Hackerangriff auf Heartland Payment im Jahre 2008

Der grösste Hackerangriff jemals

Seit 2008 führt das US-Unternehmen Heartland Payment Systems die Liste an und gilt als weltweit größer Hack aller Zeiten. Im Zuge des Hacks wurden über 130 Millionen Kreditkarten-Daten gestohlen. Der Schaden des Unternehmens belief sich auf knapp 110 Millionen Dollar.

Der Organisator und Kopf der Unternehmung konnte 2010 gefasst werden. Albert Gonzales bekam 20 Jahre Haft für den Angriff auf das Unternehmen.

Quelle: https://www.diepresse.com/5123711/die-zwoelf-groessten-hacker-angriffe#slide-0

So lief der Millionen-Hack

Der nun angeklagte Hacker Albert Gonzalez scheint einer dieser Experten zu sein. Das erkannte der US-Geheimdienst offenbar schon 2003, als der Mann zum ersten Mal wegen Datendiebstahls angeklagt wurde. Dem " Wall Street Journal " zufolge wurde Gonzalez daraufhin vom Secret Service zeitweise als Informant und freier Mitarbeiter engagiert, sollte helfen, Hacker und andere Internet-Kriminelle aufzuspüren. Offenbar nutzte der Mann aus Miami die Informationen aus diesem Nebenjob allerdings auch, um Verdächtige und Kriminelle über polizeiliche Ermittlungen zu informieren und liebte einen aufwendigen Lebensstil.

Er war nicht der einzige in diesem Hackerangriff. Gonzalez hat mit Hilfe seiner Kontakte eine internationale Truppe zusammengetrommelt. Im Anschluss begannen sie damit, ihre Angriffe aufwendig vorzubereiten, Schadsoftware zu schreiben. Um sicher zu gehen, dass ihre Software unentdeckt bleibt, sollen die Hacker ihre Schnüffelprogramme gegen insgesamt 20 Antivirenprogrammen getestet haben.

Ab dem September 2007 begannen die Hacker dann, die Netzwerke ihrer Opfer zu infiltrieren. Die Methode war offenbar immer gleich: Über eine Sicherheitslücke schleusten sie eigene Software in die Datenbanken der Unternehmen ein. Die erweiterte die von den Opfern genutzte Datenbanksprache SQL (Structured Query Language) um einige eigene Befehle. Derart in das System integriert konnten die Diebe automatisch Kreditkartennummern, Prüfziffern und Kundendaten abfragen und auf ihre eigenen Server überspielen lassen.

Experten zufolge sind derartige Schwachstellen in SQL-Datenbanken durchaus vermeidbar. Erst im Januar 2009 wurde das Leck bei der größten der drei angegriffenen Firmen, dem Finanzdienstleister Heartland Payment Systems, entdeckt. Nun bewahrheiten sich die Befürchtungen von Experten, die schon damals glaubten, es könnte sich dabei um den größten Fall von Kreditkarten-Datenmissbrauch in den USA handeln.

Quelle: https://www.spiegel.de/netzwelt/web/datendiebstahl-in-den-usa-so-lief-der-millionen-hack-a-643436.html

Der Begriff der Personenbezogenen Daten ist, so wie die Daten im Gesetz definiert sind und die Rechtsprechung formuliert wird, **möglichst weit auszulegen**.

Warum werden personenbezogene Daten kategorisiert?

Der Gesetzgeber sieht vor, das personenbezogene Daten einer **unterschiedlichen Schutzbedürftigkeit** unterliegen. Das heißt, dass manche Informationen strenger geschützt werden müssen, als andere. Wenn man bedenkt, dass beispielsweise die **Augenfarbe eines Menschen** andere Rückschlüsse auf diesen zulässt als seine Sozialversicherungsnummer, ist dies nur verständlich.

Das Datenschutzrecht unterscheidet zwischen vielen verschiedenen Kategorien. Dazu gehören:

- Allgemeine Personendaten
- Kennnummern
- Bankdaten
- Patientendaten
- physische Merkmale
- oder Besitzmerkmale.

Von besonderem Interesse sowohl für Betroffene wie für Verarbeitende sind die **besonders schutzwürdigen personenbezogenen Daten**, die in Art. 9 Nr. 1 DSGVO definiert sind.

Die allgemeinen personenbezogenen Daten

Die meisten Daten lassen sich umgangssprachlich mit dem Begriff **allgemeine personenbezogenen Daten**

Google

unterschied datenschutz und datensicherheit

Alle | Bilder | Bücher | Videos | News | Mehr | Suchfilter | SafeSearch

Ungefähr 366'000 Ergebnisse (0.35 Sekunden)

Während man sich beim Datenschutz ausschließlich mit personenbezogenen Daten befasst, besteht das Ziel bei der Datensicherheit darin, alle Arten von Informationen zu schützen, unabhängig davon, ob sie digital oder analog sind, von einer natürlichen Person stammen oder nicht. 05.10.2022

Compliance Aspekte
https://compliance-aspekte.de › artikel › datenschutz-vs-...

