Expert Notes

Informieren. Aufklären. Sensibilisieren.

18. Mai 2020 Ausgabe **5.**

Expert Notes. Der regelmässig erscheinende Fachbericht der Neo One zu aktuellen Themen.

Eine Publikation der Neo One.

Digital

Videokonferenzen, Streaming-/ Messenger-Dienste. Optimales Hilfsmittel oder grosse Gefahr?

Flexibel zu sein, ist seit jeher einer der Schweizer Tugenden. Flexibilität und schnelles Umdenken war und ist in Krisenzeiten immer gefordert. Wo verbergen sich aber die Gefahren von flexiblem Handeln?

Ein grosser Teil der Wirtschaft und damit verbunden ein beachtlicher Teil der arbeitenden Bevölkerung, hat in den letzten Monaten auf Home Office Betrieb umgestellt. Erste Forschungen wollen gar die aus der Krisennot geborene, neue Art zu arbeiten, als den Zukunftsstandard schlecht hin erkoren haben. Dieser soll den Ruf haben, vermeintlich bessere Work-/ Life-Balance, einfachere Kombinationslösungen für Familie/Beruf und noch mehr Flexibilität zu bieten.

Aktuell nutzen viele Unternehmen Tools und Dienste von verschiedenen Anbietern wie Zoom, Google Hangouts oder Teams von Microsoft für Videokonferenzen oder als Streaming-Dienste. Der Aufbau dieser Dienste musste umgehend geschehen, was das Abwägen von Sicherheit vernachlässigte. Zu wenig wurde geprüft, wie sicher solche Streaming-Dienste überhaupt sind. Anstatt in der Krise richtig zielführend agiert zu haben, finden sich nun viele Unternehmensleitungen mit Fragen konfrontiert, welche zu Beginn hätten geprüft werden müssen.

Die Sicherheit spielte entsprechend eine zu wenig gewichtete Rolle, denn es zählten ja vermeintlich wichtigere Faktoren wie Geschwindigkeit und Flexibilität. In den nachstehenden Artikeln wollen wir darauf näher eingehen.

Jan Braunschweiler
Inhaber & Geschäftsführer

IT

WhatsApp, Signal und Threema – Wissen wir was wir da nutzen?

Die Auswahl an Anbietern für Videokonferenzen oder auch Messenger ist vielfältig. Welcher Dienst in der Regel genutzt wird, hängt meistens auch davon ab, ob die eigenen Kontakte, das Businessumfeld, auch das jeweilige Programm nutzen, denn sonst kann man sich darüber nicht erreichen und der ursprüngliche Nutzen verliert seinen Zweck. Gleichzeitig gibt es eine Reihe von Funktionen- und Securityaspekte, die beleuchtet werden müssen.

WhatsApp ist heute nach wie vor der am meisten eingesetzte Messenger-Dienst. Sicherheits- und Datenschutzbedenken haben dazu geführt, dass beispielsweise die EU-Kommission ihren Mitarbeitenden empfahl, den Dienst Signal anstelle von WhatsApp einzusetzen. Die israelische Sicherheitsfirma NSO Group hat ein Programm entwickelt, welches selbst in den WhatsApp-Account von Amazon-Chef Jeff Bezos eindrang.

Im Gegensatz zu WhatsApp ist die Signal-App nicht wie WhatsApp eine kommerzielle Entwicklung eines Kommunikationskonzerns, sondern von Datenschutzaktivisten und Cyber-Sicherheitsexperten entwickelt worden. Daher steht der Programmcode von Signal als Open-Source-Software online, sodass ständig weiterentwickelt und verbessert werden kann. Ausserdem setzt Signal seit mehr als einem Jahr auf das Prinzip des versteckten Senders («sealed sender»), bei dem auch die sogenannten Metadaten einer Nachricht, also das Wer? Wann? An wen? geschützt werden sollen. Dazu speichert Signal, nach eigenen Angaben, auch keine IP-Adresse eines Absenders. Ähnlich geht auch die Threema-App vor. Auch sie verschlüsselt Ende-zu-Ende und verzichtet auf Metadaten. Das geht bei Threema so weit, dass Nutzer kein Profil mit hinterlegter Email oder Telefonnummer einrichten müssen, sondern eine anonyme ID zugewiesen bekommen. Dafür ist der Threema-Programmcode im Vergleich zu Signal nicht vollständig quelloffen. Threema an sich ist aber eine 100% Swiss-Made Software und DSGVO-konform. Ebenfalls gibt es von Threema eine Business Version (Threema Work), welche Unternehmen die Möglichkeit bietet, selbst vertrauliche Daten «intern» zu halten.

