Expert Notes

Informieren. Aufklären. Sensibilisieren.

21. April 2020 Ausgabe **3.**

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

Eine Publikation der Neo One.

IT

Trügerisch echt.

Erneut findet eine neue und leider sehr vertrauenswürdig aufgebaute «Betrüger-Masche» statt, welche den Unternehmen stark schaden könnte. Betrüger versuchen sich als Webhosting-Partner der Firma auszugeben und weisen darauf hin, dass man vermeintlich mehrfach wegen dem neuen EU-Datenschutzgesetz DSGVO aufgefordert wurde, schriftlich Informationen einzureichen und dies nicht gemacht habe.

Die Aufmachung zeigt sich leider sehr vertrauenswürdig und es wird mit der Schliessung des Accounts und somit der Deaktivierung des Webseitenbetriebs gedroht. Man könne jedoch ohne grossen Aufwand einfach kurz auf den Link klicken, um alles zu verifizieren und so nicht mehr betroffen zu sein und den Schaden abzuwenden.

Problemstellung

Klickt der Kunde/User auf den Link, gibt er sich in die grosse Gefahr, mittels «Phishing/Datenklau» Opfer von Datendiebstahl, Trojanern oder anderen Virenattacken zu werden.

N- Tipp

- Zeigen Sie solche E-Mails mittels eines Fotos umgehend einer Fachperson
- Leiten Sie solche E-Mails nicht weiter
- Löschen Sie solche E-Mails umgehend, ohne Inhalte anzuklicken
- Sollten diese E-Mails nicht in Ihrem Spamordner gelangt sein, so gilt es, Ihre Security-Systeme dringend zu optimieren
- Sorgen Sie für abgestimmte Sicherheitskonzepte zwischen Ihren Informatiklösungen und dem Betrieb Ihrer Web- und Digitallösungen

Michel Hipp
Leitung ICT / Senior ICT System Engineer

IT

Stetiger und aggressiver denn je.

Gemäss den jüngsten Informationen, welche der Melde- und Analysestelle Informationssicherung MELANI vorliegen, werden Viren/Trojaner wie «Emotet» momentan auch aktiv dazu verwendet, um gezielt Computer und Server in Unternehmensnetzwerken mit einem Verschlüsselungstrojaner (Ransomware) namens «Ryuk» zu infizieren. Dabei verschlüsselt «Ryuk» auf dem Computer oder Server abgelegte Dateien und fordert nach erfolgter Verschlüsselung vom betroffenen Unternehmen eine erhebliche Summe an Lösegeld (CHF 200'000 und mehr). Betroffen sind ausschliesslich Geräte wie Computer und Server, welche mit einem Windows Betriebssystem laufen. Durch die vorhandene Wurm-Komponente besteht bei einer erfolgreichen Infektion ein hohes Risiko, dass sich der Trojaner im Unternehmensnetzwerk weiterverbreitet und einen erheblichen Schaden anrichtet.

Quelle: https://www.melani.admin.ch/

Problemstellung

Unser «way of life», sei es privat oder geschäftlich, führt uns punktuell oder ganz häufig und immer wieder dazu, «24/7» online zu sein. Geschäftstätigkeiten und private Nutzung der Digitalisierung bedingen mehr denn je hohe Sicherheitsanforderungen. Es ist die Art wie wir arbeiten und leben, die uns massiven, stark unterschätzten Cyber-Risiken aussetzt.

N- Tipp

- Umgehende Aktualisierungen aller Systeme zur Schliessung von Lücken
- Regelmässiges Einspielen von Updates
- Sicherstellen von regelmässigen Datensicherungen
- Backups und entsprechende Daten nicht nur in Cloud-Diensten speichern
- Informieren über die Risiken
- Schulung und Sensibilisierung im Umgang mit den heutigen digitalen Mitteln

Ronny Troxler
ICT Consultant & Senior
ICT System Engineer

IT

Hohe Schadenssummen mit vermeintlich bekannter Masche.

