ausecus.

Penetrationstests für Leittechnik & Kritische Infrastrukturen

Technische Schwachstellen und Sicherheitslücken

www.ausecus.com

VORGEHENSWEISE BEI KRITISCHEN INFRASTRUKTUREN

1. Vorbereitung und Planung

- Rahmenbedingungen festlegen
- Vereinbarungen (z.B. zur Vertraulichkeit)
- Erarbeitung und individuelle Abstimmung der Test- und Angriffsmethodik

2. Testdurchführung

- Stets kontrolliertes Vorgehen zum Schutz Ihrer Systeme und Anlagen
- Informationsbeschaffung und Eindringversuche
- Gewährleisten der Integrität Ihrer Systeme und Anlagen
- Analyse und Verifikation der Ergebnisse

3. Ergebnisbericht

- Übersichtliches Management-Summary
- Detailliert aufbereitete Dokumentation
- Bewertung und Einordnung der gefundenen Schwachstellen
- Aufzeigen von praktikablen Gegenmaßnahmen und individuellen Handlungsempfehlungen

ausecus.

KONTAKT

Erfahrung aus der Praxis

Unsere Mitarbeiter bringen langjährige Erfahrung mit ISMS und aus der IT-Sicherheit Leittechnik bei Energieversorgern, Stadtwerken und in der Industrie mit.

Durch unser herstellerübergreifendes Wissen und pragmatisches Denken sorgen wir dafür, dass die Schwerpunkte der IT-Sicherheit und Ihres ISMS-Projektes an den richtigen Stellen gesetzt werden und die Durchführung möglichst effizient und zielgerichtet ist.

ausecus GmbH
Werner-von-Siemens-Straße 6
D-86159 Augsburg
Tel. +49 / 821 / 20 70 97 - 0
Fax +49 / 821 / 20 70 97 - 99
info@ausecus.com
www.ausecus.com

Penetrationstests für Kritische Infrastrukturen

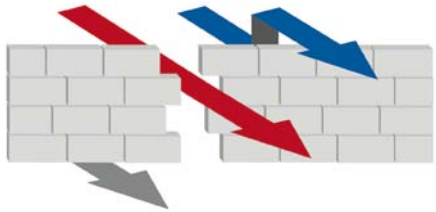
Die Angriffsmuster bei den größten IT-Sicherheitsvorfällen in Kritischen Infrastrukturen zeigen, dass neben Social Engineering auch eine Vielzahl technischer Schwachstellen ausgenutzt wurde. Um einen proaktiven Schutz zu gewährleisten und den Anforderungen aus ISO/IEC 27001/-02 und 27019 gerecht zu werden, sollten diese Schwachstellen im Rahmen von Penetrationstests aufgedeckt und anschließend geschlossen werden.

Für Betreiber Kritischer Infrastrukturen ist dieses Vorgehen essentiell bei der Prävention von IT-Angriffen. Bei einem Penetrationstest finden unsere IT-Sicherheitsexperten Netzwerk- und Systemschwachstellen. Als Penetrationstester analysieren wir technische Schwachstellen in der Infrastruktur, in den Leit- und Prozesssteuerungssystemen und in der eingesetzten Automatisierungstechnik.

Wir dokumentieren die Ergebnisse während den Tests akribisch und stellen Ihnen neben einem übersichtlichen Management Summary die komplette Dokumentation zur Verfügung. Im Anschluss daran erarbeiten wir mit Ihnen gemeinsam weitergehende und für Sie individuell geeignete Schutzmaßnahmen.

Penetrationstests in Leit-, Fernwirk- und Automatisierungstechnik

Im Rahmen eines Penetrationstests erhalten unsere IT-Sicherheitsexperten Informationen über potentiell vorhandene Schwachstellen in den Komponenten des Netzwerks. Diese Schwachstellen werden priorisiert und nach ihrer Kritikalität bewertet. Anhand der Bewertungen kann dann entschieden werden, welche der vorhandenen Schwachstellen den größten Erfolg für einen Eindringversuch versprechen und welche damit im Angriffsfall konkret ausgenutzt werden würden.



Ein Angreifer würde im Anschluss diese Schwachstellen ausnutzen, um in das System einzudringen. Da jeder „Exploit", also das Ausnutzen einer Schwachstelle, mit einer Ausfallgefährdung der Systeme einhergeht, nutzen unsere IT-Sicherheitsexperten diese Mittel nicht automatisch. Bei Schwachstellen, die sich nur so verifizieren lassen, sprechen wir das Ausführen des „Exploits" mit Ihnen ab. Eine Durchführung kann dann beispielsweise in einer kontrollierten Testumgebung stattfinden.

Die Gefährdung des Gesamtsystems bleibt dadurch beherrschbar und es kann trotzdem eine fundierte Aussage über die System- und Netzwerksicherheit getroffen werden. Unsere hervorragend ausgebildeten Netzwerksicherheitsexperten können durch ihr Praxiswissen gewährleisten, dass der Test immer sicher und im abgesprochenen Rahmen stattfindet.

White-Box-Test
Eine bewährte und effektive Methode

Durch unsere langjährige Erfahrung bei Energie- und Wasserversorgern, Stadtwerken, Erzeugungsanlagen, Entsorgungsanlagen und in der Prozessleittechnik können wir gefundene Schwachstellen genau bewerten und ihre Bedeutung in der Praxis einschätzen.

Unsere IT-Sicherheitsexperten arbeiten in jedem Fall praktikable und effiziente Gegenmaßnahmenvorschläge für Sie aus. Gerne begleiten unsere Experten Sie auch bei der Umsetzung der Gegenmaßnahmen in Ihren Netzwerken, Firewalls oder an Ihren Systemen.

Diese Vorgehensweise als sogenannter **White-Box-Test** hat sich in der Praxis über Jahre hinweg bewährt. Sie als Betreiber haben damit die Möglichkeit, mit geringem Zeitaufwand eine tiefgreifende technische Sicherheitsprüfung Ihrer Systeme und Netzwerke durchzuführen – und das bei beherrschbaren Risiken.