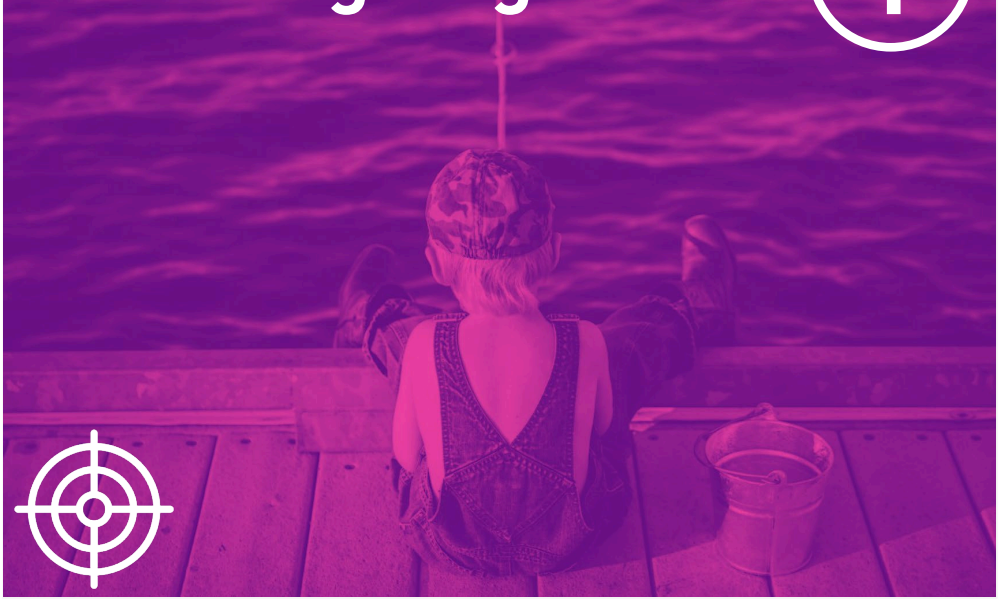
BearingPoint **Factory Defender** ist ein Kartenspiel, bei dem sich IT- bzw. OT-Security Interessierte spielerisch in die Rolle der Angreifer und Verteidiger versetzen und verschiedene Angriffskombinationen und Verteidigungsmaßnahmen ausprobieren können. Dabei wird ein produzierendes Unternehmen simuliert, welches erstmalig in Securitymaßnahmen investiert und sich plötzlich mit Angriffen konfrontiert sieht. – Fragen zum Spiel an: besecure@bearingpoint.com

Ablauf

1. Die Spieler werden zu Beginn in zwei Gruppen, die Angreifer und die Verteidiger, aufgeteilt. Die Beratung der Gruppen erfolgt heimlich, sodass die jeweils andere Gruppe die eigene Strategie nicht mitbekommt.
2. Ziel der Angreifer ist es, durch die geschickte Kombination von Angriffen, die Lebenspunkte der Verteidiger von 3 auf 0 zu reduzieren. Die Verteidiger müssen dies durch die passende Auswahl von Verteidigungsmaßnahmen verhindern.
3. Beide Gruppen haben nun 5-10 Minuten Zeit (wenn das Spiel bereits gespielt wurde und die Spieler mit den Karten vertraut sind, sollten 5 Minuten reichen) um sich für eine Kombination aus Angriffen bzw. Verteidigungsmaßnahmen zu entscheiden.
4. Die Angreifer wählen 5 Angriffskarten aus.
5. Die Verteidiger wählen Verteidigungsmaßnahmen aus, haben jedoch nur ein Budget von €50.000 zur Verfügung. Viele der Maßnahmen wirken gegen mehrere Arten von Angriffen.
6. Die beiden Gruppen kommen nun wieder zusammen und die Angreifer spielen den ersten Angriff aus. Dabei wird die Nummer des Angriffs sowie der Text vorgelesen. Die Reihenfolge der Angriffe spielt keine Rolle. Die Verteidiger geben bekannt, ob sie eine oder mehrere Verteidigungsmaßnahmen gegen den Angriff besitzen.
7. Jeder Angriff verursacht dabei entweder einen oder zwei Punkte Schaden. Jede Verteidigungsmaßnahme, die gegen den jeweiligen Angriff wirkt, reduziert den Schaden um einen Punkt. Das heißt zwei Verteidigungsmaßnahmen gegen den gleichen Angriff können auch den Schaden von z.B. 2 auf 0 Punkte reduzieren.
8. Schaffen die Angreifer es die Lebenspunkte auf 0 zu reduzieren, haben sie gewonnen. Falls nicht, haben die Verteidiger gewonnen.

