Lions Club
Bad Homburg – Weißer Turm

Jasper Köcke
Sekretär 2018/2023

448. Protokoll

Clubtreffen

07. 02. 2023

Clublokal „Kronenhof“
Zeppelinstrasse
Bad Homburg v. d. H.

<u>Teilnehmer</u> : (persönlich anwesend: 19, sowie digital zugeschaltet: 2. Als Gäste: zwei unserer Damen, sowie Joachim Steurer und Volker Fietze)

Bonk, Bopp, Braunberger, Foeller, Geduldig, Gümmer, Kaffka,, Kaiser, Klöpper, Köcke, Maier, Schaefers, C. Schulz, H. Schulz, Schweighöfer, Schweizer, Simon, Slusny, Warneke, Zühlke,

Präsident Frank Slusny begrüsst alle Anwesenden herzlich zu seinem eigenen Vortrag über Cybersicherheit sowie auch Aspekte seiner Arbeit im Unternehmen „Palo Alto“.

Zu den weiteren Tagesordnungspunkten zählten persönliche Vorstellungen unserer Gäste Herren Fietze und Steurer. Diese erfolgten vor dem Vortrag von Frank.

Aufgrund des ausführlichen darauf folgenden Vortrags unseres Präsidenten, der daran anschliessenden angeregten Diskussion unter den Mitgliedern, sowie der Vorstellung der beiden Herren war bald unser Zeitlimit erreicht. Weitere TOPs, wie z.B. die Nutzung der LionsApp (vorgestellt durch unseren LF Carsten Schulz) und eine Aktualisierung der in den vergangenen Clubjahren erstellten Listen wurden daher auf ein kommendes Clubtreffen verschoben.

<u>TOP 1:</u> Cyberattacken und Cybersicherheit

Vortrag von Frank Slusny über komplexe Dienstleistungen im Bereich der Cybersicherheit, sowie auch unterschiedliche Arten von Cyberattacken. Aufgrund seiner Funktion als „Director Strategic/Global Accounts Germany" bei Palo Alto Networks, einem der weltweit grössten IT-Sicherheitsdienstleister, konnte Frank uns zu diesem komplexen Thema viele interessante Sachverhalte und Neuigkeiten erläutern.

Palo Alto Networks, Inc. ist ein amerikanisches multinationales IT-Sicherheitsunternehmen mit Hauptsitz in Santa Clara, Kalifornien. Seine Kernprodukte sind eine Plattform, die Firewalls und Cloud-basierte Angebote umfasst, die diese Firewalls um weitere Sicherheitsaspekte erweitern.

Als einer der weltweit führenden Anbieter von Cybersicherheitslösungen ist Palo Alto Networks dafür bekannt, jeweilige aktuelle Sicherheitsgrade stets zu hinterfragen. Im Mittelpunkt seiner Entwicklungen steht der erfolgreiche Schutz seiner Kunden vor Cyberattacken im digitalen Zeitalter. Auf diese Sicherheitslösungen vertrauen Zehntausende Unternehmen und deren Kunden. Palo Altos wegweisende Security Operating Plattform schützt Unternehmen dank kontinuierlicher Innovationen bei der digitalen Transformation. Sie vereint die neuesten bahnbrechenden Erkenntnisse hinsichtlich Sicherheit, Automatisierung und Analyse. Durch Bereitstellung einer echten Plattform und der Förderung eines wachsenden Netzwerks aus Pionieren - wie etwa Palo Alto - profitieren Unternehmen von hoch effizienten und innovativen Cybersicherheitslösungen für Clouds, Netzwerke und Mobilgeräte.

Frank skizziert in seinem Vortrag eine vielfältige, komplexe Welt von Cyberbedrohungen, welche nicht nur branchenspezifische Angriffe enthält, sondern sich ihrerseits auch in einzelne „Branchen" und vielfältige Vorgehensweisen aufgespalten hat. So gibt es beispielsweise für spezifische Cyberangriffe kalkulierte Schadensbereiche, für deren Behebung auf dem Erpressungsweg unterschiedlich hohe Lösegeldsummen verlangt werden, wobei es teilweise sogar zu „Rabattangeboten" einzelner Angreifer kommen kann – was teilweise sodann unter den Angreifern selbst wiederum zu einem Über- oder Unterbietungswettbewerb führt. Mit anderen Worten, so Frank, hat sich in der Cyberkriminalität eine regelrechte „Industrie" entwickelt. Diese treibt umso mehr unterschiedliche Blüten, als ständig neue, oftmals hochsensible Datenbereiche (etwa aus der Vielfalt kritischer Infrastruktur u.a.) kontinuierlich entstehen und sich weiterentwickeln. Im Umkehrschluss zeigt dieses Szenario auch den riesigen Geschäftsbereich eines Dienstleisters wie Palo Alto Networks!

Die angeregte Diskussion während und nach Franks Vortrag unter den Mitgliedern berührte auch Themen wie die zunehmende Bedeutung von KI, und hier wiederum Aspekte und Entwicklungen wie „deep learning", fake-news, oder auch den sich intensivierenden Wettbewerb zwischen KI und HI (Humanintelligenz).

