Merkblatt zum IT-Grundschutz für Rechner von Gästen im Forschungszentrum

Die vom Vorstand beschlossene IT-Sicherheitsrichtlinie (http://intranet.fz-juelich.de/goto?id=985162) des Forschungszentrums verpflichtet die Betreiber und Nutzer aller Rechner und sonstiger IT-Systeme im Forschungszentrum dazu, Ihren Beitrag zu dem wichtigen Ziel zu leisten, eine angemessene IT-Sicherheit zu gewährleisten. Dazu gehört insbesondere die Beachtung der IT-Sicherheitsregeln für den Grundschutz (http://intranet.fz-juelich.de/goto?id=985172). Dies gilt auch für Rechner von Gästen, die am JuNet teilnehmen. Dieses Merkblatt fasst die für diese Gruppe besonders wichtigen Regelungen zusammen, um Gästen den Einstieg zu erleichtern. Es kann und soll jedoch in keinem Fall die IT-Grundschutzregeln ersetzen.

1. Anschluss ans JuNet

1.1 Anmeldung

Jeder Rechner muss beim JSC angemeldet (https://junet-portal.fz-juelich.de/cgi-bin/public/start_junet.cgi) werden und einen benannten Administrator haben, der Mitarbeiter des Forschungszentrums ist, und der eine Selbsterklärung zu den IT-Sicherheitsregeln für den Grundschutz abgegeben hat.

1.2 Sicherheitscheck

Vor Anschluss des Rechners an das JuNet muss der Sicherheitszustand überprüft werden (aktuelle Patches, Virenscanner, Viren-Freiheit). Der Check umfasst:

- das Betriebssystem „netzsicher“ machen (Mindestanforderung an Patchlevel)
- sofern nicht vorhanden: automatisch aktualisierenden Virenscanner installieren
- Windows- und soweit möglich auch Linux-Systeme durch Online-Update aktualisieren

2. Konfiguration der Systeme:

2.1 Passwortschutz und Zugang

Alle Benutzerumgebungen auf dem Rechner müssen durch ein nicht-triviales Passwort geschützt sein. Privilegierte Benutzerumgebungen (Administrator, root) dürfen nur mit starker Verschlüsselung (z.B. ssh) über Netze zugänglich sein.

2.2 Betriebssystem und Anwendungen

Die Sicherheitseinstellungen, die Betriebssystem und Anwendungen bieten, sollten genutzt werden (z.B. Personal Firewalls, sichere Konfiguration von Web-Browsern und Email-Clients)

2.3 Netzwerk-Konfiguration

Der Rechner muss so konfiguriert sein, dass er nicht gleichzeitig in JuNet und W-JuNet kommuniziert (und so einen Nebenpfad ins JuNet eröffnen würde).

3. Weitere Verhaltensregeln

3.1 Vorsicht

Bewegen Sie sich mit der gebotenen Vorsicht im Netz: Öffnen Sie keine Email-Anhänge von unbekannten Absendern; denken Sie daran, dass Email-Absender-Adressen leicht zu fälschen sind; installieren Sie keine Software aus unbekannten oder zweifelhaften Quellen; vermeiden Sie den Besuch von Web-Seiten mit zweifelhaftem Inhalt.

3.2 Im Notfall

Bei Verdacht auf eine Kompromittierung (Viren-Befall, Hacker-Einbruch) sollte grundsätzlich vor jeder anderen Maßnahme unverzüglich das FZJ-CERT telefonisch informiert werden: 02461 / 61 – 6440. Nur so können umgehend eventuell notwendige Gegenmaßnahmen eingeleitet und möglicherweise größerer Schaden für das Forschungszentrum abgewendet werden. Nach Kontaktaufnahme und Vorabklärung des Sachverhalts wird das FZJ-CERT sie um weitere Informationen zum kompromittierten System bitten. Bitte sammeln Sie diese Information nicht vorab selbst, sondern informieren stets zunächst das FZJ-CERT.

FZJ-CERT, Oktober 2017