

IT-SECURITY

Kabellose Keyboards sind Zeitbomben

Jede Woche beantworten Sicherheits-
experten Leserfragen und geben
Ratschläge, wie sich die Sicherheit in
einem Unternehmen erhöhen lässt.

Frage: Als Informatiksicherheits-
beauftragte stehe ich vor der Frage,
ob ich zukünftig im Geschäft Wire-
less-Keyboards auch für ge-
schäftskritische Bereiche zulassen
soll oder nicht.

Zu diesem Thema sind kaum
offizielle oder öffentliche Stu-
dien und Tests zugänglich,
obwohl Militär, Geheimdiens-
te und das BSI in Deutschland
über entsprechende Informa-
tionen verfügen, weil im Spi-
onagebereich die ursprüng-
lich militärischen und politi-
schen von den wirtschaftlichen
Interessen überholt wurden.
Eine zuverlässige Risikoein-
schätzung ist somit schwierig
– dennoch existieren gewisse
Anhaltspunkte. So werden
militärische, wirtschaftlich
erfolgreiche und finanzkräftige
Organisationen häufiger
zum Ziel von Spionageangrif-
fen als andere Organisa-
tionen. Als Faustregel gilt: Je
sensitiver der Geschäftsbe-
reich, desto höher ist die Ge-
fährdung.

Im Bereich von Cordless-
oder Wireless-Tastaturen exis-
tieren drei verbreitete Techno-
logien: Funk-basierende (nied-
riger MHz-Bereich), Wireless
(2,4 oder 5 GHz) oder Blue-
tooth (2,400 bis 2,4835 GHz).

Diese haben je nach Technologie
und Rahmenbedingungen un-
terschiedliche Reichweiten von
einigen bis zu einigen 100 Me-
tern. Bei allen Technologien sind
Angriffe (zumindest theoretisch)
bekannt, der zu betreiben-
de Aufwand jedoch unterschied-
lich hoch. Das passive Abhören
von Signalen ist mit selbst gebas-
telten Antennen über eine Dis-

**«Je sensitiver der
Geschäftsbereich, desto
höher die Gefährdung.»**

tanz von über einem Kilometer
einfach zu bewerkstelligen und
vom «Opfer» nur schwer zu ent-
decken. Ohne wirkungsvolle
Verschlüsselung des Inhaltes ist
die Vertraulichkeit der Daten-
kommunikation dahin. Aktive
Angriffe wie Manipulationen
der Datenübertragung oder das
Überlagern und Stören von Sig-
nalen sind mit wesentlich mehr
Aufwand verbunden und kön-
nen entdeckt werden.

Funk-basierte Angriffe sind
für elektronisch Begabte recht
einfach zu bewerkstelligen, zu-
mal die benötigte Ausrüstung
für wenig Geld in jedem Elek-
tronikshop zu haben ist. Die
Wireless-Technologie ist einige

Jahre bekannt und deshalb sind
bereits ausgereifte Hackertools
und How-to-Anleitungen vor-
handen. Im Bluetooth-Bereich
beschränken sich die Angriffs-
möglichkeiten noch hauptsäch-
lich auf Notebooks, PDAs und
Handys – hinsichtlich Angriffen
auf Tastaturen ist derzeit kaum
Wissen oder gar entsprechende
Software öffentlich verfügbar.

Dies soll aber nicht als
Unbedenklichkeitser-
klärung interpretiert
werden. Ein Beispiel in
diesem Zusammen-
hang ist Tempest
(Transient Electromag-
netic Pulse Emanation Stan-
dard; <http://www.eskimo.com/~joelm/tempest.html>)
und van-Eck-Phreaking (<http://de.wikipedia.org/wiki/Van-Eck-Phreaking>).
1996 wurde die
Technik in Hackerkreisen erst-
mals demonstriert, davor galt
dies als Science-Fiction. Heute
kann fast jeder solche Geräte
bauen und Software im Internet
herunterladen (<http://ebox.sourceforge.net/>).

Schützen lassen sich die ka-
bellosen Kommunikationstechno-
logien einerseits mittels phy-
sischen Massnahmen wie dicken
Wänden mit hohem Armie-
rungseisenanteil, Spezialfens-
tern mit erhöhtem Bleianteil

oder Folien. Andererseits kann
mittels Beschränkung der Sen-
deleistung, Verhinderung von
Abstrahlung der Signale oder
Datenverschlüsselung (einfach-
es Bluetooth-Pairing gilt nicht
als Verschlüsselung) zusätz-
lich Risikoverminderung
betrieben werden. Bei der Wahl
von Verschlüsselungsalgorith-
men und Schlüssellängen gel-
ten die gleichen Sicherheitsan-
forderungen wie für die Kom-
munikation im Internet.

Weil die Technologien noch
nicht ausgiebig untersucht
werden konnten und keine
vertrauenswürdigen Studien
vorliegen, wird vom Gebrauch
von kabellosen Tastaturen in
geschäftskritischen Bereichen
eher abgeraten. Für Privatper-
sonen ist das Risiko einer sol-
chen Gefährdung aber eher als
gering einzuschätzen. ■



Der Autor
Martin Rutishauser
ist Consultant und
OPST/OPSA bei
der Sicherheitsbe-
raterin Oneconsult,
Thalwil. www.oneconsult.com

**Unsere Experten beantworten
Ihre Fragen.** Schreiben Sie uns:
it-security@computerworld.ch

**Ein Archiv der Helpdeskartikel
finden Sie im Internet:**
www.computerworld.ch

ILLUSTRATION: GW/THU

