Der IT-Sicherheits-Check! für Ihr Unternehmen

SECUREPOINT SECURITY SOLUTIONS

Was tun und wie es funktioniert: 15 Minuten für Ihre Sicherheit!

IT-Sicherheit ist ein komplexes Thema für Unternehmen – heute mehr denn je!

In 15 Minuten gibt Ihnen diese Broschüre einen Überblick über den Sicherheitszustand Ihres Unternehmens und fasst die aktuell wichtigen Themen im Bereich IT-Security klar und verständlich zusammen.
Gleichzeitig erhalten Sie einen Projektleitfaden, um Ihr Unternehmen optimal zu schützen und rechtssicher aufzustellen.

Wussten Sie...

... dass Sie gegenüber Dritten mit Bußgeldern bis zu 250.000 Euro haften und dies sogar trotz GmbH-Firmierung mit Ihrem Privatvermögen! Zusätzlich können weitere Schadenersatzforderungen auf Sie zukommen!

Wenn Sie jemandem (auch unbewusst/unbeabsichtigt) Schaden zufügen:
- Bundesdatenschutzgesetz (BDSG)
- Telekommunikationsgesetz (TKG)
- GmbH-Gesetz (GmbHG),
- Aktiengesetz (AktG),
- Steuerberatungsgesetz (StBerG),
- Wirtschaftsprüferordnung (WiPrO)

... dass ein Datenschutzbeauftragter schon bei unter 20 Angestellten Pflicht für Sie ist, wenn Sie personenbezogene Daten geschäftsmäßig elektronisch zur Übermittlung verarbeiten!

Laut Bundesdatenschutzgesetz (BDSG) muss jede Firma, auch unter 20 Angestellten (z. B. Ärzte, Steuerberater, Rechtsanwälte…) einen Datenschutzbeauftragten bestellen, wenn personenbezogene Daten geschäftsmäßig elektronisch zur Übermittlung verarbeitet werden.

... dass es Haftstrafen und Bußgelder für die Verbreitung von oder Zugang zu illegalen Daten (Kinderpornografie, Rassismus...) gibt.

Wenn Ihre Computer von Fremden mittels Trojaner/Bots benutzt werden, können Sie mit Haftstrafen und weiteren Folgen rechnen: Strafgesetzbuch (StGB) §184b und Jugendschutzgesetze.

... dass Sie Schadenersatz für die Bereitstellung und Verbreitung illegaler Raubkopien (Musik, Software...) leisten müssen.

Ein Verstoß gegen das Urheberrecht kann teuer werden. Wenn Azubis oder Angestellte – auch versehentlich und ohne Ihre Kenntnis – illegal Musikdateien, Filme, Software etc. aus dem Internet laden, können Sie haftbar gemacht werden.

... dass es Pflicht wird, Verbindungsdaten zu speichern, denn EU-Gesetze zur Vorratsdatenspeicherung werden in Kürze in Deutschland umgesetzt.

EU-Gesetze zur Vorratsdatenspeicherung: Dies betrifft vor allen Dingen alle Provider und Betreiber von Kunden-WLANs (Flughäfen, Hotels, Gaststätten…)

... dass personenbezogene Log-Daten nicht so einfach zum Nachweis von Taten verwendet werden dürfen:

Betriebsverfassungsgesetz, Arbeitsrecht und Vier-Augen-Prinzip: Nur ein Datenschutzbeauftragter und Administrator dürfen gemeinsam auf personenbezogene Log-Daten zugreifen. Die Daten müssen verschlüsselt sein oder es muss eine unterschriebene Betriebsvereinbarung vorliegen.

... dass Sie auch dann haften, wenn:

- kein Mitwissen Ihrerseits vorliegt,
- Mitarbeiter fahrlässig handelten oder einfach etwas ausprobieren wollten,
- Dritte Ihre EDV mittels Trojaner/Bots ohne Ihre Zustimmung benutzen,
- Sie nicht Ihrer Nachweispflicht nachgekommen sind,
- Sie keinen verantwortlichen **Datenschutzbeauftragten** schriftlich bestellt haben
- und Sie keine geeigneten technischen IT-Schutzmaßnahmen durchführen!

Analyse der IT-Sicherheit!