Phishing Angriff

1



Dieser Angriff zielt darauf ab, Zugangsdaten oder vertrauliche Informationen von Mitarbeitern oder Zugriffe auf deren Systeme zu erlangen. Die Angreifer können nun auf Systeme oder Accounts der Verteidiger zugreifen.

Die Verteidiger verlieren **einen Punkt**.

BearingPoint®

Physical Social Engineering

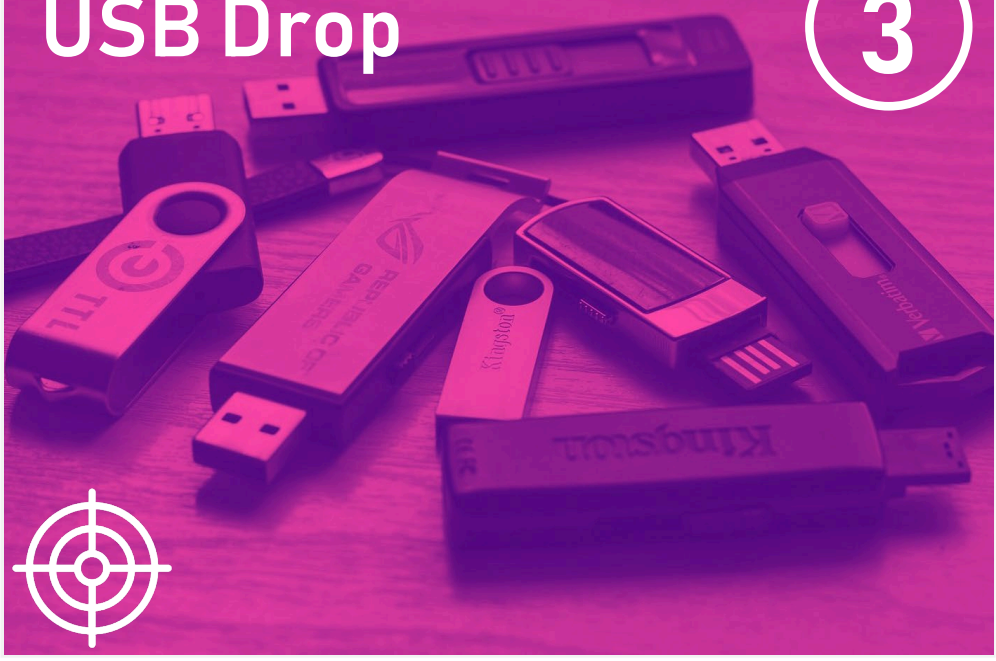
2

Dieser Angriff zielt darauf ab, physischen Zutritt zu gesperrten Bereichen zu erlangen und unbemerkt Daten zu stehlen oder Geräte oder Tools zu installieren, die später einen Fernzugriff ermöglichen. Die Angreifer haben nun Zugriff auf Daten oder Systeme der Verteidiger.

Die Verteidiger verlieren **einen Punkt**.

USB Drop

3



Bei diesem Angriff werden mit Schadsoftware vorbereitete USB Sticks in der Nähe des Ziels verteilt, in der Hoffnung, das unachtsame Mitarbeiter diese an Ihre Firmen-PCs anschließen. Die Angreifer erhalten somit Zugriff auf die Systeme der Verteidiger.

Die Verteidiger verlieren **einen Punkt**.

Ransomware

4

Eine Ransomware findet ihren Weg in das OT Netz und nutzt vorhandene Schwachstellen um sich Zugang zu kritischen Systemen zu verschaffen und diese zu verschlüsseln.

Die Verteidiger verlieren **zwei Punkte**.

Ransomware Addon: Zero Day

5

Dieser Angriff kann als Erweiterung zur Ransomware Attacke gespielt werden und zählt als ein weiterer Angriff. Zero-Day Exploits werden von signaturbasierten Erkennungsmethoden nicht erfasst (Standard Firewall).

Die Verteidiger verlieren **einen weiteren** Punkt.

WLAN Angriff

6

Bei diesem Angriff werden unzureichend abgesicherte WLANs vor Ort attackiert. Die Angreifer verschaffen sich dadurch Zugang zum Produktionsnetzwerk und vorhandene Systeme und Daten.

