MANAGING
NETWORK SECURITY

زیر نظر استاد راهنما :

جناب آقای مهندس فرداد

تهیه کننده:

امیر پدرام گلابی

فهرست مطالب

- مدل مرجع امنیت شبکه ۲
- سطح های امنیتی ۲
- بعد های امنیتی ۳
- اصول و سیاستهای امنیتی ۳
- مدیریت امنیت ۵
- اصول عادی (عملیاتهای امنیت آدرس) ۵
- چرخاندن امنیت ۶
- پردازش مداوم امنیت ۷
- پیوستگی مدیریت تجارت ۹

به همراه متن ترجمه نشده مدیریت امنیت شبکه (شرکت اریسون)

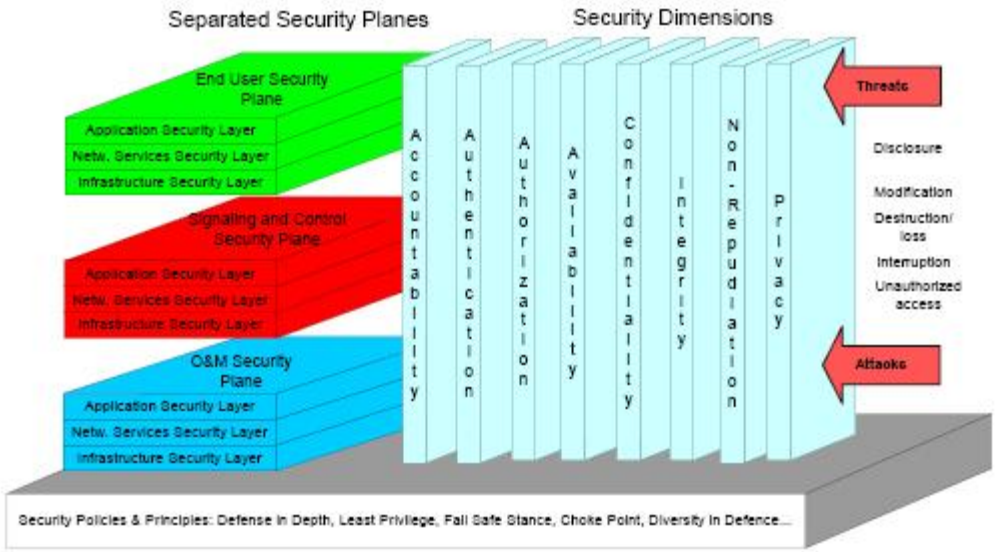
www.pedimetall.blogspot.com
Pedimetall_455@yahoo.com

مدل مرجع معماری امنیت شبکه

به سوی مسیر ساختن امنیت مناسب ،در آینده توانا بودن شبکه موبایل و تجزیه کردن تعداد پیچش ها در ابزار مهم می باشد .پیروی معماری سه گام هموار (مبنی بر استاندارد بین المللی x.805) در جهت عرضه کردن اطلاعات سودمند و مفید برای حرکت و نگه داشتن آلات دقیق و میزان مطلوب جهت عبور از این گذرگاهها.

این مدل از لحاظ معماری شامل چهار جزء می باشد :

سطح های امنیت جداگانه ،لایه های امنیتی ، سرویس دهنده امنیتی و اصول خط مشهای امنیتی می باشد .



سطح های امنیتی

شبکه ها می توانند در یک چنین مسیر مخصوص برای آنکه واقعه های یک سطح امنیتی هستند کاملا مجزا نگه داشته شده ، در نتیجه از سطح های امنیتی بعدا استفاده می شود .راه کارها از طرف سطح های امنیتی تهیه می شود توانائی به طرف متمایز کردن آدرسها ی و انجمن مستقل مشاورین کامپیوتر .کاربر نهائی آدرسهای امنیتی ، تضمین آدرس و استفاده مشتری ها از سرویس تعمیرات شبکه به دست

خود آنها ،همچنین این سطح نماینده داده های جاری شده کـاربر نهـائی مـی باشـد .علامت دهی و کنترل سطح امنیت پوششها جهت محافظت از فعالیت های مـوثر در جهت قادر ساختن تحویل اطلاعات ،از میان خدمات سرویسها و استفاده های شـبکه پوششهای سطح امنیتی O&M از عملیات و کارکردهای نهائی محافظت می کند .

