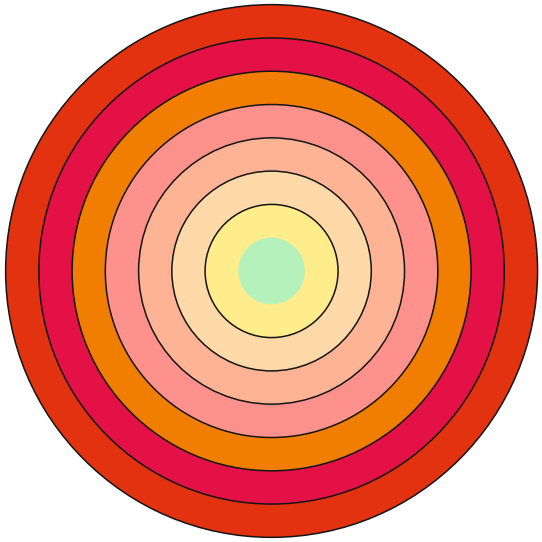


Version 1.0
5. März 2023

conus

www.conus.at

DID – DEFENSE IN DEPTH

EIN GRUNDSÄTZLICHER LEITFADEN FÜR UNTERNEHMEN UND ADMINISTRATOREN

Herangehensweise vor dem Fall der Fälle

PRODUKTLINK:
https://www.conus.at/submain/links/partner_html_files/Defense_In_Depth.pdf

CONUS GmbH.
Kirchstetterngasse 47
1160 Wien
info@conus.at
+41 (0) 1 617 51 44 - 0

DEFINITIONEN

Defense in Depth (auch bekannt als mehrschichtige Sicherheit und mehrschichtige Verteidigung) ist ein Konzept der Informationssicherung (information assurance - IA) Es verwendet mehrere Ebenen von Sicherheitskontrollen (Verteidigungsmaßnahmen), die im gesamten Informationstechnologiesystem (IT-System) platziert sind. Die mehreren Ebenen gehören nicht zum selben Sicherheitstool. Es verwendet verschiedene Sicherheitsarten, von denen jede vor einem anderen Sicherheitsangriff schützt.

ERKLÄRUNG

Tiefenverteidigung ist ursprünglich eine militärische Strategie. Ziel ist es, den Vormarsch eines Angreifers zu verzögern, anstatt ihn zu verhindern, indem Raum geschaffen wird, um Zeit zu gewinnen. Die National Security Agency (NSA) änderte das Konzept zu einem umfassenden Ansatz für Informations- und elektronische Sicherheit.

Durch die Platzierung von Schutzmechanismen, Verfahren und Richtlinien soll die Zuverlässigkeit eines IT-Systems erhöht werden. Mehrere Verteidigungsebenen können Spionage verhindern. Sie verhindern auch direkte Angriffe auf kritische Systeme. Im Hinblick auf die Verteidigung von Computernetzwerken sollten tiefgreifende Verteidigungsmaßnahmen nicht nur Sicherheitsverletzungen verhindern, sondern einem Unternehmen auch Zeit verschaffen, einen Angriff zu erkennen und darauf zu reagieren.

DAS MODELL

Die Tiefenverteidigung wird seit langem am Beispiel der Zwiebel als Beispiel für die verschiedenen Sicherheitsebenen erklärt. Die äußere Schicht enthält die Firewall.[5] Die mittleren Ebenen enthalten verschiedene Steuerelemente. Die Daten befinden sich im Zentrum und werden durch die anderen Verteidigungsmaßnahmen geschützt.

Ein neueres Konzept ist die Kill Chain. Es handelt sich um eine dem Militär entlehnte Methode, um die Tötungskette eines Gegners aufzuspüren und zu durchbrechen.[6] Lockheed Martin adaptierte dieses Konzept auf die Informationssicherheit und nutzte es als Methode zur Modellierung von Einbrüchen in ein Computernetzwerk.

QUELLEN

"Understanding layered security and defense in depth". TechRepublic. Archived from the original on 15 November 2015. Retrieved 13 November 2015.

Michiko Phifer, A Handbook of Military Strategy and Tactics (New Delhi: Vij Books India Private Limited, 2012), p. 102

"Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments" (PDF). Archived from the original (PDF) on 2010-05-13. Retrieved 2015-11-13.

Randy Tanaka. "Back to Basics – Defense in Depth". Western Independent Bankers. Archived from the original on 7 March 2016. Retrieved 13 November 2015.

