Expert Notes

Informieren. Aufklären. Sensibilisieren.

4. November 2020 Ausgabe **13.**

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

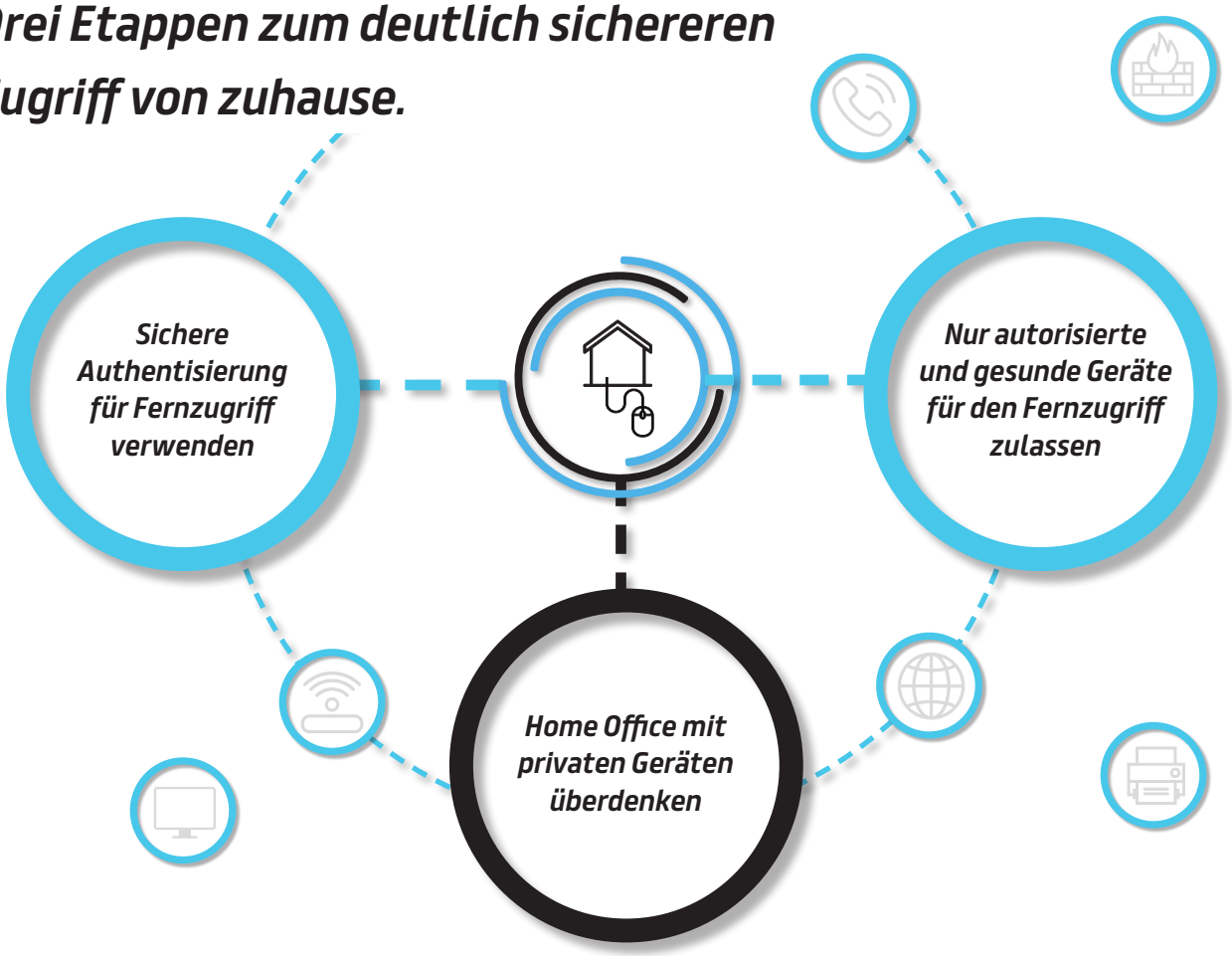
Eine Publikation der Neo One.

Leichtsinn wird durch Hektik gefördert. Die Gefahr der Pandemie im Gepäck.