بعدهای امنیت

بعد های امنیتی دستگاهای ظاهری است که تمامی راه حل های امنیتی را خلاصه می کند ،هر چند راه حل های امنیتی و طرز کار اجرای آن برای بعد هـای امنیتـی آشـنا هستند .در تمام بعد های امنیتی عرض یابی هر یک از لایه ها از سطح امنیتـی نقطـه مشترک می باشد .بیشترین واحد های مشترک عبارتند از :

- تصدیق
- اجاره
- جوابگوئی
- دسترسی پذیری
- قابلیت اعتماد
- بی نقصی
- انکار کردن و خلوت

اصول و سیاستهای امنیتی

- به سوی بالا بردن محافظت از شبکه ، با بهترین شـیوه هـا و اصـول خـاص امنیتی به طور عادی آشنا هستند ،شاید بیشتر از همه یک چیز مهم باشـد و آن دفاع در عمق اصلی است : به کار بردن طرز کار امنیتی مجزا و امنیت لایه ها به سوی تامین حفاظت .اگر یک طرز کار یا لایه های فایلها در جهت

،طرز کار و لایه های دیگر همیشه در جای خود به سوی تامین حفاظت صحیح و سلاحیت دار باشد .این قانون علمی آشنا به طور عادی در جهت حفاظت از فضای احاطه شده به وسیله یک سایت می باشد به طوری که در ابتدای پیکره نمایش می دهد .

- کوچکترین برتری اصولی دیگر اصل علمی امنیتی می باشد .آن وسایل به جهت اینکه هویت مجزا و یگانه دارند بر حسب لزوم مزایای اجرا کردن تکلیفهایشان را دارند .از این طرف حداکثر اهمیت وقتی است که به محافظت از گره می پردازد .خدمات سرویسها کارکرد همراه یک گره را تنها مزایای آنها می دانند .این کار برای سرویس کردن یک گره غیر ضروری می باشد و برای گره های در حال اجرا بدون فایده .اصل علمی دستگاهها و گره ها نیز اجرا کردن تخریب امن می باشد .این وسائل برای آن است که در هنگام عمل نکردن های سیتم یا گره اثرات جانبی و مضر آن چیز عمل نکرده را به طرف خارج بفرستد .بعضی اوقات تنوع از طرف استحکامات اصل علمی و همچنین توانائی سودمند می باشد .قاعده کلی مبنی بر استفاده کردن الگوها از لحاظ سیستم های تهیه کننده حفاظت تا حدی متفاوت می باشد .اگر یک سیستم در بر داشتن قابلیت آسیب پذیری را دارا باشد توانائی ضربه زدن به آسیب رسانها را نداشته و از این رو آسیب پذیری را سبک می کند .
- مسدود کردن نقطه و مجبور کردن مهاجمان از استفاده از کانال محدود که این کار می تواند به نمایش گذاشته شده و کنترل شود .در امنیت شبکه فضای احاطه کننده مخصوص محافظت برای سایت است .بطوریکه یک مسدود کننده نقطه هر کس را که در حال تک کردن باشد در موقیت خود

مجبور به در خواست واگزار و رعایت قوانین کانال می کند ،که این هم برای حمایت کردن و دفاع کردن در برابر حملات می باشد .

مدیریت امنیت

مقدمه :

رای های توانستن در جهت ساختن امنیت صدا که سابقه هر دو مخصوص تجارت می باشد و فرا گرفتن کامل شبکه بندی آن در جهت پشتیبانی از چرخه دوام سراسر سیستم مخابراتی ،در نتیجه پیروی پشت سر هم و پیوسته عملیات باعث عهده دار شدن در این امور می شود :

1. **مدیریت تجارت اتصال**
2. **طراحی امنیت شبکه**
3. **مجتمع سازی و پیکر بندی امنیت شبکه**
4. **حسابرسی های امنیت شبکه**
5. **پیاده سازی امنیت شبکه**
6. **مدیریت در تقلب**

اصول عادی (عملیاتهای امنیت آدرس)

- **مدیریت عملیات تمام شبکه از داخل ریسک می باشد ،به همین دلیل ریسک باید مقبول اجتناب کردن یا انتقال یافته باشد .**
- **آگاهی اپراتورهای در حال انتقال و پردازش در پشت حفاظ به واسطه افشا و یا قطع .**
- **هزینه دادرسی اپراتور تیره ،راه حل های امنیتی بسار خوب و سنجیده شده در باز پرداخت هزینه دادرسی و عملیات کاهیده ،ریسک فریب را افزایش می دهد .**

چگونگی پیروی از قسمت توصیفهای متفاوت که تحت عملیات مکمل یکـدیگر مـی باشند و شکل دادن مدام و تدبیر مناسب برای مدیریت امنیت بخشی از این قسـمت بود.

چرخاندن امنیت

مدل استاندارد صنعتی سابقا در جهت توضیح دادن مدیریت امنیت مناسب برگزیده بود ه است و تمام فعالیت امنیت شبکه باید پیرامون سیاست امنیتی پیکـره مشـاهده شود و در این باب در آورده شود .

