TYP: CYBERANGRIFF ZIEL: ALLE	Bezugsplan **RANCOMWARE- MASSIVE NICHT VERFÜGBARKEIT VON LAPTOPS**	

1. Alarm

Feststellung des Angriffs (Notiz auf dem Desktop, Dateien und Anwendungen nicht verfügbar...)	Benachrichtigung des SOC
NICHTS LÖSCHEN: Alle Informationen werden als Beweismittel für die Ermittlungen verwendet.	**DIE BENACHRICHTIGUNG SOFORT BERÜCKSICHTIGEN**
KEINE VERSCHLÜSSELTEN DATEIEN ODER ANWENDUNGEN ÖFFNEN: Die Infektion muss gestoppt werden.	**DEM SOC ALLE INFORMATIONEN** mitteilen, um das Ausmaß des Angriffs und die Prioritäten für Notfallmaßnahmen zu bewerten
	DEN ANWEISUNGEN DER SOC FOLGEN.

2. Notfallmaßnahmen

1. **Kritische Systeme isolieren**:
   - Alle Netzwerke trennen.
   - Ziehen Sie die Netzwerkkabel von den Computern ab.
   - WLAN-Verbindungen trennen.
2. **Die Stecker aller Peripheriegeräte herausziehen**
3. Wenn Sie den Computer nicht vom Netzwerk trennen können, **schalten Sie alle WLAN-Router und -Hotspots aus**
4. Das Ausmaß der Kompromittierung einschätzen und **Beweise sammeln**

3. Lösung für die Kontinuität

Bereitstellung einer virtualisierten Arbeitsumgebung, auf die vom Internet aus über jeden beliebigen Arbeitsplatzrechner in der Reihenfolge der Kritikalität der Aktivitäten zugegriffen werden kann.

4. Kriterium für die Aktivierung der Kontinuitätslösung.

Der entscheidungsbefugte Krisenstab trifft die endgültige Entscheidung über die Aktivierung der BCP.

Kriterium 1: 5% der Laptops sind unbrauchbar.

TYP: CYBERANGRIFF ZIEL: ALLE	Bezugsplan **RANCOMWARE- MASSIVE NICHT VERFÜGBARKEIT VON LAPTOPS**	

Kriterium 2: Risiko, dass sich die Ransomware auf andere Standorte/Einheiten/Anwendungen ausbreitet.