Anleitung

Je größer die Rätselrunde desto besser! Der Moderator der jeweiligen Story nimmt eine Karte vom Stapel und liest die Überschrift und den Hinweis der Deckkarte vor. Auf der Rückseite der Karte befindet sich die Auflösung, die nur der Moderator lesen darf. Der Rest der Gruppe stellt anschließend Fragen. Diese müssen so formuliert sein, dass der Moderator nur mit JA oder NEIN antworten kann. Mit den richtigen Fragen tastet ihr euch nach und nach an die Lösung heran. Sobald der Vorfall in seinen Grundzügen rekonstruiert wurde, kann der Moderator die Rückseite für alle vorlesen und das Rätsel auflösen.

SECURITY STORIES

Phishing

Angriff auf Bundestagsabgeordnete

Im März 2021 wurde ein erneuter Angriff auf den deutschen Bundestag bekannt. Russische Cracker sendeten mindestens sieben Bundestagsabgeordneten und 31 Landtagsabgeordneten Spear-Phishing E-Mails. Diese kamen von angeblich vertrauenswürdigen Absendern und wurden an die privaten Adressen der Abgeordneten geschickt.

Ransomware

WannaCry

Es begann 2017 in Russland. Inzwischen ist die Ransomware WannaCry weltweit verbreitet.
Ein Kryptotrojaner, der Daten auf betroffenen Computern verschlüsselt. Die Cracker verlangen für die Entschlüsselung eine Zahlung in Bitcoins. Besonders schwer wurde der National Health Service (NHS) in Großbritannien getroffen.

Distributed Denial of Service (DDoS)

AWS Amazon Cloud

Februar 2020 meldete die Amazon Cloud-Sparte AWS den vermutlich größten DDoS-Angriff aller Zeiten. Nach eigenen Angaben wehrten sie einen Versuch mit 2,3 Terabit pro Sekunde ab. Die Angreifer sendeten CLDAP-Anfragen an einen LDAP-Server und tarnten die Sender-IP als die des Ziels und überfluteten so den Server.

Man in the Middle (MitM)

NSA tarnt sich als Google

Berichten zufolge hat sich die NSA 2013 als Google ausgegeben.
Die brasilianische Seite „Fantastico“ hat ein Dokument von Edward Snowden erhalten und veröffentlicht, das zeigt, wie ein „Man-in-the-Middle-Angriff“ in Kooperation mit Google durchgeführt wurde.

Social Engineering

Motorola wird Ziel von Kevin Mitnick

Trotz Bewährungsstrafe hörte der Cracker Kevin Mitnick die Voicemails der Polizei ab, die ihn überwachte. Auf der Flucht verschaffte er sich durch nur neun Social-Engineering-Anrufe den Source Code der Firma „Motorola“. Diesen modifizierte er so, dass weder Handy-ID noch Netzwerkverbindungen auf ihn zurückgeführt werden konnten.

Online Services

The Spamhaus Project

Was als gemeinnütziges Projekt begann, endete in einer heißen Diskussion: Der „IP and Domain Reputation Checker“. Eine Liste, mit der die Nutzer IPs und Domains suchen können. Bei problematischen Ergebnissen, wird ein entsprechender Hinweis ausgegeben.
Der Streit entstand durch die intransparente Zuordnung in „gute“ oder „schlechte“ Domains.

Wurm

Stuxnet

Bereits 2005 wurde die erste Version des Stuxnet-Wurms im Netz hochgeladen. Auf die Zentrifugen von Urananlagen spezialisiert, sollte er das iranische Atomprogramm stören. Die Infektion verbreitete sich unter anderem über Siemens Projektdateien und Lücken im Windows-System. Fünf Jahre sollte es dauern, bis der Computerwurm entdeckt wurde.

SQL Injection

Wie aus Freepik „free Passwords“ wurde

Eine Plattform, auf der sich User online Bilder herunterladen können.
Der Anbieter Freepik bietet genau diesen Dienst an. Bei einem Angriff, der auf SQL-Injection zurückgriff, wurden von 3,8 Mio. Benutzern Mail-Adresse und gehashte Passwörter abgegriffen.
Nach eigenen Angaben arbeitet Freepik seitdem mit einer erstklassigen Security-Agentur zusammen.

SECURITY STORIES

Reflected XSS

Das Suchfeld „lert.uber.com“

Ein Uber, bitte! Bekannt als größter Taxi-Konkurrent bietet „Uber“ seine Dienste sowohl online als auch per App an.
Das Suchfeld „lert.uber.com“ ermöglichte jedoch einen Reflected XSS-Angriff.
Der Parameter, der ungefiltert vom Eingabefeld übernommen wird, bindet den Request ungefiltert in die Antwort HTML-Seite ein.

Cross Site Scripting (XSS)

XSS-Lücken beim ARD

2012 rühmte sich das öffentlich-rechtliche Fernsehnetzwerk ARD nicht.
Bei einer Untersuchung wurden auf der „ard.de“-Website mehrere XSS-Lücken gefunden und behoben. Schwachstellen ermöglichten es, bösartigen JavaScript-Code in die ARD-Website einzubinden, komplett fremde Inhalte anzuzeigen oder Besucher weiterzuleiten.

