

# Warum?

Lernen Sie bei einem Live Hacking die Gefahren kennen, die im Umgang mit bewährten und neuen digitalen Medien entstehen.

Bei allen Vortragsformaten geht es darum, den Stand der IT-Sicherheit darzustellen. Denn wer sich vor Angriffen, Sicherheitslücken und Betrugsmaschinen schützen will, der muss diese zuerst einmal kennenlernen. Zu wissen wie Kriminelle vorgehen, schafft zusätzlich eine gesunde Aufmerksamkeit um auch bei neuartigen Betrugsmaschinen die richtige Skepsis an den Tag legen zu können. Je nach Dauer der Veranstaltungen können die vielfältigen Cyber Angriffe und Schutzmaßnahmen ausführlich besprochen werden.

Das Institut für Internet-Sicherheit ist bundesweit für den flexiblen Einsatz vor unterschiedlichsten Zielgruppen bekannt.

Ob Konferenz, Messe oder Kongress. Live Hacking Auftritte sind eine willkommene Abwechslung zum üblichen Vortragsprogramm. Auf fachfremden wie auch auf IT Veranstaltungen sind die Shows ein Publikumsmagnet, der Ihnen Aufmerksamkeit verschafft. Falls Sie auf Messen mehr Besucher wünschen, ist ein einmaliger oder wiederkehrendes Live Hacking die Chance für Sie ihren Stand zu füllen und so auf Ihr Produkt aufmerksam zu machen.

Sprechen Sie uns bei Bedarf gerne an!

# Kontakt

Institut für Internet-Sicherheit  
Neidenburger Str. 43  
45897 Gelsenkirchen



[www.internet-sicherheit.de](http://www.internet-sicherheit.de)  
[www.internet-sicherheit.de/live-hacking](http://www.internet-sicherheit.de/live-hacking)



[hacking@internet-sicherheit.de](mailto:hacking@internet-sicherheit.de)



+49 (0) 209 - 9596 - 766

Sie haben Fragen, Themenwünsche oder eine besondere Art der Veranstaltung?

Rufen Sie an oder schreiben Sie eine unverbindliche E-Mail.

# Live Hacking

Institut für Internet-Sicherheit

Komplexität einfach dargestellt.



# Live Hacking Szenarien

## WLAN

Kostenlos, aber nicht umsonst!



Offene Hotspots sind nach wie vor kein Standard in Deutschland. Aber was ist wenn man doch mal ein offenes Netz findet? Ist ein seriöser Name und ein Zugangsportaal ein Indiz dafür, dass es ein seriöser Hotspot ist? Gibt es in Zeiten zunehmender Verschlüsselung denn überhaupt noch Gefahren in öffentlichen Netzwerken?

## Passwort

Wie steht es um ihre digitale Identität?



Das Passwort ist ein großes Sicherheitsproblem. Zahlreiche Datenlecks, Passwörter im Klartext oder schlichtweg zu erratende Passwörter machen den Identitätsdiebstahl einfach. Wir zeigen Ihnen Möglichkeiten ihre digitale Identität zu schützen, zu welchen Hilfsmitteln Sie greifen können und warum wir uns vom Passwort verabschieden sollten.

## Soziale Netzwerke

Das Eintrittstor für Kriminelle!



Sie gelten als Privatsache und sind für den Arbeitgeber tabu? Gut möglich - ein Angreifer schreckt jedoch nicht davor zurück Informationen zu verwenden, die frei im Internet verfügbar sind. Wir zeigen, wie Kriminelle Facebook, Instagram, Xing und LinkedIn ausnutzen um ihnen und ihrem Unternehmen zu schaden.

## E-Mails

Prinzen, Astronauten und Geschenke



Die Zeit von Betrugsemails ist längst nicht vorbei. Die immer besser werdenden Spam- und Phishing Mails beinhalten nur noch selten Rechtschreibfehler. Wir zeigen Ihnen, warum Phishing Mails selbst für Konzerne zum Problem werden und welcher technischen Methoden sich die Angreifer bedienen!

## Call ID Spoofing

Wenn die Polizei anruft!



Die Telefonnummer ist schon lange kein Garant mehr dafür, dass derjenige am anderen Telefon auch der ist, der er zu sein scheint. In Zeiten von VoIP ist das Anrufen von anderen Telefonnummern ein Kinderspiel. Wir zeigen Ihnen, wie es geht und wie Sie überprüfen können, ob Sie tatsächlich von ihrem Enkel, der Polizei oder der Feuerwehr angerufen werden.

## USB-Geräte

...und andere Wölfe im Schafspelz!



Verbieten, regulieren oder einfach zulassen? Diese Frage muss sich über kurz oder lang jede Organisation stellen, wenn es um die Handhabung von USB-Sticks geht. Wir zeigen die gefährlichsten und schädlichsten Geräte. Wie Sie sich schützen? Das ist nach unserer Vorführung kein Geheimnis mehr!

## individuelle Szenarien

Lassen Sie sich von uns Ihr persönliches Szenario zuschneiden