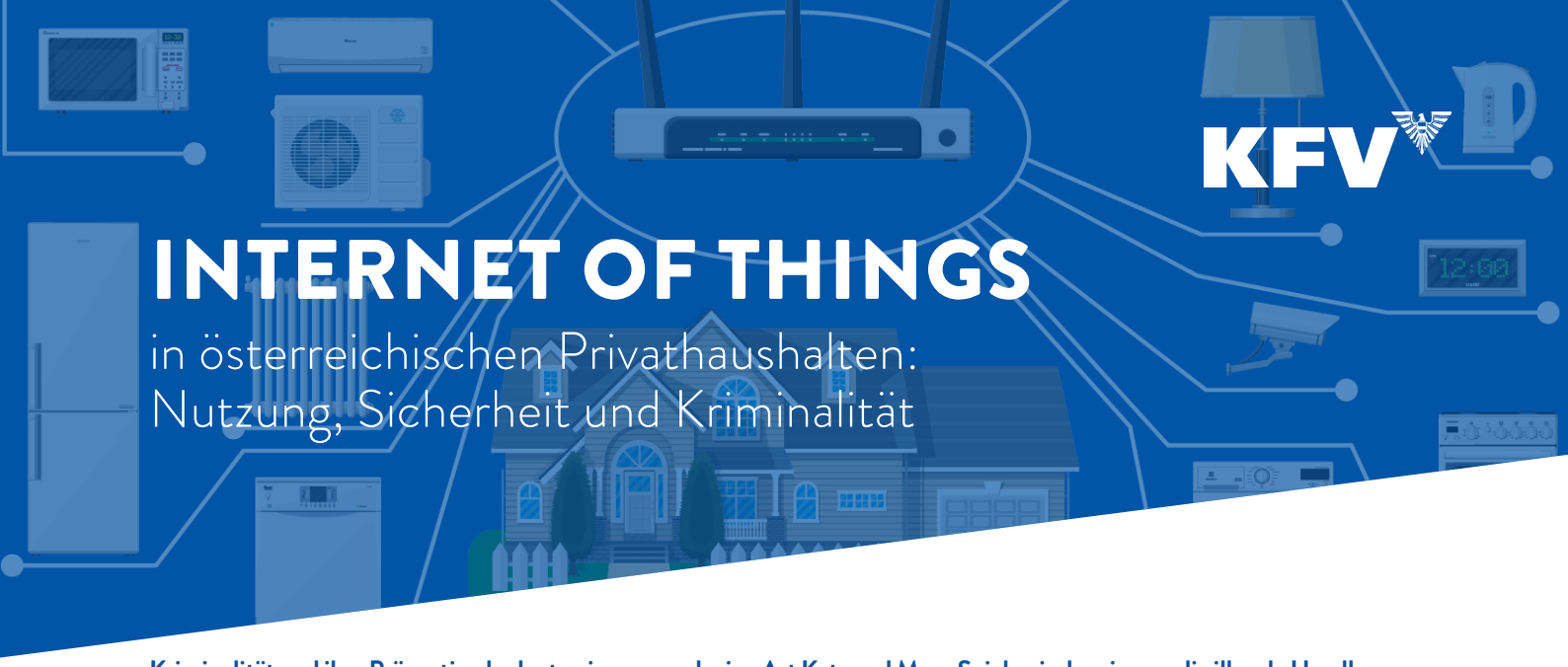


INTERNET OF THINGS

in österreichischen Privathaushalten: Nutzung, Sicherheit und Kriminalität

Kriminalität und ihre Prävention bedeuten immer auch eine Art Katz und Maus Spiel zwischen jenen, die illegale Handlungen setzen wollen und den staatlichen Strafverfolgungsbehörden. Speziell technologische Entwicklungen führen hier oftmals zu Situationen, in welchen die Prävention der Kriminalität einen Schritt voraus sein könnte oder müsste, de facto jedoch hinterherhinkt. Denn oft ist eine Sicherheitslücke oder eine Produktschwäche so lange unbekannt, bis sie ausgenutzt wird. Jede technologische Entwicklung, die in der breiten Öffentlichkeit Anwendung findet, ist von diesem Risiko betroffen.

