

# Projekthistorie

---

## 05/2016 – 07/2016

Mitarbeiterschulung im Bereich IT-Sicherheit	
Branche	Pharmazeutischer Großhandel
Aufgabengebiet	<ul style="list-style-type: none"><li>Mitarbeiterschulung im Bereich IT-Sicherheit mit Schwerpunkt "Umgang mit E-Mail und Schutz vor Ransomware"</li></ul>
Funktion	Security Consultant

Unterstützung nach Befall durch Ransomware bzw. Beratung zur zukünftigen Prävention	
Branche	Pharmazeutischer Großhandel
Aufgabengebiet	<ul style="list-style-type: none"><li>Unterstützung nach Befall durch Ransomware</li><li>Beratung zum Schutz vor Ransomware und der zukünftigen Prävention</li></ul>
Funktion	Security Consultant

Penetration Test einer IT-Infrastruktur	
Branche	Anstalt des öffentlichen Rechts
Aufgabengebiet	<ul style="list-style-type: none"><li>Penetration Test einer IT-Infrastruktur (Systemanzahl &gt;50)</li></ul>
Funktion	Penetration Tester

## 02/2016 – 03/2016

Sicherheitsüberprüfung einer Kundenwebseite und Analyse nach einem Hacking-Angriff	
Branche	Anstalt des öffentlichen Rechts
Aufgabengebiet	<ul style="list-style-type: none"><li>Prüfung der Kundenwebseite auf Sicherheitslücken</li><li>Analyse der Daten auf einen möglichen Hacking-Angriff</li></ul>
Funktion	Penetration Tester

## 05/2015 – bis heute

Implementierung einer "Check Point 4200 Appliance - Next Generation Threat Prevention (NGTP)"	
Branche	Internet Branche

Aufgabengebiet	<ul style="list-style-type: none"> <li>• Austausch einer vorhandenen Firewall durch einen „Check Point 4200 Appliance Next Generation Threat Prevention (NGTP)“-Cluster auf Basis von R77.20.</li> <li>• Implementierung Check Point Security Management Smart-1 Appliance</li> <li>• Einrichtung der Software-Blades (Firewall/VPN/Intrusion Prevention)</li> </ul>
Funktion	Security Consultant

### **02/2015 – bis heute**

<b>Sicherheitsüberprüfung / Penetration Test einer Netzwerkinfrastruktur</b>	
Branche	Internet Branche
Aufgabengebiet	Prüfung der Netzwerkinfrastruktur und Webapplikationen auf Sicherheitsprobleme (Serveranzahl >100)
Funktion	Security Consultant / Penetration Tester

### **01/2015 – bis heute**

<b>Chief Security Officer</b>	
Branche	Domain Registrar
Aufgabengebiet	Verantwortlich für die IT-Sicherheit im Unternehmen
Funktion	Chief Security Officer

### **08/2014 - 09/2014**

<b>Sicherheitsüberprüfung einer Kundenwebseite auf Sicherheitslücken</b>	
Branche	Juwelier
Aufgabengebiet	Prüfung der Kundenwebseite / des Online-Shops auf Sicherheitslücken
Funktion	Penetration Tester

<b>Sicherheitsüberprüfung einer Kundenwebseite auf Sicherheitslücken</b>	
Branche	Lebensmittelbranche
Aufgabengebiet	Prüfung der Kundenwebseite auf Sicherheitslücken und Erstellung der Dokumentation
Funktion	Penetration Tester

**Implementierung einer "Check Point 4200 Appliance Next Generation Threat Prevention (NGTP)"**

Branche	Bildungseinrichtung
Aufgabengebiet	<ul style="list-style-type: none"><li>• Planung und Durchführung des Austausches der vorhandenen Firewall durch eine „Check Point 4200 Appliance Next Generation Threat Prevention (NGTP)“ (auf R77.20).</li><li>• Migration der vorhandenen Firewall-Regeln</li><li>• Einrichtung der Software-Blades (Intrusion Prevention, AntiBot etc.)</li></ul>
Funktion	Security Consultant

**06/2014 - 07/2014****Forensische Analyse von Logdateien auf Kommunikation von Schadsoftware**

Branche	Bildungseinrichtung
Aufgabengebiet	Unterstützung des Kunden bei der Analyse auf Schadsoftware im internen Netzwerk
Funktion	Computer-Forensiker