Im Anhang zum vorliegenden Protokoll noch die Zusammenfassung seines Vortrags von Frank selbst:

Thema des Vortrags: „Cyber-Attacken, Top-Risiko für Unternehmen und Gesellschaft“

Der Vortrag begann mit einer Studie der „Allianz Global Corporate Specialities“ Versicherung über die größten Geschäftsrisiken. In der Studie Allianz Risk Barometer wurden 2.712 Risikomanagement-Experten aus 94 Länder befragt. Die größte Gefahr stellen demnach Cybervorfälle dar, dh. Cyber-Kriminalität die zu Systemausfällen, Datenschutzverletzungen und Geldstrafen führen, gleichauf mit Betriebsunterbrechungen, z.B. durch Lieferkettenverletzungen. Erst danach folgen Naturkatastrophen, Pandemie und rechtliche Veränderungen, z.B. Handelskriege.

In Deutschland schlägt sich dies zum Beispiel darin nieder, dass 67% der befragten Unternehmen laut einer Umfrage der Firma Sophos bereits Ziel von Schadsoftware-Angriffen wurden, vorwiegend mit Phishing Emails. Die Kosten belaufen sich im Durchschnitt auf 273.000 USD pro Vorfall. Zudem kommen oft Wiederherstellungskosten, die im Durchschnitt ca. 1,7M USD betragen.

Trends, die zu einer immer höheren Anfälligkeit führen, sind:

Nutzung von mehr und mehr externen IT Dienstleistungen und Cloud Services;

Wandel der Arbeitswelt durch Home Office und mobiles Arbeiten von unterwegs;

leistungsfähigere Technologien und Künstliche Intelligenz

Noch ein paar Daten: 96% der Unternehmen wurden in den letzten 12 Monaten attackiert, davon 54% öfters als dreimal. 33% erlitten durch die Attacken Betriebsunterbrechungen.

Der Schaden, der allein im Jahr 2021 weltweit durch Cybercrime angerichtet wurde, beträgt 6.000 Mrd. USD, was einem drittgrößten Wirtschaftsvolumen nach USA und China entspricht. Das durchschnittliche Wachstum beträgt 15% im Jahr. Die Milliarden, die Drogenkartelle machen, sind bescheiden im Vergleich zu den Einkünften von Cyberkriminellen.

Cyberkriminalität nutzt ebenso die vorhandenen neuen technologischen Mittel. Zudem hat eine starke Kommerzialisierung der Kriminalität stattgefunden. Es gibt neue Geschäftsmodelle, die Know-how und Schadsoftware vermietet, z.T. erfolgsabhängig verrechnet und komplexe Lieferketten, die eine hohe Industrialisierung dieses Sektors Zeugnis geben. Dabei unterstützen autokratische Nationen auf staatlicher Ebene kriminelle Cybercrime-Gruppen und profitieren sehr stark. Allein Nordkorea nimmt mehr als 1,3 Mrd. USD jährlich durch Cybercrime ein und importiert Devisen über Bitcoin-Transaktionen und andere Cyberwährungen.

Es gibt verschiedene Ausprägungen von Cyberkriminalität, dazu gehören Erpressung durch Erpressungs-Software (Ransomware), Diebstahl von Daten, Rufschädigung und Betriebsunterbrechungen durch direkte elektronische Angriffe (Denial of Services), Zerstören von Computern und daten (Wipe).

Einfallstore sind neben Phishing Emails, die Benutzer versteckt auffordern Schadsoftware auszuführen, oft Schwachstellen in Computerprogrammen. Regelmäßige Veröffentlichungen der Software-Hersteller wie Microsoft, Apple etc. fordern Benutzer auf, diese Schwachstellen durch eine Aktualisierung der

Software zu beseitigen. Mittlerweile sieht man Kriminelle innerhalb von weniger als 15 Minuten nach Veröffentlichung solcher Schwachstellen, solche über das Internet global maschinell zu erfassen, um festzustellen, wer noch alte Software nutzt um sie ebenso schnell anzugreifen.

Oft lassen sich die Angreifer Zeit um sich nach und nach in den Zielumgebungen auszubreiten, verwischen ihre Spuren in Dateien und Einträgen, legen sich für längere Zeit schlafen, um dann zu gegebener Zeit aktiv zu werden. Komplexe Angriffe erfordern das Know-how und die Logistik von Teams mit hunderten von Programmieren.

Auch militärische Konflikte begünstigen Cyberkriminalität. Hacker-Gruppen schließen sich je nach Herkunft und Orientierung verschiedene Blöcke an. Zuletzt wurde das sehr gut im Ukraine Konflikt gesehen und dokumentiert. Daraus entstehen wiederneue Bedrohungen für Firmen, die in diesen Ländern operieren oder sich zurück ziehen.

Es gibt allerdings auch bewährte Verhaltensweisen und eine Vielzahl von Vorgehensweisen und Anbietern, die sehr wohl Schutz bieten. Der Vortragende arbeitet beim Weltmarktführer für Cyber Security, Palo Alto Networks. Es ist inzwischen eine bedeutende Landschaft von IT Firmen in diesem Bereich entstanden, mit weit überdurchschnittlichen Wachstum und guten Karriereaussichten, immer auf der Suche nach neuen Talenten, die sich der guten Seite verschreiben.

Ende unseres Clubtreffens: 21:30 Uhr