IMPRESSUM

Computern im Handwerk/ handwerke.de
gegründet 1984, dient als unabhängiges Fachmagazin für moderne Kommunikation den Betrieben der **Bauhaupt- und Nebengewerbe** im „portionierten" Wissens- und Technologietransfer.

Herausgeber: Horst Neureuther

CV Computern-Verlags GmbH
Goethestraße 41, 80336 München

Telefon o 89/54 46 56-0
Telefax o 89/54 46 56-50
Postfach 15 06 05, 80044 München
E-Mail: info@cv-verlag.de
redaktion@cv-verlag.de
www.handwerke.de

Geschäftsleitung:
Dipl.-Vw. H. Tschinkel-Neureuther

Anzeigenleitung:
Dipl.-Vw. Heide Tschinkel-Neureuther
e-mail: anzeigen@cv-verlag.de

Redaktion und redaktionelle Mitarbeiter in dieser Ausgabe:
Nora Bax, Heike Blödorn, Ann-Kathrin Gräfe, Andreas Junck, Sarah Kremer, Björn Lorenz, Verena Mikeleit, Horst Neureuther (verantw.), Gundo Sanders, Sarah Tietjen, Alex Wallberger, Ines Wolf, Mike Wolfe

Anzeigenvertretung:
Medienmarketing SANDERS

Layout:
AD&D Werbeagentur GmbH, Silvia Romann, Dietmar Kraus

Druck:
Walstead NP Druck GmbH, St. Pölten

Druckauflage: 50.500
Tatsächliche Verbreitung: 50.066 (IV/23)
Auflage und Verbreitung kontrolliert.

40. Jahrgang
Erscheinungsweise: 10 x jährlich

Abo-Preis:
29,– € p.a. plus Porto inkl. MwSt.

Einzelpreis: 2,90 €
Ein Abonnement verlängert sich automatisch um ein Jahr, wenn es nicht spätestens 3 Monate vor Ablauf des Bezugszeitraumes gekündigt wird.

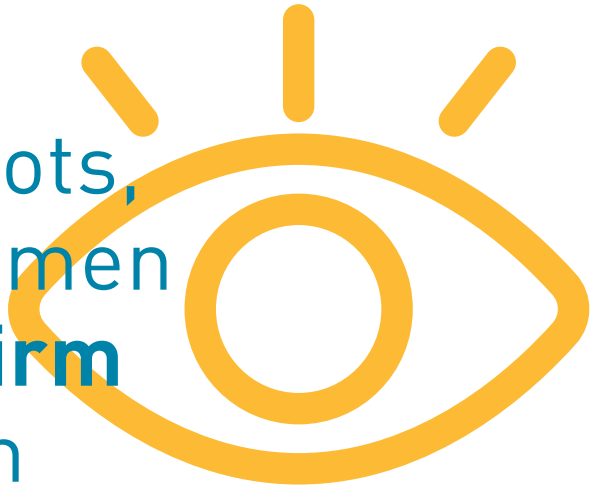
ISSN 0931-4679
Mitglied der Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V. (IVW) Berlin

Zur Zeit gilt die Anzeigenpreisliste Nr. 41 vom 01.11.2023.

Titelkopf: © Fotolia.de/yellowj

NETZWERKSICHERHEIT:

Vier Blind Spots, die Unternehmen **auf dem Schirm** haben sollten



Sogenannte Blind Spots oder auch „blinde Flecken" im Netzwerk treiben den meisten deutschen IT- und Security-Entscheidern die Schweißperlen auf die Stirn – laut einer aktuellen Hybrid-Cloud-Studie[1] von Gigamon sind das 52 Prozent. Das hat zur Folge, daß eine von drei Sicherheitsverletzungen unentdeckt bleibt. Cyberkriminelle kennen und nutzen diese dunklen Ecken gezielt aus, um sich Zugang zum Netzwerk zu verschaffen und Malware zu plazieren oder Daten zu stehlen … | VON ANDREAS JUNCK

Die folgenden Blind Spots zählen zu den kritischsten und unter Cyberkriminellen beliebtesten Schwachstellen von Unternehmensnetzwerken. IT- und Sicherheitsteams sollten diese kennen und aufdecken, bevor sie zu gefährlichen Sicherheitsrisiken werden.

Blind Spot 1: Verschlüsselter Datenverkehr

HTTPS gilt als sicheres Kommunikationsprotokoll, da es Daten verschlüsselt überträgt. Diesen Datenverkehr nutzen Cyberkriminelle immer häufiger als Tarnung und verstecken hier Malware und anderen Schadcode. In Wahrheit verbergen sich 93 % der Malware hinter einer SSL- oder TLS-Verschlüsselung – so eine Untersuchung von Watchguard Threat Lab[2]. Das Vertrauen in diese Verschlüsselungsverfahren scheint allerdings groß zu sein, denn den meisten deutschen IT- und Security-Verantwortlichen fehlt der Einblick in diesen Datenstrom. Laut der Gigamon-Studie wissen nur 21 % von ihnen, was sich in den verschlüsselten Daten befindet, die durch ihr Netzwerk fließen. Im Umkehrschluß bedeutet das, daß 79 % den Datenverkehr ungefiltert passieren lassen. Das liegt unter anderem daran, daß die Entschlüsselung, Analyse und Rückverschlüsselung viel Zeit, Geld und Rechenleistung kostet. Müssen Entscheider aus finanziellen Gründen auf die notwendigen Mittel verzichten, setzen sie ihr Unternehmen einem unnötig hohen Sicherheitsrisiko aus.