**04/2014 - 05/2014****Penetration Testing**

Branche	Lebensmittelbranche
Aufgabengebiet	Prüfung der Kundenwebseite auf Sicherheitslücken und Erstellung der Dokumentation
Funktion	IT-Sachverständiger / Penetration Tester

**02/2014 - 05/2014****Forensische Analyse von Logdateien nach einem Sicherheitsvorfall**

Branche	Öffentlicher Dienst
Aufgabengebiet	Unterstützung eines Kunden nach der Entdeckung von externen Angreifern im internen Netzwerk, bei der Analyse des Angriffs und der Dokumentation
Funktion	Computer-Forensiker / Security Consultant

**10/2012 - 01/2014****Gerichtsverwertbare Gutachten für die Strafverfolgungsbehörden**

Branche	Behörde
---------	---------

Aufgabengebiet	Erstellung von gerichtsverwertbaren Gutachten für die Strafverfolgungsbehörden
Funktion	Computer-Forensiker / Gutachter

<b>Forensische Analyse nach einem Sicherheitsvorfall</b>	
Branche	Forschung / Entwicklung
Aufgabengebiet	Unterstützung eines Kunden, nach der Entdeckung von externen Angreifern im internen Netzwerk, bei der Analyse des Angriffs und der Dokumentation
Funktion	Computer-Forensiker / Security Specialist

### 04/2012 - 09/2012

<b>Penetration Testing</b>	
Branche	Energieversorger
Aufgabengebiet	Prüfung der Kundenwebseite auf Sicherheitslücken
Funktion	Security Consultant Industrial-IT

<b>Implementierung Industrial Defender / Cisco-Switches</b>	
Branche	Energieversorger
Aufgabengebiet	Planung & Implementierung einer Industrial Defender IT-Security Infrastruktur für kritische Infrastrukturen und Konfiguration der betroffenen Switches und Interfaces
Funktion	Security Consultant Industrial-IT

<b>Durchführung einer Schulung im Bereich IT-Sicherheit</b>	
Branche	Energieversorger
Aufgabengebiet	IT-Security Schulung mit dem Thema "Konfiguration eines Astaro Security Gateway"
Funktion	Security Consultant Industrial-IT

<b>Durchführung einer Schulung im Bereich IT-Sicherheit</b>	
Branche	Energieversorger
Aufgabengebiet	IT-Security Schulung für Endanwender mit dem Schwerpunkt Live-Hacking / Penetration Testing inkl. Aufbau der Live-Hacking Umgebung
Funktion	Security Consultant Industrial-IT

<b>Penetration Testing</b>	
Branche	IT-Dienstleister

Aufgabengebiet	Suche nach Schwachstellen in Webanwendungen und Veröffentlichung der Security Advisories
Funktion	Security Consultant Industrial-IT

**01/2007 - 03/2012**

<b>Forensische Analyse nach einem Sicherheitsvorfall</b>	
Branche	Sonstiges
Aufgabengebiet	Forensische Analyse von Kundensystemen wegen dem Verdacht des Ausspähenes von Daten durch interne Mitarbeiter
Funktion	Security Consultant

<b>Betreuung der internen IT-Security Infrastruktur</b>	
Branche	Internet Service Provider
Aufgabengebiet	Betreuung der internen IT-Security Infrastruktur: <ul style="list-style-type: none"> <li>• Administration mehrere Check Point Security Gateways (Cluster)</li> <li>• Administration der firmeneigenen Intrusion Detection / Prevention Systeme von Tipping Point und Check Point</li> <li>• Administration der firmeneigenen Blue Coat Proxy SG und Blue Coat ProxyAV Systeme</li> </ul>
Funktion	Security Consultant

<b>Penetration Testing</b>	
Branche	Handel
Aufgabengebiet	Prüfung der Kundenwebseite und des Online-Shops auf Sicherheitslücken.
Funktion	Security Consultant

<b>Penetration Testing</b>	
Branche	Baugewerbe
Aufgabengebiet	Durchführung eines Penetration Test (Extern/Intern) auf die gesamte IT-Infrastruktur des Kunden, sowie eine Prüfung des Firewall-Regelwerks, der internen Backup-Strategie und internen IT-Vorschriften (mit Blick auf die IT-Sicherheit)
Funktion	Security Consultant