Eine weitere sehr verbreitete und bekannte Masche sind betrügerische Zahlungsanforderungen, welche hauptsächlich an den CEO des Unternehmens geschickt werden. Hierbei werden keine Daten verschlüsselt oder gelöscht, sondern es wird einzig beabsichtigt, Geldtransfers zu manipulieren. Das perfide an dieser Zahlungsanforderung ist, dass der Absender in der Regel aus den eigenen Reihen kommt, sprich z. B. von der Finanzabteilung. Die Betrüger ändern die Absendermailadresse so, dass es effektiv so aussieht, als kommt die Anfrage für eine Zahlung von dem bekannten Teamkollegen von nebenan. Erst wenn man das E-Mail genauer analysiert, z. B. über das Maillog des Spam-Schutzes, kann man erkennen, dass die Absendermailadresse gefälscht ist. Antwortet nun der CEO auf dieses E-Mail, erfolgen in der Regel Kontoverbindungen und weitere Zahlungsinformationen. Natürlich sollten hier bei solch hohen Beträgen bereits die Alarmglocken klingen. Diese Beträge können aber auch wesentlich tiefer ausfallen und somit ggf. unbemerkt ausgeführt werden. Auch hier gilt, bei solchen Zahlungsanforderungen lieber mal den Telefonhörer in die Hand nehmen und beim jeweiligen Mitarbeitenden nachfragen.

Problemstellung

Zahlungen werden unbewusst an einen Betrüger geleistet.

N- Tipp

- Lieber einmal kurz telefonisch nachfragen, wenn man nicht sicher ist oder etwas «komisch» findet
- Zeigen Sie solche E-Mails mittels eines Fotos umgehend einer Fachperson
- Leiten Sie solche E-Mails nicht weiter
- Löschen Sie solche E-Mails umgehend, ohne Inhalte anzuklicken
- Sollten diese E-Mails nicht in Ihren Spamordner gelangt sein, so gilt es, Ihre Security-Systeme dringend zu optimieren
- Sorgen Sie für abgestimmte Sicherheitskonzepte zwischen Ihren Informatiklösungen und dem Betrieb Ihrer Web- und Digitallösungen

Patrick Stalder
Leitung ICT / Senior ICT
System Engineer

IT

Das unverzichtbare WLAN wird zum Problem.

Angriffe auf WLAN Geräte und WLAN Lösungen nehmen aktuell erneut stark zu. Betrüger und Hacker versuchen oftmals unbemerkt in das Netzwerk von Unternehmen einzudringen, in dem sie Schwachstellen bei den WLAN Geräten, den Routern oder den Sicherheitssystemen ausnutzen. Auch via Mobiltelefone und deren sogenannten Bluetooth-Funktion entstehen immer mehr Lücken und Gefahren.

Stellen Sie sich vor, einem Hacker ist es gelungen, in Ihren Router einzudringen. Das kann für Sie unter Umständen nebst dem eigentlichen Schaden sehr teuer werden. Der Hacker kann beispielsweise die Login-Daten für Ihren Telefonzugang kapern und auf Ihre Kosten teure Gespräche führen oder dem gehackten Router werden Phishing-Websites untergeschoben, die Passwörter für Onlinebanking und -shopping abgreifen. Auch zielen viele Hacker-Angriffe darauf ab, den Router in ein Botnetz einzugliedern, um beispielsweise massenweise Spammails zu verschicken.

Problemstellung

Cyberkriminelle hacken sich via WLAN auf den Router und können erheblichen Schaden anrichten.

N- Tipp

- Ändern Sie immer und umgehend den werksseitigen WLAN-Schlüssel
- Sichern Sie auch einen Gastzugang für das WLAN mit einem starken Passwort
- Vergeben Sie feste IP-Adressen für Geräte im Heimnetz
- Verbergen Sie die Netzwerkkennung (SSID) Ihres WLAN und richten Sie einen MAC-Filter ein, damit sich nur bekannte Geräte im WLAN anmelden dürfen
- Achten Sie auf eine aktuelle Firmware (regelmässige Wartungen vollziehen)

Remo Emmenegger
Junior ICT System Engineer

IT

Sicherheitsupdates und Aktualisierungen sind die halbe Miete.

Ob private Endgeräte oder Geschäftskomponenten, in beiden Fällen zählt das Gleiche. Sicherheitsupdates immer umgehend durchführen und bei ausstehenden Aktualisierungen nie zuwarten. Viele der aktuellen Gefahren, welchen sich jeder Betrieb tagtäglich aussetzt, basieren auf dem nicht mehr wegzudenkenden Internet. Besteht eine Internet-Verbindung, wird man automatisch über kurz oder lang vor der Problematik stehen, dringend und stetig Sicherheitsupdates einzuspielen, unabhängig vom privaten oder geschäftlichen Informatikumfeld.