Die zweite Welle der Corona Pandemie fordert uns alle als Gesellschaft enorm. Der Run in die Home Offices wird in vielen Wirtschaftsbranchen leichtsinnig «schon fast panisch» vollzogen. Auch wenn die Wichtigkeit des vom Bundesrats richtigerweise empfohlenen Gang ins Home Office ausser Frage steht, gilt es diesen Gang gezielt und gesichert zu tun. Agieren Sie clever, agieren Sie konzeptionell, schaffen Sie Sicherheitsschleusen bevor Sie einfach von zuhause aus auf das Unternehmensnetzwerk zugreifen. Es gibt vieles zu beachten, dabei gewinnen Sie vor allem aber EINES: Mehr Sicherheit.

Jan Braunschweiler
Inhaber & Geschäftsführer

Drei Etappen zum deutlich sichereren Zugriff von zuhause.



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

Corona dauert an. Home Office dauert an. Das gilt es nun dringend und weiterhin zu beachten.

Bei der stark steigenden Anzahl an Home Office Benutzern im eigenen Unternehmen führt dies unweigerlich auch dazu, dass sich die Angriffsfläche des Unternehmens erhöht. Schützte man bisher das Unternehmen vor Zugriffen von aussen und fühlte sich mit einer Firewall und geschützten Endgeräten sicher, so ist die Frage berechtigt, wie man diesen Perimeter im Home Office aufrechterhalten kann.

Sichere Authentisierung für Fernzugriff verwenden

Problemstellung & Gefahr.

Werden für die Anmeldung am Endgerät nur Benutzername und Passwort eingesetzt, so ist dies innerhalb der Räumlichkeiten vielerorts ausreichend. Um es Angreifern zu erschweren den exponierten Zugang zum Netzwerk anzugreifen und auszunutzen, sollte auf eine Mehrfaktoren-Authentisierung gesetzt werden.

N-Tipp

Für den Fernzugriff sollte zwingend auf eine Authentisierung mit mehreren Faktoren (Passwort + One Time Passcode, z.B. via Authentificator App) gesetzt werden.

Mehrwert:

So wird es für Angreifer deutlich schwieriger Ihnen zu schaden.

Nächster Schritt:

Evaluieren Sie eine geeignete Mehrfaktoren-Authentisierung bei welcher der zweite Faktor (OTP) zum Beispiel auf dem Smartphone und einer Authenticator- App erzeugt wird, welcher einerseits vom VPN Gateway unterstützt wird und in die Betriebsprozesse integriert werden kann.

Home Office mit privaten Geräten überdenken

Problemstellung & Gefahr.

Werden private Geräte für den Fernzugriff verwendet, so kann nicht sichergestellt werden, ob die Geräte in einem gesunden Zustand sind. Durch private Geräte kann es passieren, dass umgesetzte Sicherheitsmassnahmen für das Unternehmensnetzwerk ausgehebelt werden.

N-Tipp

Verwenden Sie nur Geräte, welche auch sonst in Ihrem Business Umfeld eingesetzt werden, welche geprüft sind von der IT und über nötige minimale Sicherheitsstandards verfügen.

Mehrwert:

Mit dem Einsatz von geprüften und sicheren Geräten erreichen sie eine durchgängige Sicherheit.

Nächster Schritt:

Eliminieren Sie Zugriffe von privaten Geräten auf das Unternehmensnetzwerk. Tauschen Sie diese durch geprüfte businesstaugliche Geräte aus und stellen Sie ein durchgängiges Sicherheitskonzept sicher. Entscheidend ist, dass Sie nur geschäftliche Geräte für den Fernzugriff zulassen und das Verbinden von privaten Geräten unterbinden.

Nur autorisierte und gesunde Geräte für den Fernzugriff zulassen

Problemstellung & Gefahr.

Wenn der Fernzugriff eine Erweiterung des internen Netzwerks darstellen soll, dann müssen die Geräte für den Fernzugriff mindestens ebenso gut geschützt sein wie die Geräte in den Büroräumlichkeiten. Im Büronetzwerk haben Geräte oftmals nur Internetzugang über die zentrale Firewall und lokale Webfilter.

N-Tipp

Geräte im Home Office müssen abgeschottet vom restlichen privaten Netzwerk betrieben werden und über eine Konfiguration für die Nutzung eines Webfilters verfügen.

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

Bei vielen Home Office Konstrukten ist dieser Schutz aber nicht mehr gewährleistet und die Gefahr erhöht sich umgehend. Geräte haben direkten Zugang ins Internet und sind den Gefahren im Internet ausgesetzt. Ebenso sind die privaten Netzwerke, in welchen sich die Geräte befinden, nicht überwacht oder geschützt. So ist es Angreifern möglich Schaden anzurichten.