<b>Penetration Testing</b>	
Branche	IT-Dienstleister
Aufgabengebiet	Durchführung eines Penetration Test (Extern) für die gesamte IT-Infrastruktur
Funktion	Security Consultant

<b>Penetration Testing</b>	
Branche	IT-Dienstleister (ISP)
Aufgabengebiet	Regelmäßige Durchführung eines Penetration Test (Extern/Intern) für die gesamte IT-Infrastruktur
Funktion	Security Consultant

<b>Betreuung einer Kunden IT-Security Infrastruktur</b>	
Branche	Automobilindustrie
Aufgabengebiet	Betreuung der IT-Security Infrastruktur mit Check Point Security Gateways (Cluster), Blue Coat ProxySG
Funktion	Security Consultant

<b>Betreuung einer Kunden IT-Security Infrastruktur</b>	
Branche	Automobilindustrie
Aufgabengebiet	Betreuung der IT-Security Infrastruktur mit Check Point Security Gateways (Cluster), Blue Coat ProxySG und Blue Coat ProxyAV
Funktion	Security Consultant

<b>Betreuung einer Kunden IT-Security Infrastruktur</b>	
Branche	Gesundheitswesen
Aufgabengebiet	Betreuung der kundeneigenen Check Point Security Gateways (Cluster), der Intrusion Detection / Prevention Systeme von Tipping Point und Check Point, Blue Coat ProxySG und Blue Coat ProxyAV Systeme
Funktion	Security Consultant

<b>Betreuung einer Kunden IT-Security Infrastruktur</b>	
Branche	Berufsakademie
Aufgabengebiet	Administration und Betreuung eines Check Point Security Gateway
Funktion	Security Consultant

<b>Migration Kunden-Firewalls</b>	
Branche	Handel
Aufgabengebiet	<ul style="list-style-type: none"> <li>• Migration einer FreeBSD-Firewall zu einer Linux-Firewall mit iptables, carp (Ausfallsicherheit) und Squid-Proxy</li> <li>• Betreuung der Firewall und des Proxy nach der Migration</li> </ul>
Funktion	Security Consultant

<b>Nagios Netzwerk-Monitoring</b>	
Branche	Internet Service Provider
Aufgabengebiet	Implementierung und Betreuung einer Netzwerkmonitoring-Infrastruktur für mehrere hundert ISP-Dienste und Systeme
Funktion	Systemadministrator

<b>Betreuung einer Kunden Infrastruktur inkl. der IT-Sicherheit</b>	
Branche	Automobil-Industrie
Aufgabengebiet	Betreuung der (IT-Security) Infrastruktur mit Linux Firewalls / Linux-Servern und VPN-Verbindungen auf Basis von OpenVPN.
Funktion	Systemadministrator / Security Consultant

<b>Penetration Testing</b>	
Branche	IT-Dienstleister (ISP)
Aufgabengebiet	Suche nach Schwachstellen in Webanwendungen und Veröffentlichung der Security Advisories
Funktion	Security Consultant

<b>Administration unterschiedlicher Linux-Webserver</b>	
Branche	Internet Service Provider
Aufgabengebiet	Installation, Betreuung und Pflege, sowohl der firmeneigenen, als auch der Kunden Webserver
Funktion	Systemadministrator



<b>Planung, Aufbau und Wartung des internen Firmennetzwerkes</b>	
Branche	IT-Dienstleister
Aufgabengebiet	<ul style="list-style-type: none"> <li>• Installation einer Windows Server 2003 Root &amp; Sub-Domäne mit vier Domaincontrollern</li> <li>• Integration Microsoft Exchange Server 2003</li> <li>• Spam &amp; Virenschutz für das Firmennetzwerk per „postfix“, „amavisd“, „SpamAssassin“ und ClamAV als SMTP-Relay in einer DMZ (Debian Linux)</li> <li>• Internet Zugang für Mitarbeiter über transparenten Proxy (pf/Squid mit OpenBSD 3.7)</li> <li>• VPN-Zugang für Mitarbeiter über Hardware Router ZyXEL ZyWall 100</li> <li>• Installation eines Apache Webserver als Reverse Proxy für sicheren Zugriff auf interne E-Mails über Outlook Web Access</li> <li>• Installation Apache Webserver für interne Webentwicklung</li> <li>• Datensicherung (Backup-to-Disk, DFS, Bandsicherung)</li> <li>• Zentraler Virenschutz (McAfee AntiVirus Software)</li> <li>• Zentrale Überwachung des Netzwerks mittels Nagios und eines zentralen Syslogd-Servers</li> </ul>
Funktion	EDV-Servicetechniker