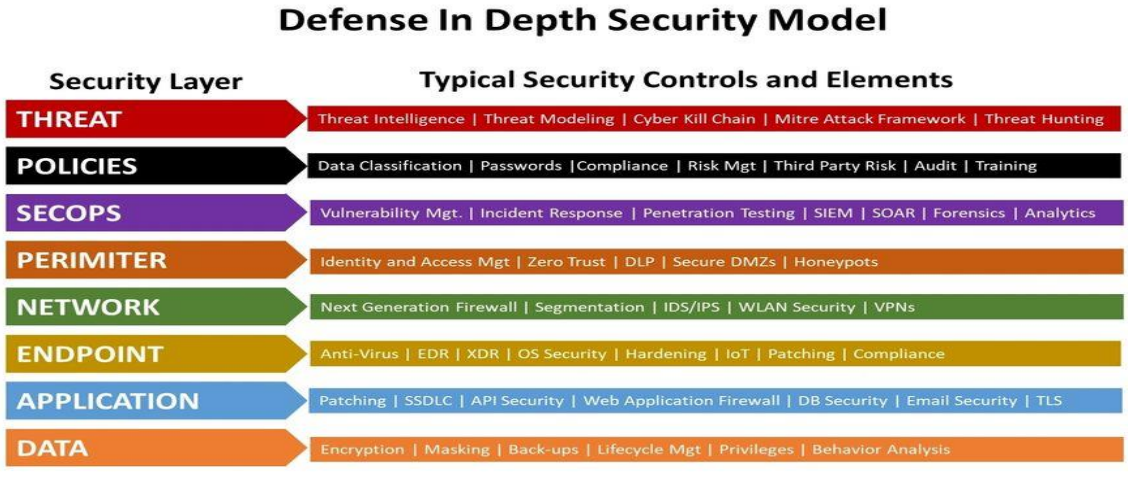
Steve Ocepek (13 August 2014). "Unraveling the Onion: A New Take on Defense-in-Depth". SecureState LLC. Archived from the original on 12 October 2016. Retrieved 13 November 2015.

"The Industrial Control System Cyber Kill Chain". SANS Institute. Retrieved 13 November 2015.

"How Lockheed Martin's 'Kill Chain' Stopped SecurID Attack". Dark Reading. Retrieved 13 November 2015.

DEFENSE IN DEPTH – ONION MODEL

DEFENSE IN DEPTH – KILLCHAIN



Businesses need Defense In Depth for holistic security protection throughout their enterprises

CIS – CENTER FOR INTERNET SECURITY

Das Center for Internet Security (CIS) ist ein Zusammenschluss von Organisationen und Einzelpersonen, um Benchmarks zu definieren, welche Computersysteme im Rahmen eines Einsatzes im Internet gegen Bedrohungen absichern.

US Anweisungen bestehen dabei üblicherweise aus einer Aktion, also der tatsächlich umzusetzenden Handlung, und einer Diskussion, welche die Hintergründe der Anweisung erläutert. Dies unterscheidet sich zum Beispiel vom in Europa verbreiteten Ansatz der IT-Grundschutz-Kataloge, bei denen vereinfacht dargestellt erst die Umgebung des Systems identifiziert und aus der Situation heraus die Bedrohungen und damit die notwendigen Maßnahmen für das jeweilige System evaluiert werden.

CIS Controls Version 8:
https://www.conus.at/submain/links/partner_html_files/CIS_Controls_Version_8.xlsx

DER IT GRUNDSCHUTZ KATALOG

„IT-Grundschutz umfasst Standard-Sicherheitsmaßnahmen für typische IT-Systeme mit ‚normalem' (mittleren) Schutzbedarf".

Die Erkennung und Bewertung von Schwachstellen in IT-Systemen erfolgt oftmals über eine Risikoanalyse, wobei für jedes System oder jede Gruppe gleichartiger Systeme einzeln ein Gefährdungspotential geschätzt und die Kosten eines Schadens an dem System ermittelt wird. Diese Herangehensweise ist sehr zeitaufwändig und dementsprechend teuer.

Der IT-Grundschutz geht von einer für das System üblichen Gefährdungslage aus, die in 80 % der Fälle zutreffend ist und empfiehlt hierfür adäquate Gegenmaßnahmen. So kann ein Sicherheitsniveau erreicht werden, das in den meisten Fällen als ausreichend betrachtet werden kann und daher die wesentlich teurere Risikoanalyse ersetzt. In Fällen eines höheren Sicherheitsbedarfs kann der IT-Grundschutz als Grundlage für weitergehende Maßnahmen genutzt werden.

Die ursprüngliche Zertifizierung nach IT-Grundschutz wurde durch eine anerkannte ISO/IEC 27001-Zertifizierung auf der Basis von IT-Grundschutz vollständig abgelöst.

Im Gegensatz zur ISO 27001 verfolgt der IT-Grundschutz den Bottom-Up-Ansatz und ist damit sehr techniklastig.

IT Grundschutz Kompendium - Edition 2023:
https://www.conus.at/submain/links/partner_html_files/IT_Grundschutz_Kompendium_Edition2023.pdf

- Schutzziele

Die IT-Sicherheit unterteilt sich in drei Schutzziele (auch Grundwerte der Informationssicherheit genannt):

- Vertraulichkeit

Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.

- Integrität

Korrektheit, Manipulationsfreiheit und Unversehrtheit von IT-Systemen, IT-Verfahren und Informationen. Hierbei ist auch die Authentizität (d. h. die Echtheit, Zurechenbarkeit und Glaubwürdigkeit von Informationen) zu berücksichtigen.

- Verfügbarkeit

Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen stehen zum geforderten Zeitpunkt zur Verfügung.

Darüber hinaus steht es dem Anwender frei, weitere Schutzziele (Grundwerte) zu definieren. Beispielhaft seien aufgeführt:

- Nichtabstreitbarkeit (Verbindlichkeit)

Es darf nicht möglich sein, ausgeführte Handlungen abzustreiten.

- Authentizität

Es muss gewährleistet sein, dass es sich tatsächlich um eine autorisierte Person (Identitätsnachweis) handelt oder Informationen echt und glaubwürdig sind.

- Zuverlässigkeit