How to protect yourself from a new breed of hacker

By Josh Klein

This is an excerpt of a speech given by professional hacker Josh Klein recently spoke on how increasingly sophisticated consumer hacking tools are making it easier than ever for anyone to pose a security risk and what hotels can do to protect themselves.

"It's an interesting time to be a hacker, because we've got more targets and better technology than ever before, not that that's very good for everybody else," Klein said. "It's not necessarily the most high-tech attacks [that are dangerous], it's often the very simple things and the human element that's most readily attacked."

As an example, Klein showed the audience a picture of the humble memory stick. To attack a company, a hacker might load five or six of these with Trojan programs and seed them in the company parking lot. Natural human curiosity means that it's likely at least one of the company's employees will find the memory stick and put it in their company computer to see what's on it, giving the Trojan program an opportunity to take over the computer and grant the hacker access to the company's network. Not only is this approach cheap—memory sticks don't cost that much money—it also requires far less time, effort and risk on the hacker's part than would attempting to hack the company's firewall remotely.

The untrustworthy memory stick is just one example of the consumer-level tools hackers can use to carry out dangerous attacks. Hardware such as "Pony Express" and software like Metasploit, Firesheep and the website Spokeo make it increasingly easy for hackers with no special technical knowledge to take over machines, steal data from company networks or discover sensitive personal information they can use to con a target into trusting them.

At the same time as these tools are becoming more available, increases in hotel automation are also providing more holes for hackers to exploit. Devices such as Voice over IP phones, TVs, wireless ID and door cards and even air-conditioning systems come with built-in computers or Internet connections that hackers can use to worm their way into a hotel's more sensitive networks. Guests bring security risks of their own.

Customers using cloud services on a hotel's network can open themselves, and in turn the guest network, to attack, and if the guest network has any way of connecting with that hotel's more sensitive networks, those areas could be at risk as well.

What can hotels do to protect themselves? Klein offered the following tips:

- Lock down your hardware: If a device has an ethernet port, it has default passwords that are just a Google search away.
- Encrypt your networks: If you have a wireless network for guests, be sure to separate it from the networks you use for business. It may also make sense to separate networks you use for more or less sensitive business functions depending on your hotel's exact needs.
- Secure your services: Services like your hotel's website, front desk kiosk and business center could all be vulnerable to attack if they are not properly locked down.
- Educate your staff: "One of the most vulnerable parts of your industry is your staff," said Klein, "because they're trained to accommodate." Unfortunately hackers can take advantage of trusting staff to gain access to guestrooms or guest data, so it is important to strike a balance between guest service and keeping your guests and your hotel safe.
- Check yourself: Run random security assessments of your system to make sure your security is up to snuff.

"The most important thing," Klein said, "is to be careful and stay educated."