Forcepoint

Die Entwicklung der Netzwerksicherheit

Cyberangriffe in den vergangenen 35 Jahren im Überblick

Zwar haben sich die Sicherheitsgrenzen im Laufe der Zeit maßgeblich verändert, doch erfordern Faktoren wie die zunehmende Anzahl an Bedrohungen und Angriffen sowie die Komplexität der vernetzten Welt unbedingt einen flexibleren und vertrauenswürdigeren Ansatz zum Schutz von Vermögenswerten, Menschen und Daten.

1986

Erster Computervirus **(Brain)** gelangt in MS-DOS

1987

Virus Vienna erstmals erfolgreich bekämpft (ITW)

1987

Erster selbstverschlüsselnder Dateivirus **(Cascade)**

1988

Erster über das Internet verbreiteter Computerwurm **(Morris Worm)**

1991

Erste Firewall mit Anwendungs-Gateways

1994

Einführung von Firewalls auf Anwendungsebene

1995

Erster Virus in Microsoft Word **(WM.Concept)**

1997

Entwicklung & Veröffentlichung der ersten Software für Datenverkehr im Web

1998

Veröffentlichung von **Snort** (Open-Source-Angriffserkennungssystem)

2000

Erster dokumentierter Denial-of-Service-Angriff **(DoS)**

2006

Vorstellung von Verschleierungstechniken auf den **Black Hat**-Konferenzen

2008

Conficker betrifft 9–15 Millionen Microsoft-Systeme

2009

Einführung von Native Clustering für höchste Verfügbarkeit und Performance

2012

Einführung softwaregestützter Sicherheit (ersetzt Blade-Technologie)

2012

Einführung des Tools Evader

2013

Hacker greifen über die Server der **Target Corporation** Daten von 70–110 Millionen Kunden ab

2013

Yahoo-Datenleck gefährdet 3 Milliarden Nutzer

2015

USA: Eine falsch konfigurierte Datenbank gibt die Daten von 191 Millionen Wählern preis

2016

Entwicklung von Forcepoint aus Websense, Stonesoft, Sidewinder und anderen Raytheon-Sicherheitslösungen

2016

Veröffentlichung erster Cloud-nativer Produktintegrationen

2016

Erste Meldungen zu **TrickBot** (auf MS Windows abzielender Computer-Malware-Trojaner)

2017

Forcepoint X-Labs erkennt eine laufende TrickBot-Kampagne gegen Kryptowährungen

2017

WannaCry (Ransomware-Angriff auf MS Windows) betrifft weltweit 230.000 Computer an einem Tag

2018

Under Armour meldet einen erfolgreichen Cyber-Angriff in die Backend-Datenbank der MyFitnessPal-App

2018

Forcepoint X-Labs erfasst die Entwicklung von Emotet (Banktrojaner, der zu einer Plattform zur Malware-Verbreitung wurde)

2019

Vorübergehende Schließung des neuseeländischen Aktienmarkts aufgrund mehrerer DDoS-Angriffe

2019

LockerGoga-Ransomware gefährdet norwegische Aluminiumproduktion

2020

Cyber-Angriff auf **SolarWinds** – Software-Lieferkette wird aufgedeckt

2020

Forcepoint veröffentlicht Integrationen für die Bedürfnisse moderner Hybrid-Infrastrukturen

2020

Robinhood meldet einen Angriff auf fast 2000 Konten

2021

Ransomware-Angriff auf **JBS Foods** führt zur Schließung von 13 Rinderschlachtfabriken in den USA

2021

Angriff auf **Colonial Pipeline** über ein manipuliertes VPN-Passwort verursacht Gasmangel an der US-Ostküste

2021

Forcepoint übernimmt Cyberinc, Deep Secure und Bitglass

2021

Tausende ahnungslose Opfer von lokaler **Microsoft Exchange Server**-Datenverletzung betroffen

2021

Ransomware-Angriff auf **Kaseya**-Lieferkette legt 1500 Unternehmen lahm

Schützen Sie Ihre Vermögenswerte. Sichern Sie Ihren Netzwerkrand ab.

Mehr über Forcepoint Next-Gen Firewall erfahren

Über Forcepoint

Forcepoint ist einer der weltweit führenden Anbieter von Cyber-Sicherheit im Bereich Anwender- und Datenschutz und hat es sich zur Aufgabe gemacht, Organisationen zu schützen und gleichzeitig die digitale Transformation und das Wachstum voranzutreiben. Die auf menschlichem Verhalten basierenden Lösungen von Forcepoint passen sich in Echtzeit an das Nutzerverhalten an und ermöglichen Mitarbeitern einen sicheren Datenzugriff bei voller Produktivität. Forcepoint mit Sitz in Austin, Texas, schafft sichere, vertrauenswürdige Umgebungen für Tausende von Kunden weltweit.

Forcepoint

forcepoint.com