Vorfallsmeldung Checkliste

1. Wer ruft an?
- Name:
- Zeit, Datum:
- Rückrufnummer:

2. Wann fand der Vorfall statt?

3. Wie wurde der Vorfall entdeckt? Wann? Durch wen?

4. Unmittelbare und zukünftige Auswirkungen auf den Anwender oder das Unternehmen?

5. Betroffene Systeme:
- Hardware / Software / Betriebssystem
- IP-Adresse oder Netzwerk des betroffenen Systems
- Netzwerktyp (Ethernet, Token Ring, ATM)
- Modem (Telefonnummer)
- Kritikalität für Geschäftsprozess oder Unternehmen
- Befinden sich kritische Informationen auf dem System?
- Physische Standort
- Physische Schutzmaßnahmen vorhanden?
- Wer ist Hauptuser / Hauptadministrator? Kontaktdaten
- In welchem Zustand befindet sich das System

6. Angreifer:
- Angreifer aktiv?
- Quell-Adresse
- Anzeichen für DoS?
- Anzeichen für Vandalismus?
- Erste Vermutung über Angreifer eines Insiders oder Outsiders

7. vorgenommen Tätigkeiten:
- Netzwerkstecker gezogen?
- Audit Logfiles analysiert?
- Remote oder lokaler Zugriff auf die Systeme möglich?
- Änderungen am Netzwerk, Firewalls etc.?
- Wer wurde informiert? (intern / extern)

8. Welche Werkzeuge sind vor Ort verfügbar:
- Ist irgendwelche Systemaudit-Software bereits im Einsatz?
- Netzwerkprotokolle
- Sniffer im Einsatz?

9. Wer kann für weitere Informationen angerufen werden:
- Systemanwender?
- Systemadministrator des betroffenen Systems
- Lokaler Netzwerkadministrator

10. Sonderwünsche:
- Wer soll im Unternehmen NICHT kontaktiert werden?
- [...]