Mehrwert:

Mit dem erwähnten Setup haben es Malware und Trojaner deutlich schwieriger auf das Unternehmensgerät bzw. -netzwerk zuzugreifen und Schaden anzurichten.

Nächster Schritt:

Stellen Sie ein professionelles Sicherheitskonzept mit gezielten Sicherheitsmassnahmen auf bevor Sie aus dem Home Office arbeiten.

Michael Schlüter
Senior ICT Security Consultant
& Cyber Security Officer

Entscheidungsträger und die fehlende Transparenz der Cyber Risiken.

Entscheidungsträger im Unternehmen müssen die richtigen Entscheidungen im Umgang mit Risiken sowie den damit verbundenen Investitionen fällen.
Für das Topmanagement ist es noch heute äusserst schwierig, sich über die Gefahren im Bereich Cyber ein klares Bild zu verschaffen. Das Thema ist extrem komplex und die Risiken, so meint man, sehr weit weg sowie schwer greifbar.

Die Komplexität der Thematik erschwert es, ein klares Bild über die Zusammenhänge der IT-Komponenten, Sicherheitsmassnahmen und den Assets einer Unternehmung zu erhalten. Dies hat auch damit zu tun, dass Cyber nicht oder nur marginal im Risikomanagement abgebildet wird.

N-Tipp

Wir empfehlen daher unbedingt ein Risikoassessment unter der Führung der Geschäftsleitung in Zusammenarbeit mit der verantwortlichen IT-Person oder externen IT-Spezialisten durchzuführen, um Gewissheit über den Zustand der IT-Infrastruktur zu erhalten und der IT-Abteilung gezielt Budget für risikominimierende Massnahmen sprechen zu können.

Gehen Sie gezielt vor.

So gehen Sie richtig vor.

- Definieren Sie die wichtigsten (IT-) Assets der Unternehmung
- Stufen Sie die Wahrscheinlichkeit ein, Opfer der verschiedenen Angreifer-Typen zu werden
- Verschaffen Sie sich ein Lagebild der IT-Infrastruktur
- Definieren Sie die Risiken und setzen die Mittel für wirkungsvolle Gegenmassnahmen ein

Jan Braunschweiler
Inhaber & Geschäftsführer

Passwort. Fingerprint. Smartphone App mit OTP. Wo geht die Reise hin?

Haben Sie sich auch schon über eine komplizierte Passwortrichtlinie geärgert? Das Passwort ist vielerorts das einzige Authentisierungsmittel und dieses birgt nach wie vor grosse Gefahren. Ein Passwort kann ohne geeignete Gegenmassnahmen mittels automatisierten Tools millionenfach ausprobiert und somit erraten werden oder die «kryptisch» abgelegten Passwörter können aufgrund von bekannten Passwörtern in sogenannten Password Dictionaries / Rainbow Tables gesucht und im Klartext ausgelesen werden. Passwörter sind besonders dann kritisch, wenn Benutzer dieses Passwort ohne weiteren Zusatz zur Authentisierung verwenden.

© created and designed by Neo One

Die sogenannte Mehrfaktoren-Authentisierung schafft Sicherheit. Das müssen Sie darüber wissen.

	Beispiel	Vorteil	Nachteil
Besitz	Sicherheits-Token, physischer Schlüssel, Smartcard, Zertifikat	Aus der Ferne schwer zu stehlen/ zu manipulieren	- Zweites Gerät bzw. Schlüssel notwendig; - Bei Ausfall muss eine Ersatzmethode zur Verfügung stehen
Wissen	Passwort, Passphrase, PIN	Leichte Implementierung	- Kann vergessen oder gestohlen werden
Persönliches Merkmal	Fingerabdruck, Gesicht, Stimme, Gangmuster	Kann nicht vergessen werden, hat man immer dabei	- Erkennungsgerät notwendig - Veränderung der Merkmale bei Unfall o.ä.

Für den Fernzugriff kann man z.B. das gewöhnliche Passwort für die Anmeldung am System in Kombination mit einem auf dem Smartphone generierten kurzlebigen Code verwenden. Diese Art von Codes können nebenbei auch für das Login bei Cloud-Applikationen wie Microsoft 365 oder Google verwendet werden. Die Authentisierung am Endgerät selber kann auch mit einem «Persönlichen Merkmal» wie den Fingerabdruck erfolgen. Dies erspart das mehrmalige Eintippen eines komplexen Passworts und bietet einen ebenso guten Schutz.

