

## Safety first!

### Angriffe auf Mobilgeräte nehmen zu – Schutz der Privatsphäre ist wichtig

Der jährliche Threat Landscape-Report des Jahres 2020 zeigt, dass im kommenden Jahr mit ausgefeilteren Methoden zur Verbreitung von Schadsoftware auf PCs zu rechnen ist. Dazu gehört beispielsweise der Diebstahl von eingehenden E-Mails mit dem Zweck, die Betroffenen auszuspionieren oder vor dem Zustellen Schadsoftware hinzuzufügen. Darüber hinaus prognostiziert die Studie ein Wiederaufleben von Exploit Kits (kleine Programme, die Sicherheitslücken auf dem Computer auffindig machen und ausnutzen. Außerdem werden Cyberkriminelle Schwachstellen ausnutzen, um Bedrohungen zu verbreiten.

### Betrug übers Smartphone nimmt zu

Laut des Reports wird für mobile Endgeräte ein erhöhtes Aufkommen von Abo-Fallen und gefälschten Apps in offiziellen App Stores vorausgesagt. Sowohl Sicherheitsforscher als auch Cyberkriminelle werden mehr iOS-Schwachstellen aufdecken. „Bösartige Anwendungen im Google Play Store und Apple Store bereitzustellen, ist nicht einfach. Deshalb stürzen sich Cyberkriminelle auf Abo-Fallen und gefälschte Anwendungen, in die aggressiver Adware, also Onlinewerbung, integriert sind, um Geld zu verdienen“, erklärt Martin Galler, Data Security & Privacy Experte von KONVERTO.

### Gefahrenquelle IoT-Geräte (Internet of Things – Internet der Dinge)

Geräte und physische Standorte werden immer intelligenter. Unternehmen können damit noch mehr Daten über Benutzer sammeln, um ihr Verhalten auszuforschen und vorherzusagen. „Intelligente Geräte und Standorte, die Daten erfassen, bieten Komfort, beschränken allerdings gleichzeitig die Kontrolle der Menschen über ihre Privatsphäre. Unternehmen, die eine Vielzahl von Kundendaten sammeln und speichern, sind attraktive Ziele für Cyberkriminelle, die diese Daten auf dem Schwarzmarkt verkaufen“, erläutert Martin Galler.

### Online geht nichts ohne Schutz

Die Gefahr, Opfer von Online-Dieben und Virenangriffen zu werden, steigt. Deshalb ist ein Rundumschutz von Computer und Smartphone unumgänglich. Mit der Antivirus-Software KONVERTO Secure sind Windows-PC, MAC, Android- und iOS-Geräte vor digitalen Gefahren geschützt: die Sicherheitssoftware schützt beim Einkaufen im Internet und macht Geldgeschäfte per Online-Banking sicher, die persönlichen Daten werden in sozialen Netzwerken geschützt, um einen Identitätsdiebstahl zu verhindern, geht das Smartphone verloren, kann es geortet werden, gesperrt oder die persönlichen Daten aus der Ferne gelöscht werden, und ein individuell einstellbarer Kinderschutz mit Zeitlimit und Inhaltsblocker schützt zudem Minderjährige vor pornografischen oder Gewalt verherrlichenden Web-Inhalten.

**KONVERTO AG** | S.p.A. via Bruno-Buozzi-Str. 8, 39100 Bozen | Bolzano  
**Info Center 800 031 031** T0471 064 500 info@konverto.eu info@pec.konverto.eu konverto.eu

Handelsregister-Nr. | Registro delle imprese Bozen | Bolzano: 02254110212 REA: 165926  
 MwSt.-Nr. | Part. IVA/Steuernummer | Cod. Fisc.: 02254110212 Gesellschaftskapital | Cap. Soc.: 1.754.000 € v.e. | i.v.



## Kinder und Jugendliche sensibilisieren und schützen

Der jährliche internationale Tag für mehr Sicherheit im Netz – Safer Internet Day (SID) – der weltweit in 140 Ländern am Dienstag, 11. Februar, begangen wurde, spricht sich besonders für den Schutz von Kindern und Jugendlichen im Netz aus. Die Generation Z ist besonders stark von den seelischen und körperlichen Folgen übermäßigen Internet-Konsums betroffen. Weltweit gibt es rund 2,3 Milliarden aktive Facebook-Nutzer, rund eine Milliarde Menschen benutzt Instagram, über Twitter werden täglich 100 Millionen Kurznachrichten versendet. Schülern sind den ganzen Tag über – auch in der Unterrichtszeit - auf Chat-Kanälen online und chatten auch nachts. Jeder sechste Jugendliche gibt außerdem an, dass er Intimfotos verschickt oder in den digitalen Medien teilt. Drei von hundert Schülern erklären, dass ihre Intimfotos ohne ihr Mitwissen an Dritte weitergegeben wurden.

