DEFENDERBOX
EINFACH.SCHNELL.CYBERSICHER.

Cybersicherheit 2024

Top 10 Trends & Prognosen

Wissenswertes zum Thema Cybersecurity für Ihr Unternehmen.

Vorwort

Aufgrund der akuten Bedrohungslage im digitalen Raum hat die Europäische Union in den letzten Jahren die Vorschriften zur Cybersicherheit immer weiter verschärft. Und was viele Unternehmen weiterhin nicht wissen, ist die Tatsache, dass sie im Fall der Fälle immer selber für ein Versäumnis im Bereich Cybersecurity haften.

In diesem Whitepaper möchten wir die aktuellen Trends & Prognosen beschreiben, die 2024 auf Sie zukommen. Auch zeigen wir auf, wie Sie Ihrer Verantwortung nachkommen können, um Ihr Unternehmen sicherer zu machen und zu schützen.

Markus Schulte, Sicherheitsexperte &
CEO der SMB Cybersecurity GmbH

"Cybersicherheit ist brandaktuell. Hört man sich im Markt um, gibt es niemanden, der das Thema für irrelevant hält. Dazu werden IT-Sicherheitsbedrohungen immer komplexer und vielschichtiger. Aus diesem Grund sollte sich heutzutage jedes Unternehmen schützen."

So machen Sie Ihr Unternehmen cybersicher!

DEFENDERBOX
EINFACH.SCHNELL.CYBERSICHER.

Ist Ihre IT cybersicher?

Klicken Sie auf den Link in der EMail und bestellen Sie einen **kostenlosen** Scan mit der DEFENDERBOX

Finden Sie es heraus

Wir schicken Ihnen die DEFENDERBOX per Post. Sie mailen uns den unterschriebenen Vertrag zur DSGVO Regelung. Sie schließen die Box an Strom & Netzwerk.

Scan/Pentest

Sie müssen nichts weiter tun. Wir starten den Pentest. Alle angeschalteten Geräte in Ihrer IT-Infrastruktur werden gescannt.

Terminvereinbarung

Wir vereinbaren einen persönlichen Termin zur Besprechung.

Negativ

Sie haben derzeit keine Sicherheitslücken! Aber wie lange noch? Vereinbaren Sie regelmäßige Scans, damit es so bleibt!

Positiv

Sie haben **Sicherheitslücken** & **Schwachstellen**. Sie möchten wissen, welche und wie Sie diese schließen. Wir haben den geeigneten Plan für Ihre Scans!

Aktuelle Bedrohungslage

Schon zu Beginn des Jahres 2024 stand Cybersicherheit an der Schwelle zu tiefgreifenden Veränderungen. Cyber-Bedrohungen werden nicht nur immer häufiger, sondern auch immer raffinierter und stellen traditionelle Sicherheitsparadigmen in Frage. In dieser sich schnell entwickelnden digitalen Landschaft ist das Verständnis der kommenden Trends eine Frage der Voraussicht und eine Notwendigkeit für entsprechende Sicherheitsmaßnahmen.

In diesem Whitepaper werden die 10 wichtigsten Cybersecurity-Trends und -Vorhersagen für das kommende Jahr vorgestellt. Gleichzeitig wird erläutert, dass Technologien wie die **DEFENDERBOX** auf diese Veränderungen abgestimmt ist, um die digitale Verteidigung zu stärken.

Trend 1:
Verstärkter Fokus auf KI & maschinelles Lernen (ML) in der Cybersecurity

KI und maschinelles Lernen (ML) werden eine immer wichtigere Rolle in der Cybersicherheit spielen. Die fortschrittlichen Datenanalysefähigkeiten von KI werden zunehmend zur Identifizierung und Vorhersage von Cyberbedrohungen eingesetzt und verbessern die Früherkennungssysteme. ML-Algorithmen werden weiterentwickelt, um neue Bedrohungen besser zu erkennen und auf sie zu reagieren, wodurch die Abwehrmaßnahmen im Laufe der Zeit verbessert werden können.

