SECURITY TAKE AWAY

powered by S@ND

Glücklicherweise gibt es nicht jeden Tag eine Cyberangriff. Aber was wäre, wenn?

Funktionieren wirklich alle Prozesse?

Stimmen alle Kontaktpersonen noch?

Wer trägt die Verantwortung?

Wissen die Mitarbeiter, was zu tun ist?

Wie wird eskaliert und an wen?

Solche und viele andere Fragen stellt man sich leider viel zu häufig in der IT-Security, denn bis etwas passiert, kann man sich nur vorbereiten und hoffen.

Wie können DryRuns Ihnen helfen, solche Fragen zu beantworten?
Machen Sie einen Testlauf bevor "das Haus brennt"!

WAS IST EIN DRY RUN?

Als DryRuns werden Prozess- und Softwaretests bezeichnet, die unabhängig von der Produktivumgebung ausgeführt werden. Der Begriff stammt aus der Feuerwehr, wo Übungen ohne Wasser und Feuer durchgeführt wurden, um Gefahren und Kosten zu vermeiden. Im Gegensatz dazu beschreibt WetRun das Testen in einer realen Umgebung.

Ein DryRun ähnelt einem Dungeons-and-Dragons-Spiel, bei dem der Spielleiter den Spielern die Freiheit gibt, eigene Entscheidungen zu treffen, während er den Spielverlauf kontrolliert. Hier bei NetDescribe in unserem S@ND-Team laufen DryRuns ebenfalls wie ein Rollenspiel ab, mit einem "Gamemaster" (GM) und mindestens einem "Spieler".
Der GM entwirft ein Incident-Szenario und beschreibt es dem Spieler. Von diesem Zeitpunkt an muss der Spieler basierend auf dem Prozess Entscheidungen treffen.

Ein großer Vorteil ist die Flexibilität, da die Situation nicht vorher festgelegt ist und es unendliche Möglichkeiten gibt, was passieren kann.

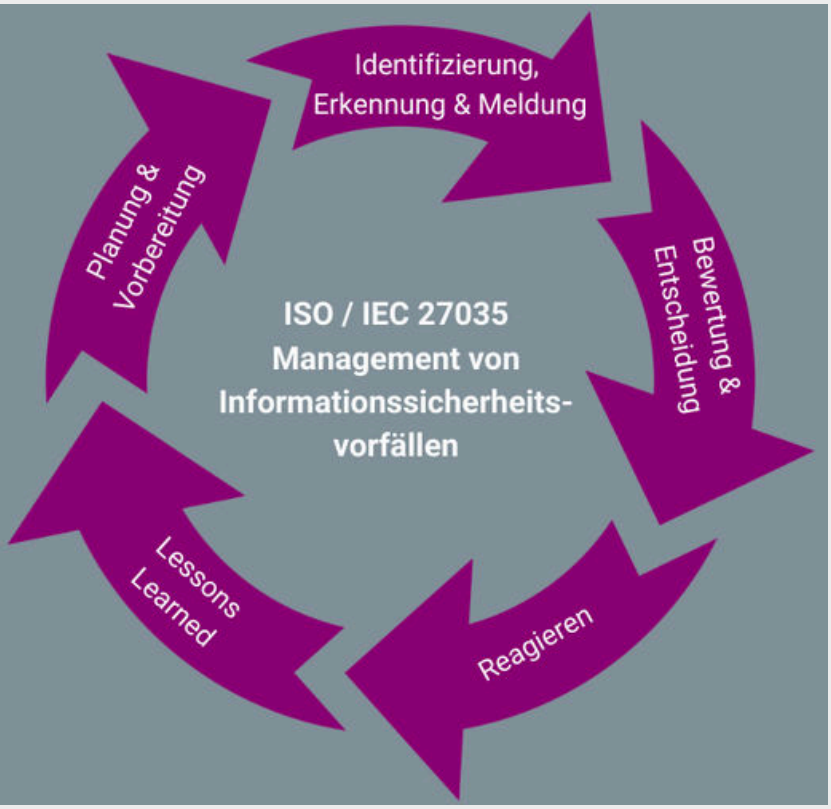
Durch das prozessbezogene Arbeiten werden alle Dokumente, einschließlich Eskalationswege und Kontaktpersonen, regelmäßig überprüft und fehlende Dokumente ergänzt.

DryRuns können auch effizient für die Einarbeitung neuer Mitarbeiter eingesetzt werden. Der GM kann sie in Situationen bringen, die im Ernstfall bereits vertraut sind. Auf diese Weise gewöhnen sie sich schnell an die saubere und strukturierte Arbeitsweise gemäß des Prozesses.

ISO / IEC 27035 - Die Standards beschreiben einen 5-Phasen-Prozess:

- **Vorbereitung** auf den Umgang mit Vorfällen
- **Identifizierung** und Meldung von Informationssicherheitsvorfällen
- **Bewertung** von Vorfällen und Entscheidung darüber, wie sie behandelt werden sollen
- **Reagieren** auf Vorfälle, Eindämmen, Untersuchen und Beheben der Probleme
- **Lehren** ziehen und Prozesse optimieren

ISO/IEC 27035 wurde erstmals 2011 als eine einzige Norm veröffentlicht und erst im letzten Jahr vollständig überarbeitet und in vier Teile aufgeteilt:
Teil 1: Grundsätze und Verfahren
Teil 2: Leitlinien zur Planung und Vorbereitung der Reaktion auf Vorfälle
Teil 3: Leitlinien für die Reaktion auf IKT-Vorfälle
Teil 4: Koordinierung



Diese 5 Schritte sollte Ihr Incident Response Plan abdecken:

1. Vorbereitung - Ausarbeitung einer Richtlinie, wie auf Vorfälle reagiert werden soll, welche Maßnahmen haben Vorrang und wer für die Bearbeitung von Vorfällen zuständig ist
2. Erkennung und Analyse der Bedrohung
3. Eindämmung, Ursache beheben und Systeme wiederherstellen
4. Aktivitäten nach einem Vorfall - Lessons Learned
5. UND regelmäßiges Testen des Plans, bevor das Haus brennt!

Wir können Sie dabei in jeder Stufe des Plans unterstützen! Kontaktieren Sie uns.

Und im nächsten TakeAway erfahren Sie mehr zu Passwörtern und Multifactor Authentication. Seien Sie gespannt!