NEO ONE
Rundum. IT bis Digitalmarketing.

Neo One AG
Grindelstrasse 6
8303 Bassersdorf

+41 43 233 30 30
hello@neo-one.ch
www.neo-one.ch

© created and designed by Neo One

Viber, ICQ und Zoom – Super Nutzen oder super bedenklich?

Gefährlich bezüglich Sicherheit sind oft auch kostenlose Kommunikations-Apps wie Viber. Bei Viber mussten die Nutzer jahrelang zustimmen, dass Viber persönliche Daten des Geräts wie Adressbuch und andere erhalten und auch die Nutzungsberichte an Dritte übermitteln darf. Ähnliches gilt auch für die Applikation ICQ (ICQnew), die zum russischen Mail.ru gehört. Edward Snowden reihte diese bereits im Jahr 2013 in Produkte ein, welche die Nutzerdaten auch an Geheimdienste weitergaben. ICQ und Mail.ru bestreiten dies aber.

Ebenfalls grosse Sicherheitsbedenken sind auch beim stark in der Corona-Zeit verbreiteten Zoom vorhanden. Alle brauchten in der Corona-Krise eine stabile und leicht zu bedienende App für Videokonferenzen. Zoom deckt diese Bedürfnisse optimal ab. Inzwischen zeigt sich, dass Zoom gravierende Sicherheitslücken hat und zwar so weit, dass beispielsweise Teilnehmende in private Videokonferenzen platzten. Das FBI gab offiziell einen Spionagegefahr-Alarm für Zoom heraus, als bekannt wurde, dass die Verschlüsselungscodes über Server in China gingen. Unter anderem hat auch der Tech-Gigant Google seine Mitarbeitenden offiziell dazu angehalten, Zoom nicht auf Arbeits-PCs zu installieren – dies aus Sicherheitsgründen. In der Zwischenzeit hat Zoom nachgebessert, wie erfolgreich wird sich jedoch zeigen.

Viele Anbieter, aber was eignet sich für meinen Betrieb?

Auch bei Videokonferenz- oder Messenger-Lösungen gibt es wohl keine Lösung, die eine 100 %-Sicherheit gewährleistet. Hingegen zeigt sich auch hier, dass eine aufeinander abgestimmte Lösung mit einer gesamtheitlichen Sicht für den Betrieb höhere Sicherheit bringt als Insellösungen. Aber natürlich bringen die grösste Sicherheit und die strengsten Datenschutzrichtlinien nichts, wenn das Produkt wenige Nutzer hat, teuer und nicht anwenderfreundlich ist sowie im Betrieb Probleme bereitet.

In der ganzen Fülle von Videokonferenz-Systemen und Messenger-Diensten wird oft vergessen, dass ja heute bereits viele Betriebe mit Office arbeiten. Sofern ein Betrieb bereits Office 365 einsetzt, welches in der Schweiz gehostet ist, resp. bei der Einrichtung in der Schweiz gehostet werden kann, kann damit auch schnell, einfach und sicher Videokonferenzen mittels Teams von Microsoft nutzen. Ebenfalls oft vergessen wird, dass viele Betriebe heute mit einer Voice Over IP-Telefonie arbeiten und besonders auch Swisscom oder andere Anbieter in diesem Bereich, Möglichkeiten für Videokonferenzen oder auch Chats bieten. Meist ist dies der sicherste und einfachste Weg für einen Betrieb, sofern die entsprechenden Kundenbedürfnisse damit abgedeckt werden können.

Problemstellung

Videokonferenzlösungen und Messenger-Dienste können auch gehackt werden bzw. andere können evtl. mithören, lesen und sehen.