Die **DEFENDERBOX** hält bereits mit KI gegen KI. Das Innenleben der Box besteht aus KI, einfach, schnell und automatisiert. Das bdeutet aber, regelmäßige Pentests, damit KI weiter lernen kann. ML wird sich wahrscheinlich weiterentwickeln, um Cybersicherheitsprotokolle autonom anzupassen und zu aktualisieren, wodurch die Abhängigkeit von manuellen Aktualisierungen verringert wird. Möglicherweise werden wir bald auch das Aufkommen von KI-gesteuerten Sicherheits-Bots erleben, die so programmiert sind, dass sie selbstständig Cyber-Bedrohungen identifizieren und neutralisieren, wodurch die Netzwerksicherheit proaktiver und weniger reaktiv wird. Diese Entwicklungen deuten auf eine Verlagerung hin zu intelligenteren und autonomeren Cybersicherheitssystemen, die von den Fortschritten in der KI und im ML angetrieben

Trend 2:
Wachsende Bedeutung der IoT-Sicherheit

Das Internet der Dinge (IoT) wird sein exponentielles Wachstum fortsetzen und eine immer größere Anzahl von Geräten miteinander verbinden. Diese Ausbreitung bringt jedoch auch eine Reihe von Sicherheitsherausforderungen mit sich. Die Vielfalt und Allgegenwärtigkeit von IoT-Geräten machen sie zu attraktiven Zielen für Cyberangriffe, und ihre Vernetzung kann zu weit verbreiteten Schwachstellen führen.

Ein Hauptaugenmerk wird 2024 auf der Verbesserung der IoT-Sicherheit liegen. Ein bedeutender Fortschritt wird in der Entwicklung von robusteren, standardisierten Sicherheitsprotokollen für IoT-Geräte erwartet. Dazu könnten universelle Verschlüsselungsstandards und obligatorische Sicherheitszertifizierungen für neue Geräte gehören. Ein weiterer Bereich der Verbesserung könnte die Integration von KI- und ML-Algorithmen in IoT-Systeme sein. Diese Technologien achten dann auf ungewöhnliche Muster, die auf eine Sicherheitsverletzung hindeuten, und eine schnellere Reaktion auf Bedrohungen ermöglichen.

Darüber hinaus wird wahrscheinlich die Aufklärung der Nutzer über die IoT-Sicherheit einen höheren Stellenwert erhalten. In dem Maße, in dem sich die Nutzer potenzieller Risiken und bewährter Verfahren bewusst werden, wird sich die allgemeine Sicherheitslage von IoT-Netzwerken verbessern.

Trend 3:
Ausweitung Homeoffice & die Auswirkung auf die Cybersicherheit

Arbeiten im Homeoffice, ein Trend, der erheblich an Dynamik gewonnen hat, wird die berufliche Landschaft im Jahr 2024 weiter prägen. Diese Verschiebung verstärkt den Fokus auf die Fernarbeitszugänge und die VPN Cybersicherheit.

Die **DEFENDERBOX** ist in diesem Szenario ein wichtiger Akteur, die den Sicherheitsaspekt dieses Arbeitsmodells in den Scans bzw. Pentests berücksichtigt. Dies gewährleistet betriebliche Kontinuität und eine sichere digitale Umgebung, was angesichts der zunehmenden Cyber-Bedrohungen im Zusammenhang mit dem Fernzugriff von entscheidender Bedeutung ist.