1 Strategische Sicherheit Bitte beantworten Sie nun die folgenden Fragen:	**Antwort:** ja	nein	Notizen
Hat die Geschäftsführung die IT-Sicherheitsziele formuliert und sich zu ihrer Verantwortung für die IT-Sicherheit bekannt? Dazu zählen:			
• Besteht eine aktuelle, fortlaufende Dokumentation über die wichtigen Anwendungen und IT-Systeme, deren Schutzbedarf und Risiko-Einschätzung?	☐	☐	Mindestens einmal jährlich sollten alle IT-Schutzmaßnahmen definiert und überprüft werden. Neben der allgemeinen Sicherheit für Ihr Unternehmen, wird das bzgl. Basel II und III als Softfact auch Ihre Unternehmensbilanz bei der Bank verbessern. Weisen Sie die Bank im Bilanzgespräch darauf hin!
• Gibt es ein dokumentiertes IT-Sicherheitskonzept, bestehend aus einem Handlungsplan, der Sicherheitsziele definiert, priorisiert und die Umsetzung der Sicherheitsmaßnahmen regelt?	☐	☐	
• Gibt es Checklisten dafür, was beim Eintritt neuer Mitarbeiter und beim Austritt von Mitarbeitern zu beachten ist (Berechtigungen, Schlüssel, Passwörter, Unterweisungen, Arbeitsanweisungen)?	☐	☐	
• Werden Mitarbeiter regelmäßig zu sicherheitsrelevanten Themen geschult?	☐	☐	Ihre Mitarbeiter müssen wissen, was IT-Security bedeutet und was Sie im Unternehmen durchsetzen wollen.
• Gibt es personelle und technische Maßnahmen zur Erhöhung des Sicherheitsbewusstseins der Mitarbeiter?	☐	☐	
• Sind für alle IT-Sicherheitsmaßnahmen Zuständigkeiten und Verantwortlichkeiten festgelegt? Vertretungsregelungen?	☐	☐	
• Sind die bestehenden Richtlinien und Zuständigkeiten allen Mitarbeitern bekannt und können diese jederzeit auf diese Dokumentation zugreifen?	☐	☐	
• Ist ein IT-Sicherheitsbeauftragter/Datenschutzbeauftragter[1] schriftlich benannt worden und ist dieser qualifiziert?	☐	☐	Achtung: Auch bei Unternehmen <20 Mitarbeiter ist bei der elektronische Verarbeitung personenbezogener Daten zum Zweck der Übermittlung ein Datenschutzbeauftragter notwendig.
• Gibt es einen schriftlichen Risiko-Plan, um auch bei EDV-Ausfällen arbeiten zu können?	☐	☐	
• Wird die Wirksamkeit von IT-Sicherheitsmaßnahmen[2] regelmäßig überprüft?	☐	☐	
• Sind und werden gesetzliche und/oder vertragsrechtliche Gesichtspunkte in der unternehmensweiten IT-Sicherheit berücksichtigt?	☐	☐	
• Werden IT-Sicherheitserfordernisse bei allen Projekten frühzeitig berücksichtigt (z. B. bei Planung eines neuen Netzes, Neuanschaffung von IT-Systemen und Anwendungen)?	☐	☐	Speziell Ärzte und Kliniken sollten auf KV-SafeNet achten!
• Ermöglichen die eingesetzten Security-Produkte, dass der Netzwerkverkehr überwacht, gefiltert, protokolliert und diese Daten archiviert werden können?	☐	☐	Log-Daten zum späteren Nachweis sind verschlüsselt zu erfassen und dürfen nur durch einen Datenschutzbeauftragten und Administrator gemeinsam angesehen werden. So können die Daten bei Rechtsverstößen (Arbeitsrecht, Betriebsverfassungsgesetz...) gerichtlich verwendet werden.
• Werden Log-Daten für einen späteren Nachweis bei Vorfällen rechtskonform und über die Dauer von 10 Jahren gesichert?	☐	☐	
• Werden vertrauliche Informationen vor Wartungs- und Reparaturarbeiten von Datenträgern gelöscht/gesichert?	☐	☐	
• Wurde eine Betriebsvereinbarung unterzeichnet, die regelt, was im Unternehmen erlaubt ist und was nicht, z. B.: Darf auf Log-Daten zugegriffen werden, darf ein Mitarbeiter Downloads durchführen, werden illegale Webseiten gesperrt, ist die Privat-Nutzung von Firmen-E-Mails erlaubt oder nicht und wenn ja, darf auf diese zugegriffen werden etc.?	☐	☐	
• Werden und wie werden Verstöße gegen die IT-Security-Richtlinien in Ihrem Unternehmen geahndet?	☐	☐	Was sind die Folgen für Mitarbeiter: Abmahnungen etc.
Anzahl:	☐	☐	

2 Operative Sicherheit

Bitte beantworten Sie nun die folgenden Fragen:

	Antwort: ja	nein	Notizen
Client- und Netzwerkschutz:			
• Ist auf Clients (Rechner, Server, mobile Geräte etc.) ein aktuelles Schutz-Programm (Firewall, AV-Programm) installiert?	☐	☐	Beachten Sie, viele Netzwerk-Systeme (Kopierer/Drucker, Faxe, Switche, spezielle Server, die Netzwerkkommunikation etc.) können nicht direkt geschützt werden, das geht nur mittels einer UTM. Außerdem verfügen Sie damit gemeinsam mit dem Clientschutz über ein zweistufiges Sicherheitssystem.
• Ist zum Gesamtschutz für das Netzwerk ein UTM-System bestehend aus Firewall, AV, VPN-Server, Spam-Filter, Web-Filter, Intrusion Detection, Log-Server etc. installiert?	☐	☐	
• Werden regelmässige monatliche Reports gemacht, aus der die Unternehmensleitung ersieht: Was passiert im Netzwerk, wer macht was und wo sind Schwachstellen?	☐	☐	
• Werden bei einer Standortvernetzung bzw. Homearbeitsplätzen Daten hochverschlüsselt übermittelt (VPN)?	☐	☐	
Rechte der Anwender, Umgang mit Passwörtern:			
• Sind den IT-Benutzern Rollen und Profile zugeordnet worden?	☐	☐	
• Sind alle Mitarbeiter in der Wahl sicherer Passwörter geschult?	☐	☐	
• Werden Computer beim Verlassen mit Passwörtern gesichert?	☐	☐	
• Wird überprüft, ob Passwörter irgendwo öffentlich notiert sind?	☐	☐	Z. B. Passwörter auf Haftnotizen!
• Wurden voreingestellte oder leere Passwörter geändert?	☐	☐	Oftmals wird vergessen, die Passwörter der Werkseinstellung von IT-Systemen zu verändern!
Notfallvorsorge:			
• Gibt es einen Verantwortlichen, der sich über Sicherheitseigenschaften der Systeme und relevante Sicherheits-Updates informiert und die IT-Systeme schnell aktualisiert?	☐	☐	
• Sind die wichtigsten Passwörter für Notfälle sicher hinterlegt?	☐	☐	Was tun bei Notfällen! Betriebsunterbrechung vermeiden, denn das kostet Geld!
• Gibt es einen Notfallplan mit Anweisungen/Kontaktadressen?	☐	☐	
• Kennt jeder Mitarbeiter den Notfallplan und ist er zugänglich?	☐	☐	
Reports, Datenschutz/Verschlüsselung:			
• Gibt es ein Konzept, das beschreibt, welche Daten nach innen und nach außen (zum Internet) angeboten werden?	☐	☐	
• Ist geregelt, auf welche Daten Anwender zugreifen dürfen?	☐	☐	Monatliche UTM-Reports zeigen der Firmenleitung auf, was im Netzwerk los ist und wie Probleme gelöst werden können: Mitarbeiter surfen zu viel im Internet, wer macht genau was und welche Kosten verursacht es. Es gibts immer mehr Vorfälle, in denen Know-How, Vertriebsdaten, personenbezogene Daten etc. aus Firmen entwendet werden bzw. diese damit erpresst werden. Eine Vielzahl von Daten unterliegen gesetzlichen Archivierungsrichtlinien, z. B. kaufmännische Daten (Rechnungen etc.) müssen 10 Jahre aufbewahrt werden, Log-Daten unterliegen arbeitsrechtlichen bzw. dem Betriebsverfassungsschutz-Gesetzen. Hier kann Ihnen das Securepoint UMA (Unified Mail Archive) helfen.
• Wird geloggt/reportet: Wer hat was im Netzwerk gemacht und wer ist verantwortlich?	☐	☐	
• Werden gesetzliche Aufbewahrungspflichten berücksichtigt?	☐	☐	
• Werden personenbezogene Daten sicher verarbeitet?	☐	☐	
• Sind die Sicherheitsmechanismen auch aktiviert?	☐	☐	
• Werden vertrauliche Daten und gefährdete Systeme wie Notebooks ausreichend durch Verschlüsselung oder andere Maßnahmen – z. B. bei Verlust/Diebstahl – geschützt?	☐	☐	
Wartung von IT-Systemen, Datensicherung:			
• Gibt es eine Backup-Strategie und ist festgelegt, welche Daten wie lange und wo gesichert werden?	☐	☐	
• Bezieht die Sicherung auch tragbare Computer und nicht vernetzte Systeme mit ein?	☐	☐	
• Sind die Sicherungs-/Rücksicherungsverfahren dokumentiert?	☐	☐	
• Gibt es ein Testkonzept bei Systemänderungen?	☐	☐	
Infrastruktursicherheit:			
• Besteht ein angemessener Schutz der IT-Systeme gegen Feuer, Überspannung, Wasserschäden und Stromausfall?	☐	☐	
• Ist der Zutritt zu IT-Systemen und Räumen geregelt? Müssen Besucher, Handwerker, Servicekräfte etc. begleitet bzw. beaufsichtigt werden? Ist ein Einbruchschutz vorhanden?	☐	☐	
Anzahl:	☐	☐	

Wo stehen Sie?

SECUREPOINT SECURITY SOLUTIONS

Auswertung Ihres Unternehmens:

Diese Checkliste soll Sie sensibilisieren. Sie zeigt Ihnen wesentliche Lücken in der IT-Sicherheit im Unternehmen auf und hilft Ihnen eine angemessene Lösung zu finden.

