Quelle: Pixabay

WHAT IS RED TEAMING?

Die Learnings

Learning 1

Ihr seid sicher?

Learning 1

Ihr seid sicher?

Ganz sicher nicht, es ist nicht die Frage „ob“ - sondern „wann“

Learning 2

Ihr habt wie wir in den letzten Jahren
so viel in IT-Security investiert …

Learning 2

Ihr habt wie wir in den letzten Jahren
so viel in IT-Security investiert …

und trotzdem wird es mit sehr hoher Wahrscheinlichkeit
nie mehr aufhören. Der Ressourcenbedarf war riesig.

Selbst unsere Dienstleiter hatten Probleme,
schnell genug zu skalieren.

Learning 3

Das Tempo war die Hölle …

Learning 3

Das Tempo war die Hölle und wir waren zu langsam …

Es geht im Fall der Fälle nicht um Stunden,
sondern um wenige Minuten

Der Versatz zwischen Alarm, Analyse, Planung und Abwehr war zu groß. Auch haben Prozesse nicht wie vorgesehen funktioniert.

Learning 4

Seid bestmöglich vorbereitet und trainiert es regelmäßig …

Learning 4

Seid bestmöglich vorbereitet und trainiert es regelmäßig …

Ein paar exemplarische Fragen, die uns beschäftigt haben:

- In welchem Raum treffen wir uns
- Wer hat eigentlich welche Rolle
- Wer entscheidet das Runterfahren der Systeme
- Können wir unsere Mitarbeiter:innen aus dem Urlaub zurückholen
- Zahlen wir den Abbruch des Urlaubs auch für die Familie
- …

Learning 5

Wir werden langsamer …

Learning 5

Wir werden langsamer …

Das permanente Hinterfragen wird ein Muss, ebenso wie das Auditieren unserer Partner. Die gewonnene Freiheit, die die Cloud in den letzten Jahren mit sich brachte, wird sich zukünftig anders gestalten.

Auch wird uns die Aufarbeitung der Ergebnisse sehr lange beschäftigen.

Learning 6

Verlasst euch nicht auf eure Dienstleister …

Learning 6

Verlasst euch nicht auf eure Dienstleister …

Testet sie und ihre Produkte!
Pentest & Co. sind gut und sinnvoll, aber kein Reality-Check

Learning 7

Die Belastung für das Team ist immens …

Überlegt euch vorher, wie damit umgehen werdet und bereitet euch bestmöglich vor. Im Zweifel arbeitet das Team mehrere Wochen/Monate in diesem Modus.

Security first!

Denn sonst gibt es kein Business mehr