Expert Notes

Informieren. Aufklären. Sensibilisieren.

14. April 2020 Ausgabe **2.**

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

Eine Publikation der Neo One.

IT

Die vermeintlich nicht interessanten Opfer.

Wir sind nicht interessant für einen Angriff! In der Theorie mag das stimmen. Jedoch werden professionelle Angreifer ihren Angriff nie direkt beim eigentlichen Ziel starten. Sie nehmen sich KMUs vor und prüfen dort, wie weit Sie mit Ihrer Attacke kommen. Dann wird nachjustiert und erst wenn sie sich sicher sind, dass ein Angriff auch erfolgreich sein wird, werden Sie sich mit dem eigentlichen Ziel befassen.

Im Umkehrschluss heisst das:

N- Tipp

- Sicherheit geht alle an, privat und geschäftlich
- Der Sicherheitsfaktor wird in den nächsten Jahren massiv zunehmen, bereiten Sie sich vor
- Agieren Sie präventiv und nicht reaktiv
- Stellen Sie sicher, dass Ihre Mitarbeitenden immer sensibilisiert und geschult sind
- Nicht warten, leben Sie Sicherheit vor und schützen Sie Ihre Firma, Ihre Daten und Ihre Mitarbeitenden.
- Sicherheit kostet Geld, stellen Sie realistische Budgets frühzeitig auf
- Das Stillstehen Ihrer Firma während Tagen, oder sogar Wochen, muss in Ihren Worstcase-Szenarien abgefasst werden

Verantwortung wahrnehmen:

«Kann ich es mir als CEO oder Verwaltungsratspräsident leisten, dass meine Firma während Tagen oder Wochen, komplett stillsteht und alle meine Daten, inkl. den Backups, verschlüsselt sind?

Ronny Troxler
ICT Consultant & Senior ICT System Engineer

IT

Den Menschen mit neuen Technologien mitnehmen.

Unternehmensleitungen versuchen mittels neuester Technologien und Arbeitsmitteln am Markt zu agieren und so Vorteile und Effizienz zu sichern. Dabei wird oft ausser Acht gelassen, dass neuste Technologien nichts nützen, wenn wir den Menschen sprich die Mitarbeitenden nicht «mitnehmen». Besonders in der aktuellen Lage, mit Pandemie-Herausforderungen in der Schweiz, gilt es, Umgehungslösungen und Notfalllösungen einzusetzen, dabei aber auch den Mitarbeitenden genaustens zu instruieren. Schnelle Umsetzungen wie Home Office-Zugriffe zu realisieren, ohne dass die betroffenen Mitarbeitenden, die diese Zugriffe nutzen, richtig geschult werden, erhöhen das Risiko für das Unternehmen beträchtlich. Grundsätzlich sollte ein Unternehmen vor der Nutzung der Mitarbeitenden solcher Fernzugriffe, die Mitarbeitenden angemessen bezüglich Phishing-Kampagnen und Sicherheitsrichtlinien schulen. Die Mitarbeitenden sollten ebenfalls die Prozesse und Verfahren des Unternehmens zur Meldung eines Sicherheitsvorfalles kennen und könnten so in einem vermuteten Angriffsfall schnell intern kommunizieren und reagieren.

Problemstellung

Den Mitarbeitenden fehlen oft die entsprechenden Informationen und sie werden nicht geschult, auf was sie im Alltag genau achten müssen und wo Vorsicht geboten ist. Genau diesen Umstand nutzen Hacker leider mit Erfolg aus.

N- Tipp

- Eine Grundschulung aller Mitarbeitenden vollziehen mit den entsprechenden aktuellen Informationen
- Regelmässige Schulungen, Workshops aller Mitarbeitenden vornehmen
- Prozesse im Zusammenhang mit einem Sicherheitsvorfall erläutern
- Regelmässige Betriebsinformationen zur Sensibilisierung von Cyber-Gefahren

Remo Emmenegger
Junior ICT System Engineer

IT

Ein Trugschluss, zu meinen man sei sicher.

Wir haben eine Firewall und einen Virenschutz, was soll schon passieren? Korrekt, die meisten Betriebe haben Firewall und Virenschutz der neusten Generation im Einsatz. Trotzdem beginnt die Sicherheit beim Anwender. Ist der Anwender respektive das Passwort des Anwenders erst einmal kompromittiert, ist ein potenzieller Angreifer schon im Netzwerk. Das Aussperren von unberechtigten Personen von ausserhalb ist das eine, was passiert aber, wenn der Angreifer sich auf dem Netzwerk sauber authentifizieren kann, da er ja das Passwort hat? Somit dürfte allen klar sein, dass dann eine Firewall und ein Virenschutz zwar einen Schutz bieten, jedoch einen stark reduzierten.

N- Tipp

- Insellösungen reichen nicht aus
- Fachlich begleitete Gesamtkonzepte legen die Basis
- Regelmässige Sicherheitsüberprüfungen und ICT Audits gewährleisten Sicherheit
- Spezifische Angriffssimulationen, Penetrationstests stellen die Systeme zielführend auf die Probe

Kenan Baysal
Junior ICT System Engineer

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

Digital

Webseiten werden oft aus dem Sicherheitsdispositiv ausgeklammert.