Grundsätzlich sollten Sie alle Fragen in allen Bereichen der Checkliste mit „Ja" beantworten, nur dann können Sie sicher sein, dass Sie auf dem richtigen Weg sind!

Diese strukturierte Vorgehensweise und das Feststellen des Bedarfs in IT-Sicherheit soll Ihnen einerseits die Gewissheit geben das Optimale zu tun, aber auch klar aufzeigen:

„Wo sind die Schwächen, was ist wichtig, was muss getan werden und steht alles in einem vernünftigen Kosten-/Nutzenverhältnis!"

1 Strategische Sicherheit

- **0 bis 10 Fragen beantwortet:** Sie sollten sich äußerst dringend zum Thema IT-Sicherheit beraten lassen!
- **11 bis 14 Fragen beantwortet:** Gut, dass Sie etwas tun! Jedoch sollten Sie schnell die offenen Fragen abarbeiten.
- **15 bis 17 Fragen beantwortet:** Gratuliere, Sie haben es fast geschafft ein Vorzeige-Unternehmen im Bereich IT-Security zu sein! Aber haben Sie das alles auch operativ umgesetzt?

2 Operative Sicherheit

- **0 bis 14 Fragen beantwortet:** Achtung: Sie haben zu wenig in der IT-Sicherheit umgesetzt. Sehr große Schwierigkeiten könnten auf Sie zukommen!
- **15 bis 22 Fragen beantwortet:** Sie haben schon einige richtige Schritte im Bereich IT-Sicherheit getan. Sie müssen jedoch noch viel mehr tun.
- **23 bis 26 Fragen beantwortet:** Gratuliere, wenn Sie für die strategische Sicherheit im Unternehmen genauso viel getan haben wie im operativen Bereich, dann sind Sie ein Gewinner!

Bestandsaufnahme/Projektcheck!

Infrastruktur / Projektcheckliste
Checkliste für Projekt-Dokumentation und IT-Security-Auswahl:

Notizen:

1. Infrastruktur-Daten/Internet-Anbindungen:

1.1. Welchen Internet-Zugangsprovider nutzt Ihr Unternehmen:
_____

Liegen die Providerdaten für die Authentisierung vor?

1.2. Gibt es vorhandene Kommunikationshardware:
( ) DSL-Modem ( ) Router:

1.3. Welche Anbindung verwenden Sie zum Internet-Zugang:
( ) Standleitung ( ) ADSL/VDSL ( ) SDSL ( ) UMTS
( ) mit DynDNS

Wenn keine feste IP-Adresse vorhanden ist, ermöglicht DynDNS den Betrieb von VPN über den kostenlosen Securepoint DynDNS-Dienst: http://www.spdns.de/

1.4. Welche Bandbreiten benötigen oder haben Sie:
( ) 2 MBit ( ) 4 MBit ( ) 16 MBit ( ) >16 MBit:
_____
Benötigen Sie größere Bandbreiten:
_____

1.5. Wie hoch ist die Gesamtanzahl an EDV-Anwender/Rechner und Server am Standort: _____

Wird benötigt z. B. zur Definition von UTM Appliance-Größen bzgl. des Datendurchsatzes.

1.6. ( ) Wird von Ihnen Multi Path Routing benötigt?

Zusammenfassung mehrerer DSL-Leitungen für Redundanz/Load-Balancing und Bandbreiten.

1.7. Ist QoS/Bandbreitenbindung für Dienste/Ports nötig?
( ) Wird VoIP genutzt?
( ) Benötigen andere Dienste QoS, wenn ja, welche:
_____

Der einwandfreie Betrieb von z. B. VoIP benötigt Quality of Service (QoS), um Mindest-Bandbreiten z. B. für Sprache zu garantieren.

1.8. ( ) Benötigen Sie IPv6 für Ihr Netzwerk?

IPv6 ist für die UTM/VPN Version 11 (ab September 2012) von Securepoint verfügbar.

1.9. Wird zur Sicherheit eine Hochverfügbarkeitslösungen benötigt?
( ) Cold-Standby-Lösung erwünscht?
( ) über eigener virtuelle Plattform
( ) auf Securepoint-Appliances
( ) Hot-Standby-Lösung (Fail-Over-Cluster) erwünscht?
( ) über eigener virtuelle Plattform
( ) auf Securepoint-Appliances

Achtung: Vorteil durch minimale Ausfallzeiten mit Hochverfügbarkeitslösungen!