Die Verteidiger verlieren **einen Punkt**.

BearingPoint®

Lieferantenangriff

7

Dieser Angriff zielt darauf ab, Lieferanten des Ziels zu infiltrieren und sich über deren Wartungszugänge Zugriff auf die Zielumgebung zu verschaffen.

Die Verteidiger verlieren **einen Punkt**.

Public Service Hack

8

Dieser Angriff zielt auf öffentlich erreichbare Services, wie zum Beispiel Lieferantenportale oder VPN, ab. Die Angreifer verschaffen sich über Hacks Zugang zu den Systemen der Verteidiger.

Die Verteidiger verlieren **einen Punkt**.

BearingPoint®

SCADA Wurm

9

Der wohl berühmteste Wurm für SCADA Systeme ist Stuxnet. Diese spezialisierten Angriffe nutzen gezielt Schwachstellen in SCADA Systemen aus und verursachen Schaden.

Die Verteidiger verlieren **zwei Punkte**.

BearingPoint®

Trojaner

10

Durch das Downloaden eines Files von einer unsicheren Website wurde ein Trojaner am Ziel platziert. Die Angreifer haben nun potentiell Zugriff auf das gesamte System.

Die Verteidiger verlieren **zwei Punkte**.

BearingPoint®

Verärgerter Mitarbeiter

11

Ein gekündigter Mitarbeiter möchte sich rächen und verwendet noch aktive Remote-Zugänge um die Anlagensteuerung zu sabotieren.

Die Verteidiger verlieren **einen Punkt**.

BearingPoint®

OT Firewall

1

€ 20.000

Sandboxing: + € 5.000

Diese Maßnahme trennt das Business- vom Produktionsnetz und ermöglicht den Einsatz von Schutztechnologien. Folgende Angriffe werden dadurch um einen Punkt reduziert:

4 6 9 10

Mit dem Sandboxing Addon wird auch noch dieser Angriff um einen Punkt reduziert:

5

BearingPoint®

OT Threat Detection 2

€ 15.000

OT Threat Detection Systeme erkennen Schwachstellen und Anomalien in OT Umgebungen und erlauben so, Angriffe frühzeitig zu erkennen und womöglich zu verhindern. Folgende Angriffe werden dadurch um einen Punkt reduziert:

4 9 10 11

BearingPoint®

Mitarbeiter-schulungen

3

€ 20.000

Security Awareness Schulungen wie Phishing-Kampagnen, Information Security Trainings und regelmäßige Informationen zu aktuellen Bedrohungen helfen Mitarbeiter zu sensibilisieren und das Unternehmen zu schützen. Folgende Angriffe werden dadurch um einen Punkt reduziert:

1 2 3 10

BearingPoint®

Sicherer Fernzugriff

4

€ 10.000

Eine sichere Fernzugriffslösung ersetzt gängige Methoden wie Teamviewer, RDP oder VPN-Tunnel und ermöglicht dem Anlagenbetreiber, Zugriffe gezielt zu steuern, zu überwachen und abzusichern. Folgende Angriffe werden dadurch um einen Punkt reduziert:

7 8 11

BearingPoint®

OT Netzwerk-Segmentierung

5

€ 15.000

Netzwerksegmentierung im OT-Netz bietet dieselben Vorteile wie in der IT, nämlich eine bessere Kontrolle der Datenflüsse und verhindert, dass sich Angreifer oder Schadsoftware ungehindert ausbreiten können. Folgende Angriffe werden dadurch um einen Punkt reduziert:

4 9 10

BearingPoint®

Penetration Testing

6

€ 15.000

Durch regelmäßige Penetration Tests und simuliertes Phishing lassen sich die eigene Umgebung und Prozesse auf Schwachstellen und mögliche Angriffsstrategien überprüfen, um so frühzeitig Maßnahmen zur Erhöhung der Sicherheit setzen zu können. Folgende Angriffe werden dadurch um einen Punkt reduziert:

1 6 8

BearingPoint®

Backups und BCM

7

€ 20.000

Moderne und robuste Backup- und Restore-Lösungen sind oft die „Last Line of Defense“ und stellen sicher, dass wenn Schutzmaßnahmen nicht wirken, die betroffenen Systeme verlässlich und schnell wiederhergestellt werden können. Folgende Angriffe werden dadurch um einen Punkt reduziert:

4 5 9 10

BearingPoint®

Factory Defender

BearingPoint®

Factory Defender

BearingPoint®