Problemstellung

Viele Betriebe machen sich keine Gedanken rund um präventive Massnahmen und reagieren auf Sicherheitsschwachstellen dann, wenn Sie in Erscheinung treten und/oder die Daten bereits verschlüsselt wurden. So gibt es nach wie vor eine grosse Anzahl an Betrieben, die auch ein altbekanntes CredSSP-Update, welches im Schadenfall zu unerreichbaren Servern führt, noch nicht reagiert haben.

N- Tipp

- Frühzeitige, fachlich begleitete Bewertung der Bedrohungslage
- Durchführung von Sicherheitsanalysen, ICT Audits und Penetrationstest
- Ausarbeitung der nötigen Massnahmen
- Umsetzung der dringenden Massnahmen im Expressverfahren
- Sicherheit des Betriebs auf strategischer Basis erhöhen

Kenan Baysal
Junior ICT System Engineer

Das gibt zu denken!

Privat wie auch geschäftlich nutzen wir alle die tollen Vorteile und Annehmlichkeiten der Digitalisierung, der Informatik und den vielen Begleiterscheinungen wie Apps und Social Media.

Gleichzeitig sind sich viele Nutzer den Gefahren nur wenig bewusst. Es fehlt an Aufklärung von den Schulen über die Arbeitswelt bis hin zum privaten Haushalt.

Müssten wir nicht zunächst verstehen, was wir täglich anwenden?

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.*

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

Phishing

– Unter dem Begriff Phishing versteht man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen.

Malware

– Als Schadprogramm, Schadsoftware oder Malware – englisch badware, evilware, junkware oder malware – bezeichnet man Computerprogramme, die entwickelt wurden, um unerwünschte und gegebenenfalls schädliche Funktionen auszuführen. Malware ist damit ein Oberbegriff, der u. a. das Computervirus umfasst.

Riskware

– Als Riskware bezeichnet man Computerprogramme, die von ihrem Urheber zwar nicht programmiert wurden, um Schaden anzurichten, jedoch sicherheitskritische Funktionen aufweisen. Diese Funktionen können zum Beispiel zum Beenden oder Neustarten laufender Prozesse oder gar zum Fernsteuern des Computers benutzt werden.

Tracking

– Tracking umfasst alle Bearbeitungsschritte, die der gleichzeitigen Verfolgung von Objekten dienen. Davon unterschieden wird das Tracing, das eine zeitlich versetzte Verfolgung anhand von Aufzeichnungen betrifft, z. B. in der Programmierung als Ablaufverfolgung.

MDM-Software

– Mobile Device Management Software steht für die zentralisierte Verwaltung von Mobilgeräten wie Smartphones, Netbooks, PDAs oder Tablets durch einen oder mehrere Administratoren mit Hilfe von Software und Hardware.

Trojaner

– Als Trojanisches Pferd, im EDV-Jargon auch kurz Trojaner genannt, bezeichnet man ein Computerprogramm, das als nützliche Anwendung getarnt ist, im Hintergrund aber ohne Wissen des Anwenders eine andere Funktion missbräuchlich ausführt und ausnutzt.

Emotet

– Emotet ist ein Computer-Schadprogramm in Form eines sogenannten «Banking-Trojaners», das auf modernere Versionen des Betriebssystems Windows von Microsoft abzielt.

MELANI

– Die Melde- und Analysestelle Informationssicherung MELANI ist eine Organisation der Bundesverwaltung der Schweiz. Der Schweizerische Bundesrat schaffte MELANI, um dem Auftrag der Bundesverfassung auch im Internetzeitalter Rechnung tragen zu können.

Ransomware (Ryuk)

– Ransomware, auch Erpressungstrojaner, Erpressungssoftware, Kryptotrojaner oder Verschlüsselungstrojaner, sind Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann.

Spam

– Als Spam oder Junk werden unerwünschte, in der Regel auf elektronischem Weg übertragene massenhafte Nachrichten bezeichnet, die dem Empfänger unverlangt zugestellt werden, ihn oft belästigen und auch häufig werbenden Inhalt enthalten.

Business Email Compromise

– Der CEO Fraud ist eine Betrugsmasche, bei der Firmen unter Verwendung falscher Identitäten zur Überweisung von Geld manipuliert werden.

CredSSP-Update

– CredSSP wird zur verschlüsselten Übertragung von Remote-Anmeldeinformationen eingesetzt.