***Neo One** vereinfacht Ihre IT, vernetzt Informatik mit Digitallösungen und steigert die Systemstabilität*

N- Tipp

- Abgestimmte Lösungen für den geschäftlichen Bereich nutzen
- Sich beraten lassen, welche Lösung über einen hohen Sicherheitsstandard verfügt und die Anforderungen des Betriebes optimal erfüllen kann
- Überprüfung, ob beim Telefonie-Anbieter ebenfalls Videokonferenzlösungen und Chats möglich sind (Vereinfachung und Sicherheitsaspekte)
- Auch Videokonferenz- und Chat-Lösungen sollten regelmässig überprüft und gewartet werden

Ronny Troxler
ICT Consultant & Senior
ICT System Engineer

Digital

Webhost-Dienstleister wurden Zielscheibe von Phishing-Kampagnen

Kürzlich wurden Kunden von verschiedenen Webhosting-Dienstleistern (Bsp. Infomaniak, Hostpoint usw.) Zielscheibe einer Phishing-Kampagne. In Mails, die scheinbar von diesen Firmen versendet wurden, wurde von Ihnen verlangt, sich anzumelden oder Ihre Produkte über Websites zu verlängern, die unberechtigterweise die Identität von diesen Firmen (Infomaniak, Hospoint usw.) verwendeten.

© created and designed by Neo One

Die meisten Webhosting-Dienstleister informierten Ihre Kunden in der Folge, dass diese die Adresse der Seite genau prüfen sollen, bei der sie sich anmelden, damit sichergestellt ist, dass diese ausschliesslich ihrer Domain zuzuordnen ist. Hierzu wurden die Kunden auch darauf aufmerksam gemacht, dass wenn ihnen die Adresse verdächtig erscheint oder sie ihr Browser auf ein Risiko hinweist, den Anmeldevorgang sofort abzubrechen.

Mehrere Webhosting-Firmen informierten auch sofort über Ihre Massnahmen, welche Sie aufgrund des Vorfalles vorgenommen haben. Unter anderem waren dies:

- Kontaktaufnahme mit verschiedenen Hosting-Providern und Registrierstellen, die diese betrügerischen Sites hosten, um eine Sperrung zu erreichen
- Aktualisierung ihrer Anti-Spam-Filter, damit jegliche neuen Versionen dieser Mails abgefangen werden, bevor sie auf die Kunden zugehen
- Modifizierung ihrer E-Mail-Infrastruktur, um zusätzliche Sicherheitsbarrieren für den Schutz vor Identitätsdiebstahl einzurichten
- Unterrichtung ihrer Kunden über ihre Website, auf sozialen Netzwerken sowie die verschiedenen Kontaktschnittstellen
- Erstattung einer Anzeige bei der Polizei, um eine Ermittlung durch Interpol einzuleiten

Die Webhosting-Firmen sind nun aufgrund dieses Vorfalles wachsamer und achten nun mit Nachdruck darauf, dass in allen Bereichen die nötigen Sicherheitsmassnahmen und Aktualisierungen vollzogen werden.

Problemstellung

Kriminelle verwenden unberechtigterweise die Identität einer Firma und verschaffen sich Anmeldedaten, um sich bei dieser Firma einloggen zu können.

N- Tipp

- Überprüfen Sie die Adresse der Webseite, auf der Sie sich befinden, bevor Sie Ihren Benutzernamen oder die Zahlungsinformationen eingeben
- Wenn die Adresse verdächtig erscheint oder der Browser auf ein Risiko hinweist, brechen Sie den Anmeldevorgang immer sofort ab
- Informieren Sie sofort eine Fachperson über einen allfälligen Vorfall
- Arbeiten Sie immer mit einer Zwei-Faktor-Authentifizierung, da sich Dritte auch dann nicht anmelden können, wenn Sie Ihr Passwort besitzen
- Halten Sie Ihre Informatiklösungen stets aktuell und führen Sie regelmässige Wartungen Ihrer Systeme durch

Fabian Müller
Leiter Operations & Digital

IT

Firmware-Updates machen, nicht machen, wieso überhaupt?