Unterschied zwischen Datenschutz und Datensicherheit

Informationen zu hervorgehobenen Snippets • Feedback geben

Weitere Fragen

Was ist unter Datenschutz und Datensicherheit zu verstehen?

Was versteht man unter Datensicherheit einfach erklärt?

Eine umfangreiche Zeitleiste der Hacker-Geschichte, einschließlich der aufkommenden terroristischen und staatlichen Hackerangriffe der modernen Zeit finden Sie hier.

Arten von Hackerangriffen/Hackertypen

Ganz allgemein kann man sagen, dass Hacker wegen einem der folgenden vier Gründe in Rechner und Netzwerke einzubrechen versuchen.

- Die Aussicht auf finanziellen Gewinn durch Diebstahl von Kreditkartennummern oder die Täuschung von Banksystemen.
- Außerdem motiviert eine höhere „street cred" und das Aufpolieren ihres Images in der Hackersubkultur einige Hacker, wenn sie ihre Spuren auf Websites hinterlassen und als Beweis für ihren Hack etwas zerstören.
- Dann gibt es noch Spionage in Unternehmen, wenn Hacker einer Firma Informationen zu einem Produkt oder Diensten eines Wettbewerbers stehlen wollen, um sich einen Marktvorteil zu verschaffen.
- Und letztendlich führen ganze Nationen staatlich unterstützte Hackerangriffe durch, um an geheime Informationen von Unternehmen und/oder Staaten heranzukommen, die Infrastruktur ihres Gegners zu destabilisieren und Verwirrung im betroffenen Land zu stiften. (Man ist sich einig, dass China und Russland solche Angriffe ausgeführt haben, einschließlich einen auf Forbes.com. Zusätzlich machten vor Kurzem Angriffe auf das Democratic National Committee (DNC) große Schlagzeilen, vor allem nachdem Microsoft behauptet, dass Hacker, die für die Hackerangriffe auf das Democratic National Committee verantwortlich gemacht werden, zuvor unentdeckte Schwachstellen in Microsofts Windows Betriebssystem und Adobe Systems Flash-Software entdeckt hätten. Es gibt auch Beispiele, wo die US-Regierung Hackerangriffen mit Wohlwollen begegnet.)

Allianz für Cyber-Sicherheit

TOP 12
MASSNAHMEN BEI CYBER-ANGRIFFEN

Diese Fragen sollten Sie sich stellen!

Die Bewältigung eines Cyber-Angriffs ist stets individuell und Maßnahmen müssen auf die Gegebenheiten der IT-Infrastruktur vor Ort, die Art des Angriffs und die Zielsetzungen der Organisation angepasst werden. Die in den 12 als Fragen formulierten Punkten implizierten Maßnahmen dienen als Impuls und Hilfestellung bei der individuellen Bewältigung.

Das Dokument richtet sich an IT-Verantwortliche und Administratoren, in erster Linie in kleinen und mittelständischen Unternehmen.

- Wurden erste Bewertungen des Vorfalls durchgeführt, um festzustellen, ob es sich um einen Cyber-Angriff oder lediglich um einen technischen Defekt handelt?
- Haben Sie kontinuierlich Ihre Maßnahmen abgestimmt, dokumentiert und an alle relevanten Personen und Verantwortlichen kommuniziert?
- Wurden System-Protokolle, Log-Dateien, Notizen, Fotos von Bildschirminhalten, Datenträger und andere digitale Informationen forensisch gesichert?
- Haben Sie stets die besonders zeitkritischen und damit vorrangig zu schützenden Geschäftsprozesse im Fokus gehabt?
- Wurden betroffene Systeme vom Netzwerk getrennt? Wurden Internetverbindungen zu den betroffenen Systemen getrennt? Wurden alle unautorisierten Zugriffe unterbunden?
- Wurden Backups gestoppt und vor möglichen weiteren Einwirkungen geschützt?
- Wurden Maßnahmen unternommen, um das gesamte Maß der Ausbreitung festzustellen? Wurden alle angegriffenen Systeme identifiziert?
- Wurden die beim Cyber-Angriff ausgenutzten Schwachstellen in Systemen oder (Geschäfts-) Prozessen durch relevante Maßnahmen adressiert und behoben?
- Wurden, nach Abstimmung, die Polizei oder relevante Behörden (Datenschutz, Meldepflichten, etc.) benachrichtigt?
- Wurden die Zugangsberechtigungen und Authentisierungsmethoden für betroffene (geschäftliche und ggf. private) Accounts überprüft (z.B. neue Passwörter, 2FA)?
- Wird das Netzwerk nach dem Vorfall weiter überwacht, um mögliche erneute Anomalien festzustellen?
- Wurden die betroffenen Daten und Systeme wiederhergestellt oder neu aufgebaut?

Das Dokument ist ein gemeinsames Produkt nachfolgender Organisationen: Bundeskriminalamt, Charter of Trust, Deutscher Industrie- und Handelskammertag e.V., eco – Verband der Internetwirtschaft e.V., Initiative Wirtschaftsschutz, Nationale Initiative für Informations- und Internet-Sicherheit e.V., VOICE - Bundesverband der IT-Anwender e.V., Allianz für Cyber-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik

Stand: September 2019