INTERNET OF THINGS

Seit einigen Jahren ist nun die nächste Entwicklungsstufe der Digitalisierung in der Bevölkerung angekommen: Das „Internet of Things“ (Internet der Dinge, kurz IoT) tritt auch in Österreich seinen Siegeszug an. Die Vorteile dieser smarten Geräte und ihre Vernetzung untereinander und mit dem der einzelnen User*in sind mannigfaltig. Das Haus wird automatisch gereinigt, die Fensterläden werden selbständig bei Sonneneinstrahlung geschlossen, der Kühlschrank bestellt in Eigenregie Milch und Joghurt. Doch auch die Sicherheit zu Hause kann erhöht werden, durch smarte Schließsysteme oder Überwachungskameras. Sensoren sammeln, kommunizieren, analysieren und handeln basierend auf Informationen, ohne dass der Mensch selbst aktiv werden muss.

DIE RISIKEN (VON IOT)

Für IoT ist das Hauptrisiko schlicht die rasant und unaufhaltsam steigende Anzahl an mit dem Internet verbundenen Geräten. Jedes Gerät ist ein potentielles Sicherheitsrisiko, und je kleiner und „unwichtiger“ das Gerät, umso wahrscheinlicher ist es, dass dieses nicht ausreichend vor Fremdzugriff geschützt wurde.

Sind die Zugangsdaten erst einmal geknackt, können im schlimmsten Fall Geräte ferngesteuert und manipuliert werden. So kann dann der/die Einbrecher*in die Haustür per Mausklick öffnen, während sein/e Komplize/in über die Sicherheitskameras im Haus darauf achtet, dass niemand den Täter bei der Arbeit stört.

EINFALLSTOR ZU SENSIBLEN DATEN

Doch diese Vernetzung ist auch das größte Risiko der neuen Technologie. Ein*e Cyberkriminelle*r muss sich nicht abmühen, um in ein Haus einzudringen. Stattdessen wird in das mangelhaft gesicherte Schließsystem eingedrungen und die Tür springt von selbst auf. Die Daten des Saugroboters können Rückschlüsse darauf geben, wann niemand zu Hause ist - eine nützliche Information für Einbrecher*innen! Ein schlecht gesicherter smarter Kühlschrank kann wiederum das Einfallstor in den eigentlich gut gesicherten Stand-PC mit sämtlichen sensiblen persönlichen Daten darstellen.

METHODIK

Das KFV will mit der hier vorliegenden Studie einen Beitrag zur Prävention von Cyberkriminalität über IoT-Geräte schaffen. Ausgehend vom Status Quo der Nutzung von IoT in österreichischen Privathaushalten wurde über eine repräsentative Bevölkerungsbefragung wird die Sicherheit der österreichischen Nutzer*innen kritisch analysiert. Anschließend wird aufgezeigt, worauf zu achten ist, um diese Innovationen möglichst sicher nutzen zu können. Darüber hinaus wird auch dargelegt, wie die Rechtsprechung die User*innen von IoT-Geräten besser schützen kann.

Stichprobe: 1.000 Östereicher*innen ab 18 Jahren

Studienzeitraum: Mai – Juni 2021

IoT (Internet of Things) in Österreich

Die bei weitem gängigsten IoT-Geräte kann man dem Bereich smartes IT-Equipment zuordnen (92 % der Nutzer*innen), zB Smart TV oder digitale Assistenten.

Die Befragten sehen bei IoT für fast alle (Lebens-)Bereiche einen entweder „sehr großen" oder „großen" Nutzen. Den größten sehen sie bei Kindersicherheit sowie bei Einbruchsschutz.

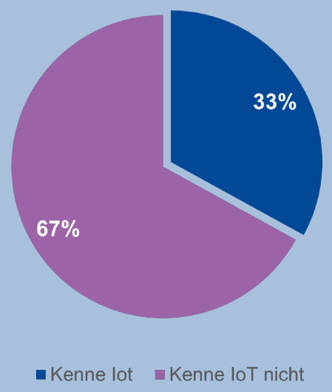
35 % der Befragten geben jeweils an, ihre Daten mit Unternehmen aus Sicherheitsgründen oder zum Zweck der wissenschaftlichen Forschung teilen zu wollen. Die Bereitschaft zum Teilen von Daten mit Unternehmen oder dem Staat ist dagegen weit geringer.