IT-Forschung

Studentisches Experiment kostet $100 Mio.

Der 23-jährige Student Robert Morris setzte 1988 einen Computerwurm im Internet frei.
Ursprünglich sollte das Programm Computer zählen. Morris betonte sein „Versehen“, während in Code-Kommentaren Wörter wie „steal“ oder „attack“ gefunden wurden. Eine Diskette des Morris-Wurms ist im Computer History Museum ausgestellt - Robert inzwischen Professor am MIT.

Stored Xss

Angriff auf den „Steam React Chat-Client“

Der Steam-Chat-Client nutzt moderne und sichere Technologien.
Basierend auf „React“ ist der Dienst mit allen modernen JavaScript-Anwendungsframeworks ausgestattet.
Dennoch wurden Stored XSS-Optionen publiziert. Steam ist beispielsweise für die JavaScript-URI-Injection anfällig.

Insider

Edward Snowden

Sein Name ist weltbekannt: Edward Snowden - ehemaliger Mitarbeiter der NSA brachte 2013 den Spionageskandal ins Rollen. Er veröffentlichte Dokumente, die bewiesen, dass die USA und Großbritannien andere Länder ausspionieren. Auch Privatpersonen sind betroffen. Snowden droht seitdem die Inhaftierung.

SECURITY STORIES

Trojaner

Emotet

Emotet - Ein Trojaner, der Kontakte und Mail-Verläufe analysiert und sich so über seine vermeintliche Glaubhaftigkeit verbreitet.
Nach dem Öffnen eines Anhangs oder Links wird weitere Schadsoftware installiert. Die Folgen reichten von Produktionsausfällen bis hin zum Kontrollverlust der eigenen Daten.

Programmfehler in OpenSSL-Code

Heartbleed

Der Heartbleed-Bug: Ein schwerwiegender Programmfehler in älteren Versionen der Open-Source-Bibliothek OpenSSL, durch den über verschlüsselte TLS-Verbindungen private Daten von Clients und Servern ausgelesen werden können. Dazu wurde die periodische Überprüfung ausgenutzt, die prüft, ob die Verbindung zum Server noch besteht - der sogenannte Heartbeat.

Chiffre

Caesar

Das vermutlich älteste Verschlüsselungsverfahren reicht bis ins Jahr 50 v. Chr. zurück: Die Caesar-Chiffre.
Der Klartext wird durch eine Verschiebung des Alphabets verschlüsselt. Eine einfache Häufigkeitsanalyse oder ein systematischer Buchstabenaustausch macht die Chiffre sehr leicht zu knacken.

Brute-Force

„Club Nintendo“ Konten

2013 wurde ein erfolgreicher Brute-Force-Angriff auf die Club Nintendo-Website bemerkt. Ca. 24.000 Gamer-Konten wurden gehackt und Namen, Privatadressen, Telefonnummern und E-Mail-Adressen eingezogen. Rechnungsinformationen wie hinterlegte Kreditkarten oder ähnliches blieben unversehrt. Es wurden 15 Mio. nicht autorisierte Login-Versuche während des Angriffs aufgezeichnet.

Enigma

Alan Turing

Alan Turing: Der Mann, der Hitlers Geheimcode knackte.
Die Deutschen verschlüsselten
ihren Funkverkehr im 2. Weltkrieg mit der Chiffremaschine „Enigma“. Jedes einzelne Zeichen wurde mit einem individuellen Schlüssel chiffriert und ermöglicht mehr als 10^{23} Kodierungsvarianten.

Ping of Death

Historischer Netzwerkangriff

Der „Ping of Death“ - eine historische Paketbombe. Die Denial-of-Service-Attacke nutzt das „Internet Control Message Protocol“ (ICMP) und verschickt ein bösartiges Datenpaket. Seit 1998 ist die Mehrheit der Systeme gegen diesen Angriffstyp geschützt und somit nur noch sehr selten relevant.

Smurf-Attacke

University of Minnesota

1998 wurde ein „Smurf-DDoS“- Angriff auf das Netzwerk der University of Minnesota durchgeführt. Es wurde nicht nur das anvisierte Computersystem überlastet. Die Attacke löste eine Kettenreaktion aus und sorgte für Beeinträchtigungen von Netzwerken im gesamten Bundesstaat.

Input Validation

Japanese Stock Trader

Im Dezember 2005 unterlief einem japanischen Wertpapierhändler ein Tippfehler in Höhe von 1 Milliarde Dollar, als er versehentlich 600.000 Aktien zu je 1 Yen verkaufte, anstatt eine Aktie für 600.000 Yen. Mit ein paar Zeilen Code hätte sich dieser Fehler vielleicht vermeiden lassen.