Trend 4:
Quantencomputer & seine Auswirkungen auf die Cybersicherheit

Die Quanteninformatik, die sich im Jahr 2024 rasant weiterentwickelt, revolutioniert die Art und Weise, wie wir über Datenverarbeitung und Problemlösung denken. Im Gegensatz zum klassischen Rechnen mit Bits als 0 oder 1, werden beim Quantencomputing Qubits verwendet. Dank der Quantenüberlagerung können Qubits in mehreren Zuständen gleichzeitig existieren. Dadurch verarbeiten Quantencomputer riesige Datenmengen in noch nie dagewesener Geschwindigkeit und lösen komplexe Probleme viel schneller als herkömmliche Computer. Der Aufstieg des Quantencomputers bietet sowohl Chancen als auch Herausforderungen für die Cybersicherheit. In Sachen Cybersicherheit verbessern Quantencomputer Verschlüsselungsmethoden, entwickeln ausgefeiltere Algorithmen zur Erkennung von Cyber-Bedrohungen und verwalten groß angelegte, sichere Datenoperationen effizient.

Auf der anderen Seite stellt das Quantencomputing eine erhebliche Bedrohung für die derzeitigen Cybersicherheitsprotokolle dar. Seine Fähigkeit, traditionelle Verschlüsselungsmethoden wie RSA und ECC schnell zu brechen, machen viele bestehende Sicherheitssysteme angreifbar. Diese Anfälligkeit unterstreicht die dringende Notwendigkeit, quantenresistente Verschlüsselungstechniken zu entwickeln, ein Bereich, der als Post-Quantum-Kryptographie bekannt ist.

Trend 5:
Entwicklung von Phishing-Angriffen

Phishing-Angriffe sind seit langem eine ständige Bedrohung für die Cybersicherheit, und im Jahr 2024 werden sie noch raffinierter und effektiver. Moderne Phishing-Angriffe sind immer geschickter darin geworden, herkömmliche Sicherheitsmaßnahmen zu umgehen, indem sie personalisiertere und technisch fortschrittlichere Taktiken einsetzen, um Benutzer zu täuschen.

Angesichts dieser fortschrittlichen Phishing-Angriffe sind robuste Authentifizierungssysteme der Schlüssel zur Verbesserung der Sicherheit. Die **DEFENDERBOX** und Identeco, führender DSGVO-konformer deutscher Anbieter für den Schutz von Benutzerkonten, haben bereits einen Proof-of-Concept gestartet, um in Echtzeit geleakte Unternehmens-Accounts zu finden. So wird eine Sicherheitslücke umgehend geschlossen.

Trend 6:
Erhöhter Fokus auf mobile Sicherheit

Da mobile Geräte im Jahr 2024 noch mehr zum festen Bestandteil des privaten und beruflichen Lebens werden, rückt die mobile Sicherheit immer stärker in den Mittelpunkt.

Die zunehmende Abhängigkeit von mobilen Geräten für verschiedene Aufgaben, einschließlich Remote-Arbeit, Finanztransaktionen und persönlicher Kommunikation, macht sie zu attraktiven Zielen für Cyber-Attacken. Sobald sich die mobilen Devices allerdings im Netzwerk befinden, werden sie von der **DEFENDERBOX** erfasst und gescannt. Eine notwendige Sicherheitslösung.

Trend 7:
Zero Trust Sicherheit

Das Konzept der Zero-Trust-Sicherheit hat im Jahr 2023 erheblich an Dynamik gewonnen und sich von einem Nischenansatz zu einem grundlegenden Aspekt der Cybersicherheitsstrategie entwickelt.

Im Kern funktioniert Zero Trust nach dem Prinzip "never trust, always verify". Im Gegensatz zu traditionellen Sicherheitsmodellen, die sich auf die Absicherung des Perimeters konzentrieren, geht Zero Trust davon aus, dass Bedrohungen sowohl außerhalb als auch innerhalb des Netzwerks existieren. In einem Zero-Trust-Modell wird jede Zugriffsanfrage, unabhängig von ihrem Ursprung oder dem Netzwerk, in dem sie sich befindet, als potenzielle Bedrohung behandelt. Dies erfordert eine rigorose Identitätsüberprüfung, strenge Zugriffskontrollen und eine kontinuierliche Überwachung der Netzwerkaktivitäten. Die Implementierung von Zero Trust erfordert einen umfassenden Ansatz, der verschiedene Aspekte der Cybersicherheit umfasst, darunter Benutzerauthentifizierung, Endpunktsicherheit und Zugriff mit geringsten Rechten.

