Live Hacking

Live Hacking is one of the most impressive and entertaining ways to demonstrate how easy it is for criminals to gain access to third party data or to spy on others. As a stand-alone event or integrated into your regular meetings – live hacking is the ideal tool for sustainably increasing security awareness in your company.

Live Hacking topics

We offer you a large portfolio of live hacking topics which you can book as either a stand-alone event or as a package. This way, you can easily tailor the event to the needs of your target group. The topics we cover include:

- Google hacking – this confidential information can be sniffed with this hacking technique.
- Reading credit card data using a smartphone
- Phishing - how criminals hook you, what happens next and how to protect yourself.
- Unauthorized access to systems via the wireless interface of presentation remotes.
- Rubber Ducky – these are the potential dangers of USB interfaces.
- SQL injection and logging in without a password.
- WLAN - The dangers of third-party access points.

Agenda

Each session takes approximately 10 - 30 minutes and starts with a short introduction before proceeding to the actual live hacking demonstration. If required, we schedule in extra time for attendees to ask questions and discuss the issues afterwards.

Our consultants

Our Senior Consultants at the usd HeroLab have many years of practical experience in identifying vulnerabilities and performing pen tests, i.e. in legally hacking our international clients. Moreover, our pentesters are certified according to internationally recognized standards, such as the “Certified Ethical Hacker”, or the “Offensive Security Certified Professional”.

Catalog of Topics

Each hack can be combined and, if desired, packed into a „war story“. We are also happy to consider other individual wishes you may have. Live Hacking sessions take between 10 and 30 minutes.

Hack	Description	Duration
Google Hacking	Using what is known as Google Dorks, it is very easy to gain access to unprotected systems such as printers or webcams over the internet.	10 min.
Credit cards	This scenario demonstrates how credit cards with a contactless payment function can be read using a smartphone.	10 min.
Phishing	This hack demonstrates how dangerous phishing emails can be for careless or untrained users and how phishing attacks can irreversibly transfer money to an attacker‘s account.	25 min.
Prestenter Hack	This scenario demonstrates, how an attacker can get unauthorized access to the system via the radio interface of a presenter.	15 min.
Rubber Ducky	Using a USB flash drive, an attacker can compromise systems without much effort in order to access or encrypt data.	15 min.
SMS Spoofing	This scenario illustrates how easily SMS messages can be forged and addresses the risks associated with SMS spoofing in combination with other attack scenarios.	10 min.
SQL Injection	This hack shows how an attacker can use SQL Injection to get unauthorized access to a sample online bank.	20 min.
WLAN Hack	This hack demonstrates the risks connected to the use of public networks and also shows how dangerous the automatic WiFi search function of mobile devices can be.	20 min.

usd AG
Frankfurter Straße 233, Haus C1
63263 Neu-Isenburg, Germany | www.usd.de
Phone: +49 6102 8631-190 | E-mail: sales@usd.de
PGP or S/MIME for secure communication