1.10. ( ) Wird WLAN am Standort benötigt?
( ) Wieviele Accesspoints werden benötigt: _____
( ) Wird ein WLAN-Managementsystem benötigt: _____

Ab UTM Version 11 sind für kleine Appliances integrierte WLAN-Accesspoints verfügbar. Bei kleinen Standorten entfällt so der Kauf von zusätzlichen APs. Die Securepoint Network Access Controller (NAC) Appliance dient dem einfachen Management von größeren bzw. verteilten WLAN-Umgebungen mit vielen APs, z. B. in Hotels, Klinken, Unternehmen, die Gastzugänge zur Verfügung stellen etc.

1.11. ( ) Wird eine Standortvernetzung geplant?
Wieviele Standorte haben Sie (inkl. Homearbeitsplätze): _____
Fassen Sie alle die Standortdaten pro Standort zusammen (Provider, Anbindung etc. siehe jeweils die Punkte 1.1 bis 1.10.):
_____

1.12. ( ) Dokumentieren Sie jetzt schon jetzt alle technischen Daten, Zugangsdaten, Netzwerkpläne etc. und inventarisieren Sie die bestehende und mögliche zusätzlich benötigte Hard-/Software für Ihr vorgesehenes IT-Security-Konzept und einen Notfallplan!

Solche Daten sollten immer griffbereit vorhanden sein, ohne lange zu suchen. Das macht ein Projekt kostengünstiger und erleichtert alle späteren Schritte!

Notizen:

2. Projektcheck:

2.1. Welche Schutzsysteme setzen Sie in Ihrem Unternehmen ein?
Client-Schutz vorhanden?
Welcher: _____

Ist ein aktueller lokaler Schutz für Rechner, mobile Geräte etc. vorhanden!

( ) War bisher eine Netzwerkschutz-Lösung vorhanden?
Welche: _____

Router sind kein Netzwerkschutz, denn sie verfügen nicht über die Funktionen einer UTM.

Über welchen Zeitraum wollen Sie das Unternehmen schützen;
( ) 1 Jahr ( ) 2 Jahre ( ) 3 Jahre ( ) 4 Jahre ( ) 5 Jahre

Zeitraum Einsatz der UTM-Lösung; längere Zeiträume sind pro Jahr kostengünstiger!

2.2. Welchen Virenschutz wollen Sie für Ihre Netzwerkschutz-Lösung:
( ) Einfacher Virenschutz ( ) Doppelter Virenschutz

Securepoint bietet mit der UTM Version 11 zwei integrierte Virenscanner ohne zusätzliche Mehrkosten!

2.3. Möchten Sie einen Content-Filter verwenden?
( ) Sind minderjährige Mitarbeiter vorhanden?
( ) Ist privates Surfen im Internet erlaubt?
( ) Wollen Sie die private Internet-Nutzung am Arbeitsplatz einschränken?

Achtung: Hier besteht eine besondere Fürsorgepflicht bzgl. der Jugendschutzgesetze!

Welche Kategorien sollen vom Content-Filter gesperrt werden:

Der Content-Filter sperrt automatisch Internetseiten, die nicht von Mitarbeitern angesurft werden dürfen!
Hinweis: AD-Gruppen können hier ab UTM Version 11 genutzt werden, um Sperrungen detailiert vorzunehmen.

( ) Pornographie	( ) Waffen	
( ) Soziale Netzwerke	( ) Hacking	
( ) Spiele	( ) Auktionen	
( ) Dating	( ) Sport	
( ) Audio	( ) Video	( ) Downloads
( ) Shopping	( ) Portale	
( ) Ausbildung	( ) Jobs	( ) Casting
( ) Personensuche	( ) Lexika	
( ) Events	( ) Reisen	
( ) Gesundheit/Schönheit	( ) Essen	
( ) Immobilien	( ) Fahrzeuge	
( ) Investments	( ) Geld verdienen	
( ) Kommunikation	( ) Proxy	

( ) sonstige: _____

Wer soll gesperrt werden:
( ) Geschäftsleitung
( ) Management
( ) Mitarbeiter
( ) Azubis/minderjährige Mitarbeiter
( ) sonstige: _____
( ) die Einschränkungen gelten nur für bestimmte Gruppen:
Definition der Gruppen und Einschränkungen:

_____
_____
_____
_____
_____

Infrastruktur / Projektcheckliste
Checkliste für Projekt-Dokumentation und IT-Security-Auswahl:

Notizen:

2.4. Wollen Sie einen Proxy-Server verwenden?

( ) transparenter Proxy?
( ) dedizierter Proxy? Authentifizierung:
( ) lokale Datenbank ( ) Radius
( ) Active Directory ( ) LDAP
Welcher Poxy-Port wird gewünscht:

_____

_____

Die Nutzung eines Proxy erhöht die Sicherhheit Ihres Firmennetzes, da IP-Adressen „übersetzt" werden und zusätzliche Filter genutzt werden können!
Hinweis: Ein dedizierter Proxy erhöht die Sicherheit nochmals! Hier kann noch eine Authentisierung vorgeschaltet werden.