<b>Migration eines NT4.0 / Windows 2000 Server / Lotus Notes Netzwerkes</b>	
Branche	Anwaltskanzlei (Frankreich)
Aufgabengebiet	<ul style="list-style-type: none"> <li>• Umstellung auf drei Windows Small Business Server 2003</li> <li>• Bereitstellung von Terminaldiensten und VPN für externe Mitarbeiter</li> <li>• Einrichtung des Hardware Router ZyXEL ZyWall 100</li> <li>• Fileserver für Digitales Diktieren (DictaNet &amp; Dragon NaturallySpeaking)</li> </ul>
Funktion	EDV-Servicetechniker

<b>Installation Windows 2003 Server</b>	
Branche	Anwaltskanzlei (Zweigstelle/Frankreich)
Aufgabengebiet	<ul style="list-style-type: none"> <li>• Installation eines Windows 2003 Server als Fileserver</li> <li>• VPN-Verbindung zur Hauptstelle (Site-to-Site-VPN)</li> <li>• Backuplösung mit BrightStor ARCserve</li> </ul>
Funktion	EDV-Servicetechniker

<b>Einrichtung eines sicheren Homeoffice</b>	
Branche	Arztpraxis
Aufgabengebiet	Einrichten eines sicheren Homeoffice für die Mitarbeiter
Funktion	EDV-Servicetechniker

### 12/2004 - 07/2005

<b>Einrichtung eines sicheren Homeoffice</b>	
Branche	IT-Dienstleister
Aufgabengebiet	Einrichten eines IPSec-VPN mit der auf FreeBSD basierenden Firewall Komplettlösung „mOn0wall“
Funktion	EDV-Servicetechniker

<b>Administration verschiedener Linux-Webserver</b>	
Branche	IT-Dienstleister
Aufgabengebiet	Installation, Betreuung und Pflege, sowohl der firmeneigenen, als auch der Kunden Webserver (Debian)
Funktion	EDV-Servicetechniker

### 10/2003 - 05/2004

<b>Migration eines NT4.0 / Novell-Netzwerks nach Windows 2000</b>	
Branche	Transport- und Logistik
Aufgabengebiet	<ul style="list-style-type: none"> <li>• Umstellung auf Windows 2000 Server und Debian Linux,</li> <li>• Umstellung der ca. 20 Clients von Windows95/98 auf Windows 2000 Professional</li> <li>• Integration eines zentralen Virenschutzes mit Norton Antivirus Corporate Edition</li> <li>• Backuptlösung mit Veritas Backup Exec 9.0</li> <li>• Pflege und Betreuung des Netzwerkes</li> <li>• Kundensupport</li> </ul>
Funktion	EDV-Servicetechniker

<b>Einrichtung eines sicheren Homeoffice</b>	
Branche	Spedition
Aufgabengebiet	<ul style="list-style-type: none"> <li>• Einrichten eines L2TP-VPN mit Windows 2000 Server</li> <li>• Linux Firewall / Router</li> <li>• Pflege und Betreuung des Netzwerkes</li> </ul>
Funktion	EDV-Servicetechniker

### **Betreuung des internen Netzwerkes**

Branche	IT-Dienstleister
Aufgabengebiet	<ul style="list-style-type: none"> <li>• Installation Windows Server 2003 Standard Edition</li> <li>• Installation Microsoft Exchange Server 2003</li> <li>• Linux Firewall / Router Installation und Konfiguration (Debian)</li> <li>• Konfiguration der Firewall mit iptables</li> <li>• Zentrale Überwachung der Webserver und des Netzwerkes mit Nagios</li> </ul>
Funktion	EDV-Servicetechniker

<b>Administration verschiedener Linux-Webserver</b>	
Branche	Internet Service Provider
Aufgabengebiet	Installation, Betreuung und Pflege, sowohl der firmeneigenen, als auch der Kunden Webserver (Debian / Gentoo)
Funktion	EDV-Servicetechniker