Expert Notes

Informieren. Aufklären. Sensibilisieren.

15. September 2022 Ausgabe **23.**

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

Eine Publikation der Neo One.

Das bedroht Unternehmen.
Kurzfassung mit hoher Wichtigkeit.

In 20 Minuten sensibilisiert sein, ist vor allem eines; ein kurzer kleiner Invest in die Sicherheit von Ihnen und Ihrem Unternehmen. Nehmen Sie sich die Zeit, um zu verstehen, «was» Sie bedroht und «was» Sie dagegen tun können.

Weshalb müssen wir uns mit Cyber-Bedrohungen beschäftigen?

Cyber-Angriffe sind erfolgreich, weil Unternehmen diese zulassen. Dieser Milliardenmarkt ist für Kriminelle äusserst lukrativ und es braucht daher klare Cyber-Schutzmassnahmen, klare Konzepte und eine Unternehmenswerterhaltung, welche diese Themen in das operative Geschäft integrieren. Wirtschaftskriminalität hat viele Facetten und die Anzahl von Delikten ist seit Jahren hoch. Betrüger gehen dabei immer vorsichtiger und gezielter vor. Während es vor einiger Zeit noch Phishing E-Mails waren, die nicht personalisiert an grosse Verteiler gesendet wurden und so leichter zu identifizieren waren, informieren sich Betrüger nun auch in einer zweiten Strategie gezielt über ihre Opfer.

Viele Firmen und Privatpersonen wollen die Digitalisierung und profitieren davon. Aber sind wir auch bereit die Schattenseiten abzufedern und in die Sicherheit zu investieren?

Unternehmen in der Schweiz wie auch alle Privatpersonen profitieren von den digitalen Möglichkeiten. Unser «Way of Life» und unser «Way of Business» hat uns allen viele Vorteile gebracht. Es ist höchste Zeit auch die Nachteile richtig einzuordnen, Schutzkonzepte sicherzustellen und uns stetig darauf zu sensibilisieren.

So versuchen Cyber-Kriminelle zum Erfolg zu kommen:

GEFAHR

- Aufmerksamkeit schaffen
- Verleiten
- Täuschen

Das sind die Auswirkungen einer erfolgreichen Attacke:

GEFAHR

- Daten verschlüsseln & Opfer erpressen
- Daten entwenden & verkaufen oder Opfer mit dieser Drohung erpressen
- Daten zerstören & bösartige Aktionen ausführen
- Ausspionieren
- Generell Geld erpressen

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

1

Home-Office und Fernzugriffe.
Deshalb müssen wir uns gut aufstellen.

Sobald Unternehmen Fernzugriffe auf das Firmennetzwerk zulassen, seien es Home-Office-Zugriffe oder Zugriffe «on the road», entsteht heute das gewünschte, nötige und flexible Arbeiten. Es entsteht aber auch ein markantes Sicherheitsrisiko.

GEFAHR

- Phishing-Versuche mit dem Ziel Passwörter und somit Zugänge zu erhalten
- Brute-Force-Attacken mit dem weiteren Versuch, Angriffe auf Passwörter zu ergaunern
- Angriffe auf sogenannte ungesicherte Gateways. Das bedeutet das Erreichen eines Einfallstores, um Schaden anzurichten
- Angriffe mit Malware, sprich sogenannten gefälschten E-Mails als Beispiel

Gefälschte Rechnungen haben leider immer wieder Erfolg.

Sie erhalten falsche, unberechtigte Rechnungen per Post oder E-Mail von dem vermeintlich richtigen Absender.

2

GEFAHR

- Entsprechend soll der Empfänger verleitet werden Links oder Anhänge anzuklicken
- Das Ziel ist es, Schadsoftware auf diese Weise ins Unternehmen zu schleusen

3

Briefe und Paketsendungen sind unser Alltag.
Genau das ist gefährlich und wird ausgenutzt.

E-Mails, SMS und weitere Kommunikationsformen werden ausgenutzt, um mit gefälschten (Paket-)Benachrichtigungen den Empfänger dazu zu verleiten, Links anzuklicken.

Nach dem Anklicken des Links öffnet sich eine Seite, auf der dann eine Paketsoftware heruntergeladen werden soll. Dabei handelt es sich um die Schadsoftware.

GEFAHR

- Gefälschte E-Mails von der Post mit dem Ziel den Empfänger zu verleiten, auf Links zu klicken
- Gefälschte Paketdienstsendung per SMS oder E-Mail mit dem Ziel zu verleiten, auf Links zu klicken, darauf zu antworten oder eine Nummer anzurufen

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

4

Der mittlerweile schon altbewährte Verschlüsselungstrojaner ist immer noch äusserst verbreitet und richtet grossen Schaden an.

Der Verschlüsselungstrojaner ist ein Schadprogramm, welches ins Unternehmen geschleust wird (z.B. durch Phishing-E-Mails) und zur Folge hat, dass der Rechner, PC, Zugriff für den Nutzer oder jegliche Nutzer gesperrt und nicht mehr zugänglich ist.