Wir alle haben das Wort Firmware im einen oder anderen Zusammenhang schon gehört. Firmware gibt es auf Drucker, NAS, Handy, Switches und vielen, anderen Geräten. Firmware-Updates sollten wie Sicherheits-Updates ebenfalls regelmässig gemacht werden. Mit Firmware-Updates erhalten auch alte Geräte neue Funktionen und werden immer besser. Das beste Beispiel für Firmware-Updates ist der US-Autohersteller TESLA. Die TESLA Fahrzeuge erhalten in regelmässigen Abständen Firmware-Updates (in diesem Zusammenhang ist jedoch von Software-Updates die Rede) und damit werden die Autos, trotz des Alters, immer moderner und überraschen die Anwender mit neuen Funktionen. Auch bei Drucker oder Handy verhält es sich gleich. Regelmässige Updates schützen das Gerät vor Attacken und bringen neue Funktionen. Eine Firmware kann jeweils nur durch den Hersteller verändert werden.

Problemstellung

Natürlich kann so ein Firmware-Update auch immer mal schief gehen. Dann ist man auf den Hersteller Support angewiesen und muss schauen, wie man die alte Firmware wieder zum Laufen bringt. In ganz seltenen Fällen funktioniert dies gar nicht mehr und das entsprechende Gerät muss durch den Händler mit einer neuen Firmware bespielt werden.

N- Tipp

- Firmware-Updates regelmässig einspielen, damit die Funktion des Geräts gewährleistet ist

Remo Emmenegger
Junior ICT System Engineer

© created and designed by Neo One

Sich im Kleinen mit Informatik zu befassen, heisst immer mehr, von unserer digitalen Welt zu verstehen. Machen Sie den ersten kleinen Schritt.

Nice to know

Monitoring

– Fernüberwachung von Vorgängen des Systems.

NAS – Network Attached Storage

– Dateiserver eingebunden im Netzwerk zur zusätzlichen Absicherung der Daten im geschäftlichen Bereich.

Landingpages

– Landingpages ist eine speziell eingerichtete Webseite, die nach einem Mausklick auf ein Werbemittel oder nach einem Klick auf einen Eintrag in einer Suchmaschine erscheint. Im Online-Marketing werden Landingpages daher als Mittel zur Suchmaschinenoptimierung (SEO) eingesetzt.

Metadaten

– Metadaten sind strukturierte Daten, die Informationen über Merkmale anderer Daten enthalten. Metadaten beschreiben also die eigentlichen Daten auf eine Art und Weise. Metadaten wären bei einem Buch zum Beispiel Autor, Titel, Erscheinungsjahr, ISB Nummer etc.

Firmware

– Technische Geräte wie etwa Smartphones benötigen für den ordnungsgemässen Betrieb eine Firmware. Die Firmware kann quasi als grundlegende Betriebssoftware angesehen werden.

N-Coach.
Mieten und profitieren.

Mieten Sie Ihren N-Coach und profitieren Sie operativ wie auch strategisch für Ihr Unternehmen. Die einfachen Fragen im täglichen Businessumfeld sind unterschiedlich und individuell, ganz genau wie die Firmen, Anwender und Mitarbeitenden selbst.
Die wirtschaftlichen Tätigkeiten werden komplexer und bedürfen immer vertiefterem und interdisziplinärerem Fachwissen. Deshalb gibt es den N-Coach. Der N-Coach begleitet für ein paar Stunden und hilft bei der einen speziellen Pendenz oder auch über eine längere Zeit während einem grösseren Projekt. Der N-Coach liefert wichtige Erfahrungswerte und überprüft strategische Konzepte oder gestaltet diese auf Wunsch mit.

***Neo One** vereinfacht Ihre IT, vernetzt Informatik mit Digitallösungen und steigert die Systemstabilität.*

***Neo One** legt die Basis, damit Ihre Kunden Ihre Botschaften sowohl gedruckt als auch digital verstehen.*

***Neo One** optimiert Ihre Strategie und stimmt alle Digitalmarketingmassnahmen mit unseren interdisziplinären Fachleuten aufeinander ab.*

***Neo One** gestaltet Lösungen, die mit allen IT-, Software und Drucksystemen kompatibel sind.*

NEONE
Rundum. IT bis Digitalmarketing.

Neo One AG
Grindelstrasse 6
8303 Bassersdorf

+41 43 233 30 30
hello@neo-one.ch
www.neo-one.ch

© created and designed by Neo One