( ) URL-Filter gewünscht?
Welche Webseiten sollen gezielt geperrt/freigegeben werden:

_____

_____

_____

Als Ergänzung zum Content-Filter können hier direkt und gezielt Internet-Adressen freigegeben oder gesperrt werden.

( ) Anwendungen blockieren?
Welche Anwendungen sollen geperrt/freigegeben werden:
( ) Teamviewer ( ) Netviewer
( ) AOL ( ) Gizmo
( ) ICQ ( ) MSN
( ) Skype ( ) Trillian
( ) Yahoo ( ) Webradio

( ) Größenlimitierung in MByte für:
( ) Downloads: _____ ( ) Uploads: _____

Down-/Uploads die in der Größe begrenzt werden sollen.

( ) Bandbreitenkontrolle erwünscht?
( ) Global
( ) Spezifisch (pro PC/Server):

_____

_____

2.5. Wollen Sie ein Intrusion Detection System verwenden?

( ) Wollen Sie das IDS zum Loggen aktivieren, um über Auffälligkeiten im Netzwerk infomiert zu sein?
( ) Wollen Sie das IDS zum Blocken von Anwendungen aktivieren?
Hier muss eine spezifische Analyse der von Ihnen genutzten Anwendungen (Datenbanken, Kommunikation etc.) und zu blockenden Anwendungen gemacht werden, da keine betriebswichtigen Anwendungen durch das IDS gestört werden dürfen!

Ein Intrusion Detection System (IDS) ist ein System zur Erkennung von Angriffen, die gegen Ihr Netzwerk gerichtet sind. Das IDS erhöht die Sicherheit im Netzwerk, da es durch Mustererkennungen Angriffe loggen und blocken kann.
Bestimmte Anwendungen können direkt gesperrt werden, obwohl sie sich „intelligent" verhalten und von sich aus versuchen, einen offenen Port an der Firewall zu finden.
Trotzdem ist eine gewisse Vorsicht beim Einsatz eines IDS nötig, wenn Anwendugnen automatisch geblockt werden sollen, da es durchaus vorkommen kann, dass spezifische Anwendungen beim Kunden angriffsähnliche Muster erzeugen, die dann geblockt werden könnten, aber keinen Angriff darstellen und dies könnte Geschäftsprozesse stören.

Notizen:

2.6. Wollen Sie einen Spam-Filter verwenden?

( ) Geschieht die E-Mail-Zustellung via POP3?
- ( ) Virenschutz erwünscht?
- ( ) Spamfilter erwünscht?
- ( ) Whitelisting vom Mail-Sendern:

_____

_____

( ) Geschieht die E-Mail-Zustellung via SMTP?
- ( ) Grey-Listing erwünscht?
- ( ) Empfängervalidierung gegen AD erwünscht?
- ( ) Whitelisting von Empfängern erwünscht:

_____

_____

- ( ) Sollen Spams im Festplattencache gehalten werden?
- ( ) Sollen E-Mails bei Virenbefall geblockt & gelöscht werden?
- ( ) Sollen E-Mails bei Virenbefall bereinigt & weitergeleitet werden?
- ( ) Soll der Attachmentfilter genutzt werden?
  Welche Anhänge sollen geblockt werden:

_____

_____

Grey-Listing bezeichnet eine zusätzlich effektive Form der Spam-Bekämpfung bei E-Mails, bei der die erste E-Mail von unbekannten Absendern zunächst abgewiesen und erst nach einem weiteren Zustellversuch angenommen wird. Hierbei werden E-Mails von Botnetzen effektiv ausgefiltert, da diese keine „richtigen" Mailserver sind und in der Regel nur einmal E-Mails zustellen und nicht erkennen, dass ein zweiter Zustellversuch nötig ist.

( ) Sollen E-Mails rechtskonform archiviert werden?
- ( ) Bedeutet es für Sie einen Schaden, wenn E-Mails verloren gehen oder absichtlich gelöscht werden?
  Wieviele E-Mail-Accounts bestehen in Ihrem Unternehmen:

  _____

  Ca. wieviele E-Mails werden pro Account bei Ihnen gespeichert:

  _____
- ( ) Archvieren Sie die E-Mails gesetzeskonform?
  Prüfen Sie, ob Sie die folgende Daten elektronisch z. B. in E-Mails verwenden. Für die folgenden Dokumente/Daten werden gesetzliche Aufbewahrungsfristen verlangt:

2 Jahre: Daten zu Nahrungsmittelfertigung nach Markteinführung
3 Jahre: Daten zu Morphinen/Medikamenten nach Verkaufsende
4 Jahre: Daten zu Finanzaudits bei AG nach Prüfung
5 Jahre: Biologische Produkte nach Fertigung
6 Jahre: Einfuhr-/Exportunterlagen, Frachtbriefe, Geschäftsbriefe, Protokolle, Gutachten, Zollbelege, Angebote, Preislisten, Handelsbriefe, Schriftwechsel, Reklamationen, Verträge
10 Jah.: Gehaltslisten, Personaldaten, Rechnungen, Prozessakten, Journale, Jahresabschlüsse, Kassenbücher, Kontoauszüge, Behandlungsakten, Grundbuchauszüge, Lieferscheine
21 Jah.: Medizinische Aufzeichnungen bei Kindern
30 Jah.: Dokumente zu giftigen Inhaltsstoffen nach Audit-Ende, Roñtgenbehandlungen, Krankengeschichte, Haftungsfälle
100 Jah.: Lebensversicherungspolicen
dauerhaft: Gerichtsurteile, Baupläne

Hinweis: Viele E-Mails müssen nach den gesetzlichen Aufbewahrungsfristen archviert werden. Dies betrifft z. B. kaufmännische E-Mails (Rechnungen, Lieferscheine, sonstige Geschäftskorrespondenz etc.).
Die Aufbewahrungsfristen liegen zwischen zwei Jahren bis unendlich. Rechnungen müssen z. B. 10 Jahre archiviert werden.
Mit der Securepoint UMA (Unfied Mail Archive) können Sie dies erreichen.

Infrastruktur / Projektcheckliste
Checkliste für Projekt-Dokumentation und IT-Security-Auswahl:

Notizen:

2.7. Wollen Sie eine sichere Vernetzung mittels VPN durchführen?

( ) Site-to-Site-VPN für Standorte mit jeweils eigenem Netzwerk?
Wieviele Standorte sollen vernetzt werden: _____
Wie groß ist der jeweilige Standort (Anzahl Anwender/Rechner):
Standort 1: _____ Standort 2: _____
Standort 3: _____ Standort 4: _____
Standort 5: _____ Standort 6: _____
Standort 7: _____ Standort 8: _____
Standort 9: _____ Standort 10: _____
Weitere Standorte: _____
_____

Die VPN-Server und UTMs mit VPN-Funktionalität von Securepoint sind kostengünstig verfügbar. Wenn ein externer Standort direkt in das Internet gehen soll, muss zum Schutz des Standorts eine eigene UTM verwendet werden! Grundsätzlich ist auch ein Schutz gegenüber Standorten von Vorteil, da ein eventuelles Sicherheitsproblem sich dann nicht ausbreiten kann.

( ) Sind VPN-fähige Geräte an den Standorten vorhanden? Welche:
_____
_____

( ) Benötigen Sie an den Standorten weitere VPN-Server?
(Anwender sollten dann nur über die Zentrale ins Internet)
Wenn ja, wieviele: _____
( ) Benötigen Sie an den Standorten weitere UTM-Server?
(Anwender können dann auch vom Standort direkt ins Internet)
Wenn ja, wieviele: _____

Berücksichtigen Sie, dass bei einer Standortvernetzung und einem zentralen Zugang zum Internet am Hauptstandort eventuell höhere Bandbreiten an den Nebenstandorten und eventuell auch am Hauptstandort nötig sind.

( ) Client-to-Site-VPN für mobile Geräte?
( ) Verfügen die mobilen Geräte über VPN-Clients? Welche:
_____
_____

Viele mobile Geräte (iPhone, Smartphones, iPad, Laptops etc.) verfügen schon über integrierte VPN-Clients. Der Securepoint OpenVPN-Client ist ebenfalls kostenlos verfügbar.

( ) Verfügen die Standorte über feste IP-Adressen oder muss zusätzlich ein DynDNS-Dienst eingesetzt werden?

Wenn keine feste IP-Adresse vorhanden ist, ermöglicht DynDNS den Betrieb von VPN über den kostenlosen Securepoint DynDNS-Dienst: http://www.spdns.de/

Welcher VPN-Typ soll verwendet werden (und ist eventuell auf der Gegenstelle schon vorhanden)?
( ) IPSec ( ) OpenVPN (SSL VPN)
( ) L2TP over IPSec ( ) PPTP

PPTP ist nicht mehr sicher und wird nicht empfohlen. PPTP wird jedoch aus Kompatibilitätsgründen von Securepoint noch angeboten.
Für OpenVPN bietet Securepoint ebenfalls kostenlose VPN-Clients.

Welche Authentifizierung soll verwendet werden?
( ) Preshared-Key ( ) x509-Zertifikat

X509-Zertifikate sind aufwendiger, aber bieten einen sehr hohen Schutz!

Welche Verschlüsselung soll verwendet werden?
( ) 3DES ( ) AES 128/256Bit
( ) Twofish ( ) Hash-Algo.
( ) MD5-HMAC/SHA1

( ) Benötigen Sie zur Authentifizierung Soft- oder Hardwaretokens?