GEFAHR

- Keine Zugriffe mehr auf Daten
- Keine Zugriffe mehr auf Systeme
- Teils als Unternehmen eingeschränkt oder nicht mehr handlungsfähig
- Erpressbar (solange kein gutes Datensicherungskonzept vorhanden ist)

5

Die User auf den falschen Weg führen und verleiten.

Deshalb ist Phishing leider so erfolgreich.

Phishing ist ein «auf elektronischem Wege» versuchter Betrug. Als Köder dient ein speziell echt wirkendes und konzipiertes E-Mail, welches die Opfer zu falschem Handeln zwingen soll.

GEFAHR

- Opfer werden dazu gebracht, sensible Daten preiszugeben
- Opfer werden dazu verleitet, auf Links zu klicken
- Opfer werden dazu verleitet, den Weg für Schadsoftware zu ebnen

6

Die Verfügbarkeit stören und überlasten.

Folgendes ist so gravierend an DDoS-Attacken.

Unter DDoS (Distributed Denial of Service = Verweigerung des Dienstes) versteht man einen Angriff auf Computer-Systeme mit dem erklärten Ziel, deren Verfügbarkeit zu stören. Das Datenvolumen erreicht oft mehrere hundert Gbit/s. Dies sind Volumen, die eine einzelne Organisation in der Regel ohne fremde Hilfe nicht mehr bewältigen kann.

GEFAHR

- Ausfall sämtlicher Dienste, die mit dem Internet kommunizieren
- Reputationsverlust
- Finanzieller Verlust, insbesondere wenn eine Firma oder eine Organisation von einer Internetplattform abhängig ist
- Daten auf dem Computer unbrauchbar machen
- Finanzieller Schaden bei Bezahlung des Lösegeldes
- Existenzielle Bedrohung von Firmen/Behörden, wenn ebenfalls das Backup verschlüsselt wurde

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

Die CEO Betrugsmasche wird nach wie vor stark unterschätzt.

Vermeintlich dringende Zahlungsaufforderung vom CEO, Geschäftsherr, Finanzchef oder dem VR-Präsidenten.

7

Die Angreifer beschaffen sich im Vorfeld Informationen über ein Unternehmen, eine Behörde oder einen Verein aus unterschiedlichen öffentlichen Quellen. Mit diesen Informationen wird dann ein Szenario ausgearbeitet und ein massgeschneiderter Angriff durchgeführt. Der eigentliche Betrug findet häufig mit einer E-Mail des angeblichen CEO an die Finanzabteilung oder einer E-Mail vom angeblichen Vereinspräsidenten an den Kassier statt. Durch eine glaubwürdige Geschichte soll die angeschriebene Person dazu bewegt werden, angebliche und dringende Zahlungen auszulösen.

GEFAHR

- Teils hoher finanzieller Verlust

8

Datenabfluss ist ein weiterer grosser Hebel für eine Erpressung.

Die Ursachen von Datenabflüssen sind vielfältig und reichen von Diebstahl durch Mitarbeitende, über vergessene und schlecht gewartete Server bis hin zu Backups, die nicht ordnungsgemäss geschützt sind.

Gefolgt auf den Datenabfluss kommt es zu Erpressungen, Lösegeldforderungen oder der Durchsetzung des Schadens durch Veröffentlichung der Daten.

GEFAHR

- Unerwünschter Datenabfluss
- Hohe Kosten
- Gefahr des Weiterführens des Betriebs
- Reputationsverlust
- Verlust von vertraulichen Daten / rechtliche Problematik
- Verlust von Kundendaten / Geschäftsbeziehungsschaden

GEFAHR

- Verlust von persönlichen Daten
- Genereller E-Banking-Betrug
- Gefahr für grosse finanzielle Schäden
- Stehlen von persönlichen Daten

9

Nicht erklärbare E-Mail-Transaktionen, ausgelöst durch Schadsoftware.

Angreifer versuchen fremde Rechner über unterschiedlichste Kanäle mit Schadsoftware zu infizieren, beispielsweise über einen Dateianhang einer E-Mail, versteckt in einem Gratis-Download oder beim Besuch einer Webseite. Schadsoftware ist heutzutage meist multifunktional und besitzt oft die Möglichkeit, weitere Schadsoftware nachzuladen. Dies eröffnet den Angreifern zahlreiche Möglichkeiten. Leider lässt sich eine Infektion nicht so leicht erkennen. Anzeichen sind beispielsweise ein langsamer werdendes System oder ein erhöhter Netzwerkverkehr.

