Expert Notes

Informieren. Aufklären. Sensibilisieren.

8. September 2020 Ausgabe **11.**

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

Eine Publikation der Neo One.

Die Lebensversicherung des Unternehmens. Wie die Digitalisierung die Risiken verändern.

Mit der zunehmenden Automation, Digitalisierung und Informatikabhängigkeit geht die Wirtschaft mit Sicherheit den einzig richtigen Weg. Jedoch gilt es auch, die Prozesse, Betriebskonzepte und alle damit verbundenen Abläufe anzupassen. Nur dann kann wirklich von fortgeschrittenen Technologien und Lösungen profitiert werden. Beachten Sie für Ihr Unternehmen nachfolgenden N-Tipp, um Ihr Unternehmen sicher aufzustellen.

Das Backup. Schaffen Sie eine Grundlage.

Optimalerweise speichern Sie alle relevanten Daten und Images der Betriebssysteme und Clients auf Ihrem Backup. Diese Daten dienen dazu, verlorene Daten wiederherzustellen. Dies kann nach einer unabsichtlichen Löschung, unumkehrbarer Modifikation durch Mitarbeitende oder aber durch Verschlüsselung der Daten durch einen Angreifer notwendig sein. Die Existenz einer Unternehmung hängt nicht wenig von der Wiederherstellbarkeit eines Backups ab! Es sind diverse Fälle in der Wirtschaft bekannt, welche Unternehmen zur Geschäftsaufgabe gezwungen haben, weil die Daten über Monate nicht mehr rekonstruierbar waren.

Die Wiederherstellung. Erstellen Sie Ihren Disaster Recovery Plan und führen Sie regelmässige Failover Tests durch.

Ein Notfallwiederherstellungsplan hilft Ihnen, nichts dem Zufall zu überlassen. Ein genau auf den Betrieb abgestimmter Ablauf zur Ausführung von Notfallwiederherstellungsprozessen ist massgebend, um die vielen Risiken der digitalen Systeme, von welcher die Organisation abhängig ist, schnell wieder zur Verfügung stellen zu können. Das sogenannte Disaster Recovery und der Incident Response Plan sind der Schutz des Unternehmens im Katastrophenfall. Ein solcher Katastrophenplan muss konzipiert werden, ist aber nur dann brauchbar, wenn regelmässige Test durchgeführt werden. Haben Sie grössere Datenmengen schon einmal in einem Recovery Test wiederhergestellt und die Systeme auf Funktionsfähigkeit und die Daten auf ihre Lesbarkeit überprüft? Wenn nicht, ist dies höchste Zeit. Ein Einspielen von mehreren Terabytes Daten erfordert einerseits Zeit, und anderseits müssen die darunterliegenden Systeme bereitstehen. Zudem muss die Reihenfolge beim Aufstarten/Wiederherstellen der Systeme klar sein, um die Datenkonsistenz nicht zu gefährden und priorisierte Business-Prozesse zu bevorzugen. Wiederherstellungstests sollten regelmässig durchgeführt werden, um für den Ernstfall wirklich gewappnet zu sein.

Die Prozessdokumentation. Prozesse & Trainings geben Gewissheit.

Definieren Sie die notwendigen Prozesse und dokumentieren Sie diese in Ihrem persönlichen Notfallhandbuch. Jährliche oder häufigere Tests für das Training der Krisenbewältigung in einem Disaster-Fall helfen die Prozesse zu verinnerlichen. Eine Bewältigung eines Angriffes und dessen Folgen ist unangenehm; Stress bildet sich und die Nerven liegen blank. Behalten Sie einen kühlen Kopf und halten Sie sich an trainierte Abläufe und dokumentierte Pläne.

N- Tipp

Wie sich Ihr Incident Response Team gliedern sollte:

- Geschäftsführer/Senior Management
- IT-Security
- IT-Leitung
- Rechtsabteilung
- Kommunikation
- Externe Organisationen

Jan Braunschweiler
Inhaber & Geschäftsführer

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

Wir wurden gehackt!

Jetzt gilt es schnell, zielgerichtet und nach klarem Ablauf zu reagieren.

Ihr Unternehmen wird Opfer eines Cyber-Angriffs und nun müssen die Zahnräder richtig ineinander greifen! Der Faktor Zeit ist ein entscheidendes Mittel, um den Schaden so klein wie möglich zu halten. Mit dem N-Tipp zeigen wir Ihnen die wichtigsten Merkpunkte auf.

