Hack The Government (HTG) 2025

Häufig gestellte Fragen

Was ist ein „ethischer Hacker”?

Ursprünglich bezeichnete der Begriff *„Hacker”* Menschen, die sich leidenschaftlich für das Basteln interessierten und in der Lage waren, alle möglichen Dinge (einschließlich Ideen!) zu erforschen und zu verändern. Im Laufe der Zeit hat sich ihr Tätigkeitsbereich hauptsächlich auf Informatik und Technologie verlagert. Im Wesentlichen sind sie Erfinder, die sich durch Entdeckungsfreude und Innovationskraft auszeichnen.

Der Begriff „ethischer Hacker” ist eng mit der IT-Sicherheit verbunden. Er bezeichnet „Schwachstellenjäger”, also Experten, deren Hauptaufgabe darin besteht, Schwachstellen in IT-Systemen aufzuspüren. Der wesentliche Unterschied liegt in ihrer Vorgehensweise: Sie sind konstruktiv und handeln ausschließlich im Rahmen der Legalität.

Warum ist ihre Tätigkeit im Bereich der Cybersicherheit so wichtig?

Die größten Gefahren in einem IT-System liegen in:

1. nicht behobene (bekannte) Schwachstellen;
2. unbekannten Schwachstellen (sogenannten „Zero-Day-Schwachstellen”).

Es ist alles eine Frage der Zeit. Im ersten Fall können routinemäßige Audits oder Sicherheitskontrollen das Problem identifizieren und beheben (im Fachjargon spricht man vom „Patching” der Schwachstelle).

Im zweiten Fall kann die Zeit jedoch entscheidend sein. Böswillige Akteure haben dann die Möglichkeit, die Schwachstelle schnell auszunutzen, um eine Organisation anzugreifen oder zu schädigen, was potenziell verheerende Folgen wie Produktions- oder Dienstleistungsausfälle haben kann.

Darüber hinaus verkürzt sich mit der rasanten Entwicklung der Kommunikations- und Informationstechnologien die Zeit bis zur Ausnutzung von Zero-Day-Schwachstellen in der Regel auf weniger als 24 Stunden.

Welche Rolle spielt das ZCB?

Das Zentrum für Cybersicherheit Belgien (ZCB) verfügt über ein einfaches Verfahren, um Personen zu helfen, die Sicherheitsprobleme in Software oder IT-Diensten entdecken.

Wie funktioniert das?

Jeder kann eine Sicherheitslücke melden, auch wenn die betroffene Organisation kein offizielles Programm für solche Meldungen hat. Hier sind einige wichtige Regeln, die zu beachten sind.
Für Personen, die eine Schwachstelle entdecken:

- Sie müssen in gutem Glauben handeln.
- Sie dürfen keine böswilligen Absichten haben.
- Beschränken Sie Ihre Handlungen auf das zur Demonstration des Problems unbedingt Notwendige.
- Informieren Sie direkt die Organisation und das ZCB.

Rechtsschutz:

- Wenn Sie diese Regeln befolgen, sind Sie rechtlich geschützt.
- Ihr Vorgehen wird als konstruktiv und verantwortungsbewusst angesehen.

Was ist „Hack the Government"?

HackTheGovernment2025 ist eine Initiative des Zentrums für Cybersicherheit Belgien (ZCB) zur Stärkung der digitalen Sicherheit der belgischen öffentlichen Dienste.

Ethische Hacker sind eingeladen, die IT-Systeme bestimmter öffentlicher Einrichtungen zu testen, mit dem einzigen Ziel, Schwachstellen auf verantwortungsvolle Weise aufzudecken und zu melden. Über einen einfachen Wettbewerb hinaus handelt es sich um einen echten Aufruf zur Zusammenarbeit aller Akteure, um das Niveau der nationalen Cybersicherheit zu erhöhen.

Warum ist das wichtig?

Dieser Prozess ermöglicht es, die digitale Sicherheit auf kollaborative und ethische Weise zu verbessern. Anstatt zu bestrafen, werden Einzelpersonen dazu ermutigt, aktiv zum kollektiven Schutz beizutragen.

Zusammenfassung: Diese Initiative mobilisiert wohlwollende Experten, um Schwachstellen in öffentlichen IT-Systemen zu identifizieren und so potenzielle Angriffe böswilliger Akteure zu antizipieren. Es handelt sich um einen proaktiven Ansatz, der *letztlich* die öffentlichen Dienste und damit auch die Bürger schützt.