Exposé zur Datensicherheit im Internet

Im Zuge unseres Engagements für den Datenschutz und die -sicherheit im Internet ist es unser Anliegen, dir als User zusätzliche Informationen für deine persönliche Datensicherheit im Internet zu liefern. Hierfür nachfolgend einige Top-Gründe für Sicherheitslücken:

1. Ergänzte Betriebssysteme: Ein schwaches Glied in der Kette der sogenannten Datensicherheit sind **Betriebssysteme, welche «ergänzt» werden.** Beispielsweise verwenden einige der marktführenden Hersteller von Endgeräten als Grundlage ein Android-Betriebssystem, welchem sie jedoch eigene Apps, zusätzliche Subsysteme und teilweise versteckte Systemergänzungen für die Gerätesteuerung mitliefern. Derartige Konstrukte sind von Grund auf unsicher, da Aktualisierungen, welche beispielsweise Sicherheitslücken im Android-System schliessen, nur mit grösserer Zeitverzögerung verfügbar sind. Dies aufgrund des «Überbaus» derartiger Konstrukte, welcher vor dem Ausspielen der notwendigen Updates zuerst durch den Hersteller ergänzt werden müssen. Während die User auf Updates warten, können die kritischen Lücken, die mit den Android-Aktualisierungen publik gemacht werden, problemlos ausgenutzt werden. Je nach Hersteller sind die Wartezeiten für entsprechende Updates kürzer bzw. länger und die User sind in dieser Zeit mehr als gefährdet. Zu diesen Sicherheitslücken gibt es diverse Onlineinformationen (Google warnt vor kritischer Lücke, Datenschutz-Einstellungen auf Android, Ratgeber Smartphone, etc.).

2. Öffentliche WLAN-Hotspots: Ein weiteres schwaches Glied sind **öffentliche, teilweise ungenügend gesicherte WLAN-Hotspots,** die häufig bedenkenlos genutzt werden und über die technisch versierte Personen auf fremden Geräten ohne allzu grossen Aufwand mitlesen können.

3. Das Userverhalten: Das schwächste Glied innerhalb der Datensicherheit im Internet ist jedoch in der Regel der User selbst.

a. Eigensicherung des Endgeräts: Es ist davon auszugehen, dass die allermeisten Smartphone-User auf ihren Geräten noch immer keine Sicherheitssoftware wie Anti-Virus und Firewall verwenden und aufgrund der langsameren Geschwindigkeit auch keine VPN-Verbindungen nutzen.

b. Das Nutzerverhalten: Unbedachtes und rasches Tippen auf alles, was «interessant» aussieht, auf dubiose Links in E-Mails oder das Surfen auf Websites mit zweifelhaftem Inhalt, führen häufig zu Trojanern, welche sich auf den Geräten einnisten, zur Ausführung von ungewollten Scripts «im Hintergrund» (ohne Wissen der User) bis hin zu einer vollständigen Kompromittierung der Geräte. Häufig werden weder Verläufe noch temporäre Dateien, weder Cookies noch sonst was gelöscht, aus reiner Bequemlichkeit. Und geschätzte 80% aller Smartphone-User beachten die Privatsphären-Einstellungen der verwendeten Apps nicht und limitieren die Rechte der Apps nicht.

Es sind sehr selten Server bzw. Datenbanken, die schlecht gesichert oder dermassen exponiert sind, dass die Ursache für mangelnde Datensicherheit dort zu finden ist.

Bei einem shared Host, wie ihn Syna verwendet, werden vom Hoster selbst über die zur Verfügung gestellte Infrastruktur bereits ausserordentlich hohe Sicherheitsstandards vorgegeben. Ein «unbedarfter» Website-Betreiber beispielsweise hat gar keine Möglichkeit, das *mod security* von Apache nicht zu verwenden/zu deaktivieren, da dies nicht separat übers Server Control Panel gesteuert werden kann. Dadurch werden die häufigsten Attacken auf den Host bereits «von Haus aus» blockiert.

Fazit: In den allermeisten Fällen, in denen die Datensicherheit «nicht gewährleistet» ist, ist dies auf veraltete/fehlerhafte oder «bösartige» Software und/oder aufs Nutzerverhalten zurückzuführen.