Blind Spot 2: Lateraler Datenverkehr

Cloud Computing, Smart Devices und Remote Work: Moderne Technologien bilden heute die Grundlage für einen flexibleren und produktiveren Arbeitsalltag. Für IT- und Sicherheitsteams sind sie der Nährboden für Blind Spots: Ein großer Teil des Datenverkehrs bewegt sich zwischen Geräten, Anwendungen und Systemen lateral durch das Netzwerk und umgeht damit die meisten Sicherheits- und Netzwerk-Tools (East-West-Traffic). Laut der Gigamon-Studie wissen 47 % der deutschen Unternehmen nicht, was genau sich in diesen Daten verbirgt. Dabei können Cyberkriminelle, die Zugang zum Netzwerk haben, den lateralen Traffic nutzen, um Malware zu verstecken. Die schleicht sich dann unbemerkt an den Türstehern des Netzwerks vorbei.

Blind Spot 3: Komplexität

Früher war die Netzwerküberwachung wesentlich einfacher als heute: Alles, was in das Netzwerk wollte, mußte dieselbe Schwelle überschreiten, die um die gesamte zentralisierte IT-Landschaft herum aufgebaut wurde. Doch im Laufe der Zeit haben Unternehmen ihren Tech-Stack um moderne Technologien wie Hybrid-/Multi-Cloud-Umgebungen und IoT massiv erweitert. Auf der einen Seite erleichtern sie die Arbeit und erlauben eine flexible Arbeitsplatzwahl. Auf der anderen Seite bewegen sich Netzwerke,

[1] *https://www.gigamon.com/de/resources/resource-library/white-paper/wp-gigamon-survey-hybrid-cloud-security-2023.html*
[2] *https://www.helpnetsecurity.com/2023/04/06/malware-attack-trends-q4-2022/*

Systeme, Anwendungen und Daten zwangsläufig außerhalb der ursprünglichen Netzwerksgrenze. Diese Entwicklung hat in vielen Unternehmen zu einer sehr hohen IT-Komplexität geführt. Das macht es IT- und Sicherheitsteams nicht nur schwerer, den Überblick über alle Komponenten zu behalten. Auch Cyber-Sicherheitslösungen greifen in den wenigsten Fällen in hybriden und dezentralen Umgebungen.

Blind Spot 4: Shadow- und Legacy-IT

Es kommt vor, daß Mitarbeiter im Homeoffice mit ihren privaten Geräten arbeiten oder ohne das Wissen der IT fremde Anwendungen installieren – zum Beispiel, weil ihnen bestimmte Ressourcen fehlen, um produktiv arbeiten zu können. In der Regel fliegen diese nicht verwalteten Geräte und Anwendungen (Shadow-IT) unter dem Sicherheitsradar des verantwortlichen Teams, weshalb sie schnell zur Gefahr für das Unternehmensnetzwerk werden. Gleiches gilt für Legacy-IT. Oftmals haben Unternehmen seit vielen Jahren dieselben Geräte, wie Drucker und Kopierer, im Einsatz. Da diese mittlerweile über veraltete, potentiell unsichere Protokolle mit dem Netzwerk kommunizieren, sind sie das ideale Zugangstor für Cyberkriminelle.

Mit Deep Observability Licht ins Dunkel bringen

Lediglich 28 % der deutschen IT- und Security-Entscheider haben laut Studie vollumfängliche Einsicht in ihre gesamte IT-Landschaft – und zwar von den Anwendungen bis zum Netzwerk. Für Unternehmen, die die mangelhafte Sichtbarkeit bislang ignoriert haben, besteht dringender Handlungsbedarf. Sie müssen ihre Netzwerkumgebung transparenter machen, um ein umfangreiches Verständnis von ihrem Netzwerk zu erhalten – einschließlich aller Geräte, Anwendungen, User sowie Datenströme und -bewegungen. Erst dann können die verantwortlichen Teams jeden noch so obskuren Blind Spot aufdecken und verborgenen Sicherheitsrisiken entgegenwirken.

Dafür reichen herkömmliche Sicherheits- und Monitoring Tools allerdings nicht mehr aus, da Agents in der Regel nicht solch eine tiefgehende Netzwerkeinsicht haben und hier auch keine analysierbaren Logs erstellt werden. Mithilfe von Deep Observability hingegen profitieren IT- und Sicherheitsteams selbst in komplexen Hybrid- und Multi-Cloud-Umgebungen von Sichtbarkeit bis hinunter auf Netzwerk- und Datenpaketebene. Sämtliche Daten, die ins Netzwerk kommen oder sich innerhalb des Netzwerks bewegen, werden analysiert. Deep-Observability-Mechanismen wie Application Filtering oder Deduplizierung filtern den verschlüsselten Datenverkehr und entschlüsseln nur relevante, potentiell riskante Pakete. Das schont nicht nur die Rechenleistung, sondern auch das Budget.

Darüber hinaus bildet die vollständige Netzwerkeinsicht die Grundlage für weitere Sicherheitskonzepte wie das Zero-Trust-Modell. Denn dafür müssen Teams ganz genau wissen, wo sich sensible Daten in ihrem Netzwerk befinden und wer oder was Zugriff auf diese Inhalte hat. Demnach führt für IT- und Security-Entscheider kein Weg an Deep Observability vorbei. <<

Noch Fragen? ***https://www.gigamon.com***

Andreas Junck, Senior Sales Director DACH bei Gigamon
Bild: Gigamon