1. Der klare Plan.

Planen Sie den Ablauf der Reaktion bei einem Vorfall vor dessen Eintritt mit einem Incident Response Plan, um keine unnötige Zeit für Planung und Organisation zu verlieren. In diesem Plan werden folgende Punkte dokumentarisch festgehalten:

- Die wichtigsten Ansprechpartner
- Die Zuständigkeiten / Eskalationswege auch ausserhalb der Arbeitszeiten
- Alle Kontaktdetails von Mitarbeitenden und externen Partnern
- Wann wird kommuniziert und an wen (z.B. Datenschutzbeauftragter, Mitarbeitende, Medien)
- Mögliche Szenarien und Massnahmen

2. Die richtigen Fragen im Vorfeld.

Es gibt diverse Fragen, die Sie mit gutem Gewissen beantworten können sollten und sich deshalb vorbereiten sollten.

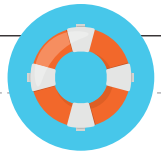
3. Die Sofortmassnahmen.

Welche Massnahmen beim Reagieren auf einen Cyber-Angriff sofort ergriffen werden müssen, unterscheiden sich stark vom Unternehmen und der Art des Angriffs.

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



Detailliert. Spezifisch. Äusserst strukturiert.

- Incident Response Plan aktivieren
- Betroffene Systeme isolieren
- Wenn Verdacht auf Einfluss von ausserhalb besteht, sollte eine Isolation vom Internet aller Systeme umgesetzt werden
- Isolation der Backups vom Netzwerk
- Nicht relevante Systeme wie Gäste-WLAN deaktivieren
- Sicherung von Logs und anderen Beweismitteln
- Aufbieten von IT-Forensikern
- Abschätzen, was der Vorfall für die Geschäftsprozesse bedeutet
- Einbeziehen der Rechtsabteilung
- Informationspflicht gegenüber Behörden und Kunden
- Kommunikation intern an Mitarbeitende über externe Kommunikationswege
- Keine (Domain-)Administratoren-Accounts auf den befallen Systemen benutzen

Übersichtlich & wirksam.

Im mindesten empfehlen wir jeder Unternehmensgrösse, die drei wichtigen Massnahmen zu lancieren.

Isolation.

Isolieren Sie die betroffenen von den gesunden Systemen, um die Ausbreitung von Malware oder der Zugriff auf Daten einzuschränken. Hierfür ist u.U. auch eine Trennung des gesamten Netzwerkes vom Internet zielführend, um die Kontrollaktivitäten der Angreifer zu unterbinden.

Backup.

Prüfen Sie, ob das Backup in den letzten Tagen korrekt gesichert wurde und stellen Sie neue Backupjobs sofort ein bzw. trennen Sie das Backupsystem vom Netzwerk. Es soll verhindert werden, dass verseuchte, veränderte oder verschlüsselte Daten ins Backup geschrieben und womöglich alte funktionierende Backups überschrieben werden. Aber es ist auch ein Schutz für das Backup-System selber, um nicht angreifbar zu sein.

Prüfspuren.

Log-Dateien sind wichtig für die Aufarbeitung des Vorfalls und für Erkenntnisse, was der Angreifer alles ausgeführt hat. Deswegen ist es enorm wichtig, Log-Dateien zu sichern, bevor diese im normalen Rhythmus überschrieben werden. Angreifer können mehrere Tage oder sogar Wochen im Netzwerk sein, bevor diese auffliegen – sichern Sie deswegen auch alte Log-Dateien.

Die Nacharbeiten.

1.

Aufarbeitung von Vorfällen sind nicht nur aus rechtlicher Sicht wichtig, sondern auch für die Verbesserung der eigenen Widerstandsfähigkeit. Lernen Sie aus den Geschehnissen und profitieren Sie auch von den Informationen der externen Partner, die Sie unterstützt haben. Oftmals kennen IT-Forensiker die internen Systeme nach einem Vorfall besser, als dies intern bisher der Fall war.

2.

Anpassungen der Sicherheitsmassnahmen und Durchführung von Schulungen. Nicht selten wird ein Unternehmen nach einem Cyber-Vorfall wieder angegriffen. Machen Sie den Fehler nicht zweimal. Optimieren Sie das Abwehrdispositiv und die Fähigkeiten, Angriffe zu erkennen und das Geschäft nach dem Angriff wieder hochzufahren.

3.

Teilen Sie Informationen, sofern betrieblich vereinbar, mit anderen Partnern, Kunden, Unternehmen und Medien, um einerseits Transparenz auszustrahlen, anderseits um auf die Gefahren aufmerksam zu machen und das Wissen an andere weiterzugeben.

Michael Schlüter
Senior ICT Security Consultant
& Cyber Security Officer

In einer Kaffeelänge zu mehr Cyber-Sicherheit. Sprechen Sie mit denjenigen, die nicht nur beraten, sondern umsetzen.

- Cyber Security ETH
- Master of Science in Business Information Systems FHNW
- Bachelor of Science in Computer Science ZHAW
- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (CEH)

Patrick Stalder
Leitung ICT
Senior ICT System Engineer

Michel Hipp
Leitung ICT
Senior ICT System Engineer

Michael Schlüter
Senior ICT Security Consultant &
Cyber Security Officer

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