Fast zwei Drittel der österreichischen IoT-Nutzer*innen geben an, auf allen Geräten sichere Passwörter zu verwenden. Weniger gut ist die Update-Disziplin der Nutzer*innen. Nicht einmal die Hälfte der befragten Österreicher*innen führt diese regelmäßig durch.

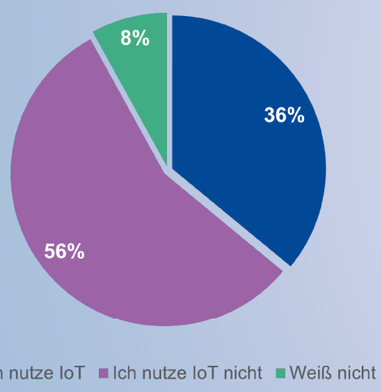
Jede*r fünfte Verkäufer*in hat beim Verkaufsgespräch keine Sicherheitsmaßnahmen genannt. Jeweils etwa die Hälfte der Befragten wünscht sich mehr Unterstützung durch den Staat oder Hersteller*innen/ Verkäufer*innen.

17 % der Nutzer*innen von IoT-Geräten gaben an, bereits einen illegalen Zugriffsversuch erlebt zu haben. 55 % der Betroffenen erlitten keinen Schaden. Bei immerhin einem Viertel der Betroffenen kam es zu finanziellem Schaden (n=14), und fünf Prozent hatten gestohlene Daten zu beklagen.

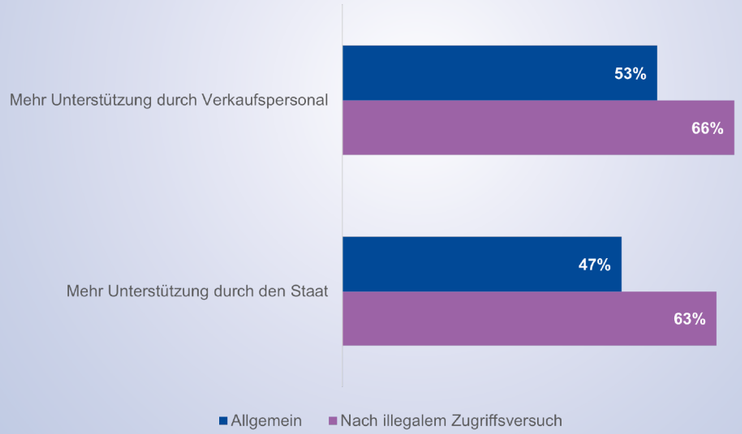
Bekanntheit des IoT in Österreich



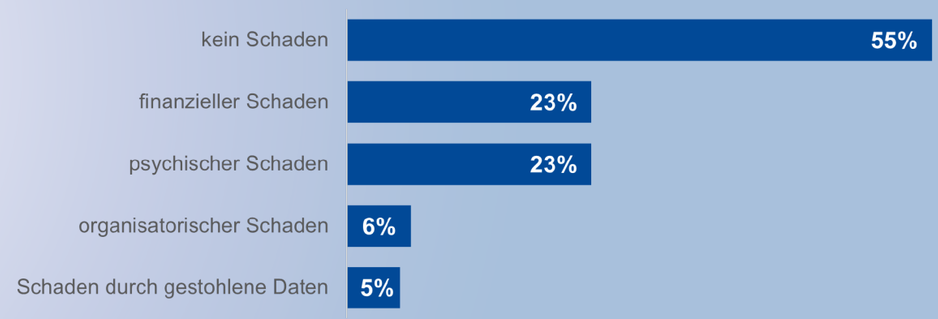
Nutzung des IoT in Österreich



Wunsch nach mehr Unterstützung im Zusammenhang mit Cybersicherheit



Durch illegalen Zugriff erlittener Schaden



Tipps für Anwender*innen

Installation und Einrichtung durch Profis!
Fragen Sie aktiv nach Sicherheitsmaßnahmen und lassen sie sich beraten.