Die Webseite bzw. die reine Verbindung kann heute durch SSL gesichert bzw. verschlüsselt werden. So wird beispielsweise die URL geprüft, ob tatsächlich eine Verschlüsselung eingesetzt wird. Im heutigen Internetverkehr ist dies die minimale Form und gehört heute grundsätzlich bei der Erstellung einer neuen Webseite standardmässig dazu, dass bei den Hostern diese Zertifikate aktiviert werden. Trotzdem gibt es auch heute noch Webseiten, bei denen dies nicht der Fall ist und welche als unsichere Webseiten gelten. Eine weitergehende Zertifizierung und sichere Variante ist die SSL mit Organisationsvalidierung. Dabei wird die Verbindung zwischen dem Unternehmen bzw. Server und dem Besuchenden verschlüsselt. Zusätzlich werden entstandene Schäden durch das «Knacken» der Verschlüsselung im Wert von bis zu CHF 1.5 Mio. versichert. Ein entsprechendes Siegel darf in diesem Fall als Grafik auf der Website eingebunden werden und die Adressleiste des Browsers zeigt sich grün eingefärbt und das Unternehmen ist klar mit dem Namen erkennbar. Um hier eine Zertifizierung zu erhalten, muss das Unternehmen beispielsweise auch einen Handelsregisterauszug übermitteln und es werden Kontrollanrufe in das Unternehmen getätigt, um die Echtheit des Unternehmens zu verifizieren. Sinnvoll ist diese Zertifizierung bei Webseiten mit Funktionen wie Online-Shop, Online-Zahlungen, User-Logins oder Datenaustausch. Zur Reputation eines Unternehmens ist dieser Vorgang auch bei normalen Webseiten sehr zu empfehlen.

Problemstellung

Wenn die Webseite über keine SSL-Verschlüsselung verfügt, wird diese im Internet als nicht vertrauenswürdig angesehen und folglich können Nachteile entstehen.

N- Tipp

- Webanalyse vornehmen und Webseite überprüfen lassen
- Umsetzung im Minimum der SSL-Verschlüsselung
- Allenfalls weitergehende SSL-Verschlüsselung mit Organisationsvalidierung vornehmen
- Regelmässige Webseiten-Wartungen durchführen
- CMS (Content Management System) Updates einspielen lassen
- Sicheres bearbeiten der Webseiten-Inhalte
- Sicheres Surfen Ihrer Webseiten-Besuchenden
- Verbessertes Ranking in Suchmaschinen
- Basis für die Nutzung von neuen Technologien (z.B. Geo-Lokalisation für die Standortbestimmung)

Fabian Müller
Leiter Operations & Digital

N-Coach.
Mieten Sie Ihren N-Coach und profitieren Sie operativ wie auch strategisch für Ihr Unternehmen.

Das gibt zu denken!

Investitionen in Technologie, Sicherheit und Arbeitsmittel werden von Schweizer Firmen fortschrittlich und zukunftsgerichtet vorangetrieben. Der Mensch der diese Arbeitsmittel und Technologien anwenden muss, damit die Unternehmen überhaupt einen Mehrwert aus den Investitionen erhalten, wird oft vergessen. Es fehlt an Schulungen, Instruktionen, Aufklärungen und regelmässigen Coachings.

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

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

VPN-Zugriff

– Das konventionelle VPN bezeichnet ein virtuelles privates Kommunikationsnetz. Virtuell in dem Sinne, dass es sich nicht um eine eigene physische Verbindung handelt, sondern um ein bestehendes Kommunikationsnetz, das als Transportmedium verwendet wird

Remote-Desktop

– Remote-Desktop bezeichnet den Fernzugriff auf den Desktop eines Computers. Dabei werden Anwendungsprogramme auf einem Computer ausgeführt und auf einem anderen Computer dargestellt und bedient. Im Gegensatz zum Screen-Sharing muss sich kein Benutzer am Server lokal anmelden.

Terminalserver

– Der Begriff Terminalserver steht für ein Funktionsprinzip der elektronischen Datenverarbeitung und für Server-Software sowie -Hardware. Bei einem Terminalserver sind Daten zentral auf einem «Server» oder «Host» gespeichert und die Programme werden dort ausgeführt, während die Ein- und Ausgabe dezentral auf Benutzerendgeräten (den Terminals oder der Clientsoftware) über ein Netzwerk stattfindet. Auf dem Server werden die Programme ausgeführt, auf dem Client oder Terminal nur der Bildschirm dargestellt sowie Maus und Tastatureingaben an den Server übermittelt.

Zwei-Faktor-Authentifizierung (Multifaktorenauthentifizierung)

– Die Zwei-Faktor-Authentisierung, häufig auch als Multifaktorenauthentifzierung benannt, bezeichnet den Identitätsnachweis eines Nutzers mittels der Kombination zweier (oder mehrerer) unterschiedlicher und insbesondere unabhängiger Komponenten.

Firewall

– Eine Firewall ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt. Weiter gefasst, ist eine Firewall auch ein Teilaspekt eines Sicherheitskonzepts. Jedes Firewall-Sicherungssystem basiert auf einer Softwarekomponente.

URL

– Ein Uniform Resource Locator identifiziert und lokalisiert eine Ressource, beispielsweise eine Webseite, über die zu verwendende Zugriffsmethode und den Ort der Ressource in Computernetzwerken.

Hoster/Hosting

– Hosting bezeichnet eine etablierte Kurzform für den Betrieb von Softwareapplikations- oder Internetdiensten.