Securepoint ID Control Soft-/Hardware-Authentifizierungstokens bietet Ihnen eine starke Zwei-Faktor- und Drei-Faktor-Authentifizierung und gewährleisten, ein noch höheres Maß an Sicherheit als eine konventionelle Benutzer-Anmeldung.

( ) Benötigen Sie VPN-Clients für Ihre mobilen Geräte?
( ) Securepoint OpenVPN-Client (Kostenlos)
( ) NCP-Client
( ) Greenbow-Client

Notizen:

2.8. Securepoint Operation Center

( ) Soll das Securepoint Operation Center (SOC) genutzt werden?
  ( ) Soll SOC im Client-Modus verwendet werden?
  ( ) Soll SOC im Server-Modus verwendet werden?

( ) Wer darf auf das SOC Zugriff haben:

_____

_____

_____

Das kostenlose Securepoint Operation Center (SOC) ist der Leitstand für Ihre IT-Security und Netzwerke.
SOC im Client-Modus läuft auf jedem Rechner. SOC im Server-Modus läuft auf einem zentralen Server, bietet den Zugriff für mehrere Administratoren und ein zentrales Management, Backup von Konfigurationen, Monitoring und Logging, wenn mehrere Securepoint Systeme eingesetzt werden.

( ) Soll das Vier-Augen-Prinzip und die Verschlüsselung von Log-Daten im SOC für das Logging genutzt werden?
  ( ) Wer sind die Datenschutzbeauftragten:

  _____

  _____

  ( ) Wer sind die Administratoren:

  _____

  _____

Insbesondere größere Unternehmen müssen aus Betriebsverfassungs- und arbeitsrechtlichen Gründen sicherstellen, dass nur ein Datenschutzbeauftragter und Administrator auf Log-Daten, die auch private Daten enthalten können, zugreifen darf. Ebenfalls sollte für Mitarbeiter dringend eine jeweils unterschriebene Betriebsvereinbarung aufgestellt werden, in der definiert ist, was ein Mitarbeiter und Arbeitgeber darf oder nicht darf (z. B. Sichtung von privaten E-Mails am Arbeitsplatzaccount)!

( ) Sollen Backups und System-Monitoring ausgeführt werden?
  ( ) Sollen Backups von System-Konfigurationen erstellt werden?
  ( ) Soll ein Monitoring der Systeme durchgeführt werden?
  ( ) Ist ein Update-Service (Einpflegen neuer Updates) erwünscht?
  ( ) In welchen Intervallen soll das geschehen?
    ( ) täglich ( ) wöchentlich ( ) monatlich

Virenscanner werden natürlich automatisch upgedatet! Dies betrifft neue Versionen oder Security-Updates von Securepoint.

( ) Welche Reports/Auswertungen sollen durchgeführt werden?
  ( ) Top Websites: Datenaufkommen der aufgerufenen Webseiten
  ( ) Top Surfer: Benutzer, die Datenaufkommen verursachen
  ( ) Webreport: Auswertung des Datenaufkommen eines Benutzers
  ( ) Surfer+Websites: Aufgerufenen Websites nach Benutzern
  ( ) Blocked Categories: Blockierte Webseiten-Kategorien
  ( ) Blocked Websites: Blockierte Webseiten
  ( ) Alerts: Ausgelöste Alarme
  ( ) IDS: Wer ist Angreiferer und Angriffsarten
  ( ) Malware: Namen, Art und Anzahl der Malware
  ( ) Possible SMTP Attack: Server-IPs bei SMTP-Angriff
  ( ) sonstige:

  _____

  _____

  ( ) In welchen Intervallen soll das geschehen?
    ( ) täglich ( ) wöchentlich ( ) monatlich

Die Auswertung dieser Daten gibt dem Management eines Unternehmens Hinweise, ob die Arbeitszeit von Mitarbeitern effektiv genutzt wird, hilft Rechtssicherheit zu erlangen, schützt vor Einbrüchen in die EDV, sorgt dafür, dass rechtzeitig Maßnahmen ergriffen werden können und verbessert damit die Unternehmensprozesse.

( ) Sollen Sicherheitsauswertungen/-analysen auf Grund der Daten und ggf. Empfehlungen für das Management erstellt werden?

Beachten Sie, dass auch hier eine geeignete Betriebsvereinbarung mit dem Mitarbeiter notwendig ist, da das private Surf-/Kommunikationsverhalten von Mitarbeitern sichtbar wird.

Benötigen Sie Hilfe für Ihr Netzwerk oder haben Sie weitere Fragen zur IT-Sicherheit?

Wir helfen Ihnen gerne! Ihr Systemhaus!

Ihr Systemhaus-Partner:

SECUREPOINT
SECURITY SOLUTIONS

Securepoint GmbH
Salzstraße 1
21335 Lüneburg
Germany

fon: ++49 (0) 41 31 / 24 01-0
fax: ++49 (0) 41 31 / 24 01-50

mail: info@securepoint.de
web: www.securepoint.de