Passwörter ändern!
Ändern Sie, wenn möglich, das Standardpasswort des Gerätes. Dieses wird oft für alle Geräte des gleichen Typs ausgegeben und ist daher leicht zu knacken.

Eigenes Netzwerk für IoT-Geräte!
So verhindern Sie den Zugriff über ein möglicherweise schlecht geschütztes IoT-Gerät auf Ihr privates Netzwerk. In diesem sind möglicherweise sensible private Daten oder Zahlungsinformationen hinterlegt.

Updates durchführen!
Regelmäßige Updates der Gerätesoftware schützen vor Fremdzugriff. Daher: Finger weg von Geräten ohne die Möglichkeit von Updates!

Auf Qualität statt Preis achten!
Sicherheit kostet. Eine einmalige Investition kann dazu beitragen, einen späteren viel größeren Verlust zu verhindern.

Alle illegalen Zugriffe - auch Versuche - zur Anzeige bringen!
Nur so kann die Polizei Tatmuster erkennen und frühzeitig warnen. Im realen Leben würden Sie einen Diebstahlversuch auch anzeigen!

Quelle: KFV (Kuratorium für Verkehrssicherheit)

PRÄVENTIONSTIPPS

IoT beginnt in Österreich langsam den Mainstream zu erobern. Doch nach wie vor sind die meisten Nutzer*innen von IoT-Geräten im an sich schon „technikaffinen“ Bevölkerungsteil zu verorten. Daher ist es auch nicht verwunderlich, dass grundsätzlich ein gewisses Maß an Sicherheitsbewusstsein und -maßnahmen in österreichs IoT-Haushalten herrscht. Doch diese Maßnahmen sind noch stark ausbaubar. Denn mit dem nicht aufzuhaltenden Siegeszug von „smarten“ Geräten und dem Internet of Things wird die heimische Technik zum Angriffsvektor für Kriminelle. Um dieser Gefahr nicht schutzlos ausgeliefert zu sein, ist es notwendig, das Schutzniveau nachhaltig zu steigern.

Hier sind für das KFV drei Maßnahmen zentral, um die Österreicher*innen fit für die Zukunft im „Internet der Dinge“ zu machen und sie bestmöglich zu schützen:

1. **Schulung des Verkaufspersonals:** Nicht nur die Nutzer*innen selbst sollten dazu angehalten werden, ihre IoT-Geräte entsprechend vor Fremdzugriffen zu sichern. Die Prävention beginnt bereits im Vorfeld, beim Verkauf und der Beratung. Hier wird in der Befragung auch offensichtlich, dass noch Luft nach oben ist. Verkaufspersonal und Installierende müssen den Endnutzer*innen mehr Informationen geben, wie sie sich selbst schützen können, wo die Gefahren liegen, und was im Falle eines Sicherheitsvorfalls zu tun ist.

2. **Konsument*innenschutz ausbauen:** Auch der Konsument*innenschutz kommt zu ähnlichen Forderungen. So werden unter anderem Basisinformationsblätter für Konsument*innen gefordert, aus denen hervorgehen soll, welche Daten übermittelt und wozu diese verwendet werden.

3. **Zertifizierung für IoT-Geräte entwickeln:** Weiters wird es notwendig werden, Sicherheitsnormen für IoT-Geräte zu definieren, um die österreichischen Nutzer*innen bestmöglich zu schützen. Hier ist es mit Sicherheit am sinnvollsten, entweder auf europäischer oder auf nationaler Ebene Zertifizierungen basierend auf dem ETSI-Standard 303 645 zu entwickeln, um verschiedene Sicherheitsstufen zu definieren. Jedenfalls wäre es sinnvoll, einen Mindeststandard zu entwickeln, dessen Sicherheitsvorkehrungen verpflichtend für neue IoT-Geräte sein müssen.

Quelle: KFV-Studie zum Thema „Internet of Things in Österreich“
Bildrechte: Vectorstock / Pixabay

Medieninhaber und Herausgeber:
KFV (Kuratorium für Verkehrssicherheit)
Schleiergasse 18, A-1100 Wien
Tel: +43-(0)5 77 0 77-0
Fax: +43-(0)5 77 0 77-1186
E-Mail: kfv@kfv.at