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

10

Die Kombinationsfalle aus Anruf und Schadsoftware

In dieser Variante sind die E-Mails oftmals begleitet von einem Telefonanruf, welcher die Versandpapiere visieren lassen will. Im Verlauf des Telefongesprächs wird mitgeteilt, dass die Papiere per E-Mail zugestellt würden. Die Angreifer versuchen auf diese Art und Weise, Schadsoftware auf einen Computer zu bringen. Hinter dem Link im PDF-Dokument verbirgt sich eine Schadsoftware. Die ausgelieferte Schadsoftware kann variieren. Meist handelt es sich um einen e-Banking-Trojaner.

GEFAHR

- Sehr spezifisch
- Gefahr, dass ein Link im PDF oder sonst wo geöffnet wird
- Gefahr des Auslösens einer Schadsoftware, welche zum Ziel hat, bei der nächsten e-Banking-Sitzung auszuspionieren

11

SMS «Voice-Nachricht» enthält Schadsoftware

Immer mehr gibt es auch SMS oder WhatsApp-Nachrichten mit einer angeblichen Benachrichtigung, dass eine «Voice-Nachricht» verfügbar sei. Um die ganze Nachricht zu hören, soll man einen Link anklicken. Nach dem Anklicken des Links öffnet sich eine Seite mit dem Logo des Herstellers/Versenders oder z.B. dem Internetprovider und der Aufforderung, eine sogenannte «apk-Datei» herunterzuladen. Dabei handelt es sich um Schadsoftware.

GEFAHR

- Sehr verleitende Variante
- Hochgefährlich, sofern man auf die apk-Datei klickt
- Schnell zu verwechseln mit einer echten, ordentlichen Voice-Message

12

Rechnungsmanipulationsbetrug mit geänderter IBAN-Nummer

Bei dieser Betrugsform wird jeweils auf eine bestehende E-Mail-Kommunikation Bezug genommen, die eine Zahlungsanweisung oder eine Rechnung enthält. Anschliessend wird die IBAN-Nummer, auf die der Betrag einbezahlt werden soll, geändert. Um an die E-Mail-Kommunikation zu kommen, müssen Angreifer entweder Zugriff auf das E-Mail-Konto des Absenders oder auf das Konto des Empfängers haben. Dies kann durch eine der vorgelagerten Massnahmen, wie obenstehend, geschehen sein.

GEFAHR

- Bereits versendete Rechnungen werden mit geänderter IBAN-Nummer nochmals versendet
- Oder es wird generell darauf hingewiesen, für zukünftige Zahlungen ein anderes Konto zu benutzen
- Dies wird ausgenutzt, um den Betrug sicherzustellen

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

Sich zu schützen beginnt damit, sensibilisiert zu sein.

Sich zu schützen wird dann zum Fortschritt, wenn man konkrete Dinge beachtet.

Sich zu schützen bleibt dann erfolgreich, wenn man permanente Massnahmen ergreift.

So schützen Sie sich im Generellen.
12 Punkteplan für Sie und Ihre ICT.

- IT ganzheitlich überprüfen
- Schwachstellen identifizieren
- IT, sicher & funktional aufstellen
- Risiken fortlaufend erkennen
- Risiken reduzieren
- IT unterhalten & aktualisieren
- Regelmässig agieren und reagieren
- IT-Prozesse dokumentieren
- Geo-redundante Backups sicherstellen
- Notfallplan / Disaster Recovery & Incident Response Plan bereit halten
- Datenwiederherstellungstests lancieren
- Mitarbeitende sensibilisieren & informieren

Auf diese Absicherungen kommt es besonders an.
Von Datenbackup über Disaster Recovery- und Incident Response-Planung.

Der Disaster Recovery Plan.
Gesichert wiederherstellen.

- Legen Sie einen Notfallwiederherstellungsplan fest
- Überlassen Sie nichts dem Zufall
- Definieren Sie alle Betriebsabläufe und Kausalitäten

Das Backup. *Schaffen Sie eine Grundlage.*

- Speichern Sie alle relevanten Daten regelmässig
- Speichern Sie Images der Betriebssysteme sowie Clients
- Stellen Sie eine vollumfängliche Daten- und Systemsicherung sicher
- Sichern Sie Ihr Backup offline

Der Incident Response Plan.
Im Notfall strukturiert agieren.

- Erstellen Sie einen Vorfallreaktionsplan
- Bestimmen Sie die Verantwortlichkeiten
- Bestimmen Sie die Chronologie der Aktionen

Das Dokument.
Prozesse genau definiert.

- Dokumentieren Sie alle Digitalisierungselemente
- Dokumentieren Sie alle Prozesse
- Erstellen Sie ein Notfallhandbuch

Der Failover Test. *Gespielter Ernstfall.*

- Führen Sie präventiv und regelmässig Failover Tests durch
- Simulieren Sie möglichst echt den Worst Case
- Schaffen Sie Verbesserungen, bevor diese effektiv gebraucht werden

Brauchen Sie Beratung, Unterstützung in Bezug auf Cyber-Sicherheit, ICT und den neuen Kollaborationslösungen?

Informieren Sie sich an einer unserer Neo One Input/Output-Veranstaltungen – unsere Fachleute helfen gerne.

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