Bericht: Vodafone und die Firma KSV Fuchs

Hintergrund: Die Firma KSV Fuchs hat seit Jahren einen Internetvertrag mit Vodafone, der eine statische IP-Adresse beinhaltet. Trotz mehrfacher Anrufe und Bitten um Änderung auf eine dynamische IP hat sich die Situation nicht verbessert.

Probleme:

1. **Unveränderte Statische IP-Adresse:** Trotz wiederholter Anfragen durch KSV Fuchs an den Kundenservice von Vodafone, bleibt die zugewiesene IP-Adresse statisch. Dies bedeutet, dass die Firma stets dieselbe IP-Adresse verwendet, was sie möglicherweise anfälliger für sicherheitsrelevante Angriffe macht und auch nicht den aktuellen Anforderungen der Firma entspricht.
2. **Eingestellte Sicherheitspakete für Business-Kunden:** Vodafone hat die Sicherheitsdienstleistungen, die speziell für Business-Kunden angeboten wurden, eingestellt. Diese Pakete umfassten Maßnahmen zum Schutz der IP-Adresse und boten einen zusätzlichen Sicherheitspuffer. Da diese Dienstleistungen nicht mehr verfügbar sind, ist KSV Fuchs gezwungen, nach alternativen Sicherheitslösungen zu suchen, um ihre Netzwerkinfrastruktur zu schützen.
3. **Vertragsänderungen ohne Lösung des IP-Problems:** Um die Problematik anzugehen, wurde KSV Fuchs ein neuer Vertrag von Vodafone angeboten, der eine neue FritzBox beinhaltete. Trotz der Besprechung, dass eine dynamische IP-Adresse erwünscht sei, blieb die IP-Adresse weiterhin statisch. Dies zeigt auf, dass die Änderung der Hardware nicht zur Lösung des IP-Problems beigetragen hat und die gewünschten Anpassungen in den Verträgen nicht korrekt umgesetzt wurden.

Pascal Gliewe • IT-System-Engineer

NetFactory
Team Systemhaus
Tel: 0721-93 33 0-33 Mail: systemhaus@net-factory.de
Fax: 0721-93 33 0-88 Web: www.net-factory.de

Net Factory Gesellschaft für Netzwerklösungen mbH
Häfenweg 16
76287 Rheinstetten
www.net-factory.de

Bericht II

Berichterstattung KSV-Fuchs

Am 29. April 2024 wurde die Firma KSV-Fuchs erneut von einem Cyberangriff getroffen. Vor Ort wurden alle Geräte und Dateien überprüft, um herauszufinden, woher der Angriff kam und ob der Angreifer noch aktiv war. Es bestand der Verdacht auf einen Wurm, der die Systeme befallen hatte. Betroffen waren zwei Computer, private Handys und ein externer Webserver.

Es gab Hinweise auf Brute-Force-Angriffe (bei denen viele Passwörter ausprobiert werden) und eine Software, die immer wieder bestimmte Programme ausführte. Frau Adam zeigte ein schädliches PHP-Skript, das in die WordPress-Datenbanken eindrang und dort Änderungen vornahm. Alle Informationen wurden gesammelt und notiert.

Zurück in der Firma wurde der NetCup-Support kontaktiert, weil ein Server für die Angriffe genutzt wurde. Auch der Account von Herrn Fuchs war betroffen und konnte nicht mehr erreicht werden. NetCup weigerte sich, den Account zu sperren, weil noch Guthaben darauf war. Nach Rücksprache werden nun neue Login-Daten per Post verschickt, damit das Geld überwiesen und der Account gelöscht werden kann.

Während der Wartezeit wurden alle Screenshots, Mails und Berichte, die Frau Adam und Herr Fuchs gegeben hatten, überprüft. Eine IT-Firma hatte eine Software programmiert, die sensible Daten enthielt und auf GitHub hochgeladen wurde. Diese Firma lieferte die Software nie aus, verlangte aber trotzdem Geld, das Herr Fuchs bezahlte. Danach begannen die Angriffe.

Die Angriffe umfassten die Übernahme vieler Accounts, wiederholte Angriffe auf die Webseite und Datenbank, Infektionen der Computer und Handys sowie möglicherweise den Diebstahl sensibler Daten. Die Firma KSV-Fuchs war dadurch stark eingeschränkt.

Beim zweiten Besuch wurde die komplette Hardware vor Ort zurückgesetzt und neu eingerichtet. Auf der UDM Pro wurde die Firewall verschärft eingestellt, sowie ein Threat- und Incident-Managementsystem aktiviert. Zusätzlich wurde auf allen PCs Sophos Intercept X installiert, um sie vor weiteren Angriffen sowie Schadsoftware zu schützen. Die Webseite sowie Domain wurde gründlich untersucht, bereinigt und danach zur Net Factory umgezogen (Webhosting), sodass eine bessere Einsicht auf Angriffe möglich ist. Außerdem wurden YubiKeys als 2FA/MFA-Methode bei unterschiedlichen Accounts eingesetzt, da diese einen höheren Schutz bieten.

Nach Überprüfung der externen Festplatten und USB-Sticks stellte sich heraus, dass sie mit Trojanern und Stealern (Schadsoftware) infiziert waren. Nachdem diese bereinigt wurden, wurden alle PCs erneut formatiert und neu eingerichtet. Der Vodafone Vertrag wurde gekündigt, weil Vodafone es nicht schaffte, aus der Statischen Öffentlichen IP

eine Dynamische zu erstellen. Zusätzlich konnte man die Vodafone Hotspots nicht deaktivieren (selbst Vodafone nicht), was mir auch zu bedenken gab, ob da nicht auch was konfiguriert wurde, was den Hackern eine Angriffsfläche bietet. Um dann das ganze Vodafone Problem zu lösen, wurde ein neuer Vertrag mit der Telekom vereinbart und dieser auch umgesetzt. Außerdem wurden VLANs eingerichtet, um die Kommunikation zwischen verschiedenen PCs zu verhindern.

Es konnte nicht genau festgestellt werden, woher die Angriffe kamen, aber das Business konnte wiederhergestellt werden, sodass Frau Adam und Herr Fuchs normal arbeiten können. Einige Probleme, wie der Zugang zu bestimmten Accounts, sind noch offen, aber nicht von hoher Priorität.

Pascal Gliewe • IT-System-Engineer • 08.10.2024

NetFactory
Team Systemhaus
Tel: 0721-93 33 0-33 Mail: systemhaus@net-factory.de
Fax: 0721-93 33 0-88 Web: www.net-factory.de

Net Factory Gesellschaft für Netzwerklösungen mbH
Häfenweg 16
76287 Rheinstetten
www.net-factory.de