Ein zwanghaftes Anwenden von komplexen Passwörtern führt nicht zwangsweise zu einer erhöhten Sicherheit. Menschen sind Meister darin, sich die Passwörter so auszusuchen, dass diese einfach merkbar sind und dennoch den Anforderungen entsprechen. Diesen Umstand machen sich Angreifer immer mehr zu nutzen und erkennen in den Passwörtern ein Muster, welches dann wiederum schneller zur Kompromittierung genutzt werden kann.

Michael Schlüter
Senior ICT Security Consultant
& Cyber Security Officer

N-Tipp

Nutzen Sie wenn immer möglich eine Mehrfaktoren-Authentisierung, sei dies bei Internetservices, beim Fernzugriff oder für administrative Arbeiten. Lassen Sie sich über verschiedene Authentisierungsmethoden beraten und prüfen Sie die Tauglichkeit in Ihrem Unternehmen.

N-Coach

© 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

One Time Passcode (OTP)

– Ein OTP ist ein sogenanntes Einmalpasswort, welches nur für eine kurze Zeit für eine einmalige Anmeldung verwendet werden kann. Dieses Verfahren ist nicht neu und wurde früher bei Bankenlogins mit Kennwort-Streichlisten geführt. Heute kommen dafür OTP Generatoren z.B. auf dem Smartphone oder einem speziell dafür vorgesehenen Gerät (z.B. RSA Token) zum Einsatz. Ein OTP kann als zusätzlicher Faktor zum bestehenden Passwort für die Authentisierung eingesetzt werden.

Authentificator App

– Eine Authentificator App bezeichnet einen OTP Generator auf dem Smartphone. Diese Authentificator App unterstützt u.U. mehrere Arten von Authentifizierungen, insbesondere aber die Generierung von Einmalpasswörtern.

Firewall

– Eine Firewall ist ein Kernelement im Abwehrdispositiv eines Computer-Netzwerks. Die Firewall stellt sicher, dass nur Verbindungen ins Netzwerk zugelassen werden, welche legitim sind und schränkt auch die Verbindungen ausgehend ins Internet ein. Eine moderne Firewall steuert dabei nicht nur die Verbindungen, sondern untersucht auch den Dateninhalt auf verdächtige oder bösartige Daten.

Endpoint Schutz

– Der Endpoint Schutz ist ein Sicherheitselement auf den Clients aber auch Servern, welcher die Aktivitäten von Benutzern und der Applikationen untersucht und dabei einerseits auf Viren prüft sowie bekanntes schadhaftes Verhalten unterbindet. Die Aufzeichnung von Aktivitäten und das Alarmieren von verdächtigem Verhalten gehört zu den Kernelementen, wie auch die Unterstützung in der Behebung von Auswirkungen.

– VPN steht für «Virtual Private Network» und bezeichnet eine sichere Art von Netzwerk in dem Aussenstellen wie auch Home Office Geräte eine sichere Verbindung von ausserhalb des Unternehmensnetzwerks in eben dieses aufbauen können.

Lokale Webfilter

– Der Webfilter ist ein Sicherheitselement, um die Daten beim Websurfen zu prüfen. Dabei werden Zugriffe auf bekannte bösartige Webseiten und Inhalte unterbunden, Downloads auf Schadsoftware untersucht und unerwünschte Dateitypen gefiltert. Ein lokaler Webfilter bezeichnet die Instanz, welche auf dem Endgerät läuft bzw. dem Unternehmenswebfilter im Netzwerk.

Password Dictionaries

– Ein Passwort Dictionary ist eine Liste mit potentiellen Passwörtern. Ein Angreifer kann sich diese Listen zunutze machen und so den Zeit- sowie Rechenaufwand minimieren, um gängige Passwörter zu erraten.

Rainbow Tables

– Passwörter werden bzw. sollten nicht im Klartext abgespeichert werden, um die persönlichen Passwörtern nicht einem Administrator oder anderen unberechtigten Personen zugänglich zu machen. Deshalb werden Passwörter mittels einer kryptografischen Einwegfunktion (Hash) «verschlüsselt» und in dieser Form unkenntlich für andere Personen abgespeichert. In Rainbow Tables werden Millionen von Passwörtern im Klartext mit den dazugehörigen Hash-Werten berechnet, womit diese Liste es einem Angreifer erleichtert, aufgrund eines Hash-Wertes das Passwort im Klartext zu erhalten.

Ronny Troxler
ICT Consultant & Senior ICT System Engineer /
ICT Training Officer & Responsible N-Coach Services

© created and designed by Neo One