Einer der Hauptvorteile von Zero Trust besteht darin, dass die Risiken, die von Insider-Bedrohungen und der seitlichen Bewegung von Angreifern innerhalb eines Netzwerks ausgehen, wirksam eingedämmt werden. Der Übergang zu einem Zero-Trust-Framework im Jahr 2024 stellt einen Paradigmenwechsel in der Cybersicherheit dar, der sich auf eine kontinuierliche Überprüfung und minimale Zugriffsrechte konzentriert, um Schwachstellen zu reduzieren und die Netzwerksicherheit insgesamt zu verbessern.

Trend 8:
Qualifikationsdefizit in der Cybersicherheit & Bildung

Im Jahr 2024 hat die Cybersicherheitsbranche weiterhin mit einer großen Herausforderung zu kämpfen: dem Qualifikationsdefizit. Da Cyber-Bedrohungen immer raffinierter werden, steigt die Nachfrage nach qualifizierten Cyber-Sicherheitsexperten. Es besteht jedoch ein deutlicher Mangel an Personen, die über die notwendigen Fähigkeiten und Kenntnisse verfügen, um diese sich entwickelnden Bedrohungen wirksam zu bekämpfen.

Diese Lücke stellt nicht nur ein Risiko für einzelne Unternehmen dar, sondern auch für die globale Cyber-Infrastruktur. Umso wichtiger ist es, mit Dienstleistern zusammen zu arbeiten, die sowohl das Knowhow als auch proaktive unabhängige Cybersecurity-Tools wie die **DEFENDERBOX** zur Verfügung stellen.

Trend 9:
Industrial Cybersecurity für Produktionsanlagen

Noch bis vor wenigen Jahren war Cybersicherheit für Produktionsanlagen eher ein Randthema. Die Bedrohungen schienen zu abstrakt und theoretisch zu sein, so dass sich Hersteller damit beschäftigten. Dies änderte sich schlagartig, als mehrere Cyberangriffe bekannt wurden und dass nun auch Automatisierungssysteme und Produktionsanlagen im Fokus von Bedrohungen stehen und diesen real ausgesetzt sind, womit in letzter Konsequenz auch hohe Verluste verbunden sein können. Zudem sind Produktionsanlagen zunehmend vernetzt (MDA) und entsprechend angreifbar.

Allerdings scannen bzw. pentesten proaktive Sicherheits-Tools wie die **DEFENDERBOX** alle erfassbaren Devices in einer IT-Infrastruktur, so auch Produktionsanlagen, um etwaige Sicherheitslücken und Schwachstellen zu identifizieren.

Trend 10:
Cybersecurity-Insurance wird zum Mainstream

Eine Cybersecurity-Versicherung wird zum festen Bestandteil der Risikomanagementstrategien von Unternehmen. Da Cyber-Bedrohungen immer komplexer und häufiger werden, greifen Unternehmen zunehmend auf Cyber-Sicherheitsversicherungen zurück, um finanzielle Risiken im Zusammenhang mit Datenschutzverletzungen und Cyber-Angriffen zu mindern. Die Kosten für diese Versicherung werden jedoch maßgeblich von der Cybersicherheitslage des Unternehmens beeinflusst.

Der Einsatz etablierter Cybersicherheitslösungen wie der **DEFENDERBOX** kann sich direkt auf die Senkung der Kosten für Cybersicherheitsversicherungen auswirken. Die Identifizierung von Schwachstellen und Sicherheitslücken und die entsprechende Behebung verbessern den Schutz eines Unternehmens vor Cyberbedrohungen.