

Cyber-Kontrolle

00

Cyber-Sicherheit-BRD

Selbst-Test

Prüf-Programme

Innen Verteidigung Justiz

Die Welt der Hacker Spione und Opfer in Gesellschaft Wirtschaft Verwaltung Bildung

BSI Cert Cyber-Abwehr-Centrum

Org-Welt

Rechts-Rahmen nach DSGVO

Netze : Heim Firmen Behörden Kritis

Endpoint-Security

BS W- 10

Snort

APP/SW

Bordmittel

Endpoint

VIRUS

Pflege

Tuning

Wartung

WER ?

Rauf auf die

Datenautobahn

Send-Home

Ziel



9

BIG-DATA

Farm/Center

Server

App

Shop

WWW

Mail

Was ist los im Netz

WS und Server

Schauen

Diagnose

netstat

PORT

Prevention

Sniffen

Snort

Ethereal

Auswerten

Wireshark

Mengenproblem

Was soll nicht sein

Netzdoku

Report lesen

Admin-Tools

Beobachten

SW

SW

ISP

LOG

IP-Adress

AUTO

Täter

Threat

Firewall

Mail

Browser

Social-E

DF-REPORT

Jeder User ist ein Admin-PC

Blick auf das Netz

1

bis

100 000

Spuren-Welt

Digitale Spuren

Forensik

Achtung send Home--Innentäter

Digitaler Forensikreport fehlt. Angriff, Methode, Werkzeug, Tools

BKA-Statistik

Detection

Investigate or destroy

Zeigt die Täter auf

Prevention

Ziel: Quelle Ausser Betrieb nehmen Dem Hacker ein Gesicht geben

Author: Werner Gugetzer 0519 Europapc.de

Cyber-Fahndung