Als problematisch werten Experten unter anderem Internet-Inhalte, die Essstörungen verherrlichen oder verharmlosen. Magersucht und Ess-Brech-Sucht werden darin als Life-Style präsentiert. Die Produzenten und Anhänger solcher Internetinhalte, die körperliche Perfektion predigen, sind in der Regel junge Frauen. Weil sie sich hauptsächlich über soziale Medien informieren, sind Jugendliche auch für absichtlich gestreute Falschmeldungen (fake news) besonders empfänglich. Laut einer deutschen Studie besucht nur eine Minderheit der Jugendlichen von Journalisten gestaltete Nachrichtenportale.

Das EU-weite SID-Netzwerk stellt auf seinen Internet-Plattformen umfangreiches Aufklärungsmaterial für Schulen, Kinder und Eltern zur Verfügung. Auch KONVERTO setzt ein Zeichen: neben hochwertigen professionellen Sicherheitslösungen für Unternehmen und Privatpersonen sind auf [konverto.eu](http://konverto.eu) auch Informationen zum Umgang mit Internetgefahren und Tipps, um Gefahren vorzubeugen, zu finden.

## **Safety first!**

### **Gli attacchi ai dispositivi mobili sono in aumento - la protezione della privacy è importante!**

Il Threat Landscape Report annuale del 2020 mostra che nel 2020 si possono prevedere metodi più sofisticati per la diffusione di malware sui PC. Tra questi rientrano, ad esempio, il furto di e-mail in entrata con lo scopo di spiare le persone colpite o l'aggiunta di malware prima della consegna. Inoltre, lo studio prevede una recrudescenza dei kit di exploit (piccoli programmi che rilevano e sfruttano le falle di sicurezza del computer. I criminali informatici sfrutteranno anche le vulnerabilità per diffondere le minacce.

#### **Le frodi con gli smartphone sono in aumento**

Secondo il rapporto, per i dispositivi mobili è previsto un aumento del numero di trappole per gli abbonamenti e di app false negli app store ufficiali. Sia i ricercatori della sicurezza che i cybercriminali scopriranno altre vulnerabilità di iOS. Distribuire applicazioni dannose nel Google Play Store e nell'Apple Store non è facile. Ecco perché i cybercriminali cadono nelle trappole degli abbonamenti e nelle applicazioni fasulle che integrano adware aggressivi, cioè la pubblicità online, per guadagnare soldi.

#### **Fonte di pericolo Dispositivi IoT (Internet delle cose)**

I dispositivi e i luoghi fisici stanno diventando sempre più intelligenti. Le organizzazioni possono utilizzarli per raccogliere ancora più dati sugli utenti per esplorare e prevedere il loro comportamento. I dispositivi intelligenti e i luoghi che raccolgono i dati forniscono comodità, ma allo stesso tempo limitano il controllo delle persone sulla loro privacy. Le aziende che raccolgono e memorizzano una grande quantità di dati dei clienti sono obiettivi interessanti per i criminali informatici che vendono questi dati sul mercato nero.

#### **Niente va online senza protezione**

Il rischio di diventare vittima di ladri online e di attacchi di virus è in aumento. Ecco perché la protezione a 360° di computer e smartphone è essenziale. Con il software antivirus KON Secure, i dispositivi PC Windows, MAC, Android e iOS sono protetti contro i pericoli digitali: il software di sicurezza protegge quando si fanno acquisti in internet e rende sicure le transazioni finanziarie tramite l'online banking, i dati personali sono protetti nei social network per evitare il furto di identità, se lo smartphone viene smarrito, può essere localizzato, bloccato o i dati personali possono essere cancellati a distanza, e un controllo parentale personalizzabile con limite di tempo e blocco dei contenuti protegge anche i minori da contenuti pornografici o violenti che esaltano i contenuti web.