Coding Errors

goto fail Bug

Der „goto fail“-Bug von Apple war eine duplizierte Codezeile, die 2014 dazu führte, dass die Prüfung eines Zertifikats für einen öffentlichen Schlüssel fälschlicherweise bestanden wurde.
Der GnuTLS-“goto fail“-Bug war dem Apple-Bug ähnlich und wurde etwa zwei Wochen später entdeckt. Der GnuTLS-Bug ermöglichte es Angreifern ebenfalls, die SSL/TLS-Sicherheit zu umgehen - das betraf über 200 Pakete auf einem typischen Linux-System.

Distributed Denial of Service (DDoS)

GitHub Incident 2018

GitHub - eine online Verwaltungssoftware. Von vielen Privatpersonen und Firmen genutzt, wird die Plattform auch immer wieder zum Angriffsziel.
2018 war GitHub 10 Minuten nicht erreichbar, aufgrund eines Distributed-Denial-of-Service (DDoS)-Angriffs. Die Strategie funktionierte, indem Memcached-Instanzen missbraucht wurden.

Replay Attacke

Software Defined Radio

Ein Software Defined Radio (SDR) empfängt und sendet Funksignale. Am Beispiel des „HackRF One“ kann eine einfache Replay Attacke durchgeführt werden. Hierbei zeichnet das Tool hackrf_transfer ein ausgehendes Signal auf. Dies kann beispielsweise der Funk für das Öffnen eines Garagentors sein. Durch simples Abspielen der Aufzeichnung kann auch der Hacker das Tor öffnen.

Kryptoanalyse

Known-Plaintext-Angriff

Bei der Known-Plaintext-Attacke besitzt der Angreifer zusätzlich zum Geheimtext auch einen Teil des Klartexts.
Mit Hilfe dieses lesbaren Abschnitts können Rückschlüsse auf den Gesamttext gezogen werden. Moderne Verschlüsselungstechniken sind weitgehend resistent gegen diese Angriffsform.

Evil Maid

Angriff auf Komponenten mit physischem Zugriff

Evil Maid - eine Bezeichnung, die nicht auf eine Spezialeinheit von Dienstmädchen („Maids“) bezogen ist.
Beim gleichnamigen Angriff geht es um die Strategie: Der Angreifer hat physischen Zugang zu einem Gerät und nutzt diesen aus. Er könnte beispielsweise Schadsoftware oder einen Keylogger installieren. Der Begriff wurde 2009 von Joanna Rutkowska geprägt.

Wardriving

Business Theft in Seattle

Wardriving: Systematische Suche nach veralteten, unsicheren WLANs während einer Autofahrt.
In Seattle machten sich zwei Männer diese Strategie zu eigen. Mit ihrem schwarzen Mercedes lokalisierten sie Wi-Fi Router, die noch den veralteten „WEP wireless security standard“ erfüllten und raubten digitales Gut im Wert von hunderttausenden von Dollar.

Broken Random Number Generator

OpenSSL Patch

Um eine von Valgrind ausgegebene Warnung zu beheben, hat ein Maintainer von Debian OpenSSL gepatcht und dabei den Zufallszahlengenerator unbrauchbar gemacht. Der Patch wurde im September 2006 hochgeladen und fand seinen Weg in die offizielle Veröffentlichung; er wurde erst im April 2008 gemeldet. Jeder Schlüssel, der mit der fehlerhaften Version erzeugt wurde, ist kompromittiert, da es die „Zufallszahlen“ leicht vorhersehbar macht.

Social Engineering

z.B. Gewinnversprechen

Nicht nur per Telefon oder E-Mail melden sich die Betrüger, sondern auch per Post. Sie schicken Briefe an ihre Opfer, in denen sie hohe Geldgewinne versprechen, die sie angeblich für den „glücklichen Gewinner“ erstritten hätten.

Hacking Corona

Angriff auf Irlands öffentlichen Gesundheitsdienst

Im Mai 2021 wütete nicht nur der Corona-Virus. Unbekannte Cracker griffen den irischen Gesundheitsdienst HSE an. Die IT musste heruntergefahren werden - Kliniken liefen kurzzeitig im Notbetrieb. Eine Manipulation oder Störung der Corona-Impfungen konnte verhindert werden.

Aktions-Karte

Eine Person aus der Runde darf sich einen beliebigen IT-Sicherheitsvorfall nach Lust und Laune auswählen und dem Rest der Runde vorstellen. Es darf gerne ein ausgefallener Vorfall sein.

SECURITY STORIES

Die Macher

Idee:	Susanne Kießling
Umsetzung:	Sophia Reinholdt, Susanne Kießling

Security Stories sind innerhalb des Projekts HITSSSE - Höhere IT-Sicherheit durch sichere Software Entwicklung entstanden, gefördert innerhalb der Initiative IT-Sicherheit in der Wirtschaft des Bundesministeriums für Wirtschaft und Klimaschutz.

HITSSSE
Höhere IT-Sicherheit durch Sichere Software Entwicklung

HSA_innos
Institut für innovative Sicherheit

IT-Sicherheit
IN DER WIRTSCHAFT

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

SECURITY STORIES