تصویر کلی امنیت شبکه مشاهده های مداوم یک ترکیـب پـردازش پیرامـون یکـی شدن سیاست امنیتی می باشد ،اینه پردازش تقسیم شده در شبکه هستند :

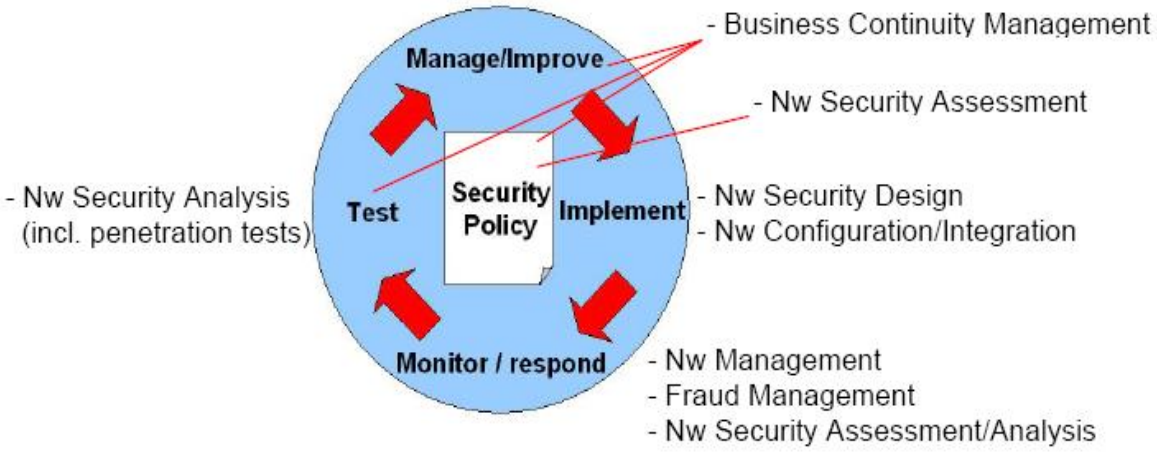
- اجرا کردن امنیت شبکه
- صفحه نمایش شبکه و جواب دادن به رویدادها
- تست امنیت از طرف شبکه
- بهتر کردن امنیت شبکه

ابزار امنیت شبکه –دستگاههای امنیت پیرامون گره ها همچون (vpn) ، دیواره های آتش ، دستگاهای پیشگیری ،آشکار سازی تجاوز (IDS/IB) ،وسیله های تصـدیق با برنامه جهت ایجاد پیکر بندی و یکپارچگی هستند .این مفهوم در جهت جلوگیری از فعالیت ها و سیاست های تهدیدات دشمن می باشد .

پاسخ دادن /صفحه نمایش – اجرا کردن سیاست امنیت به استفاده کنندگان امکـان کشف نفوذبغلاوه ثبت وقایع دیگر ،بازبینی اصول مهارتهای مراقبت در برابر تجـاوز ها را می دهد .

تست کردن – کارائی در جهت ارزیابی سیاست به سوی فاصله ء معـین از آغـاز تـا انتهای بازبینی های امنیتی ، قابلیت آسیب پذیری ،تست های پیمایش و نفوز .
اداره کردن اصلاحات –جمع کردن آگاهی بواسـطه گامهـای پیشـین تجربـه شـده و آشنا به ضمینه رشد و توسعه اقتصادی در امنیت بـازار اوراق بهـادار در برابـر بهتـر کردن سیاست موثر پیرامون تکرار حوزه گام اول .

پردازش مداوم امنیت



سیاست امنیتـی در ضـمن تجزیـه ریسـک اسـت ،کـدام قسـمت اسـاس کمپـانی هـا پردازش امنیت تجارت و پیوستگی آن است .آنها می توانند برسی کننـد ،بطوریکـه رشد یافته و هر دو جزءصحیح ارزیابی امنیت خدمات سرویس یـا یـاری دادن دوام تجارت .دوام تجارت نیز شامل یک چنین چیزی با توجه به بحران مدیریت ،فاجعـه بازیافت و سازمانبندی حالت ارتجاعی می باشد .

ریسک تجزیه و آمادگی در جهت طرح ریزی حداکثر اهمیت را داشته که بتـوان بـا آن خدمات را آغاز و روبه راه سازیم .

اجرا کردن امنیت شبکه – برای آنکه امنیت ابزاری است برای مراقبت کردن در راه و رسم مخابرات ،و همسطح کردن راه و رسم با برنامه در سیاست امنیتی .همچنـین پیکر بندی و مجتمع سازی می بایست در حفظ کردن وضعیت برطبق طرح ریزی ها اجرا گردد.

پاسخ صفحه نمایش –افـراد مـدیریت شـبکه گـزارش روزانـه صـفحه نمـایش را در صورتیکه دستگاه زمان واقعی نفوز را کشف کند را از طریق سیاست تجـاوز یافتـه و علامت ها را در جهت یافتن دنبال می کند .

مدیریت کلاهبرداری – پیشرفتهای تدریجی و چاره سـازی ،وضـع کـاربر نهـائی بـد اندیش را بیدرنگ نمایان می سازد .

آرایش دادن موضع امنیت شبکه باید متصلا به وسیله اسلوب شناسی به سوی انجـام دادن IDS/IPS میزان سازی شده و به روز رسانی شود ،ثبت وقایع قانونهای کاوش و رایانه .

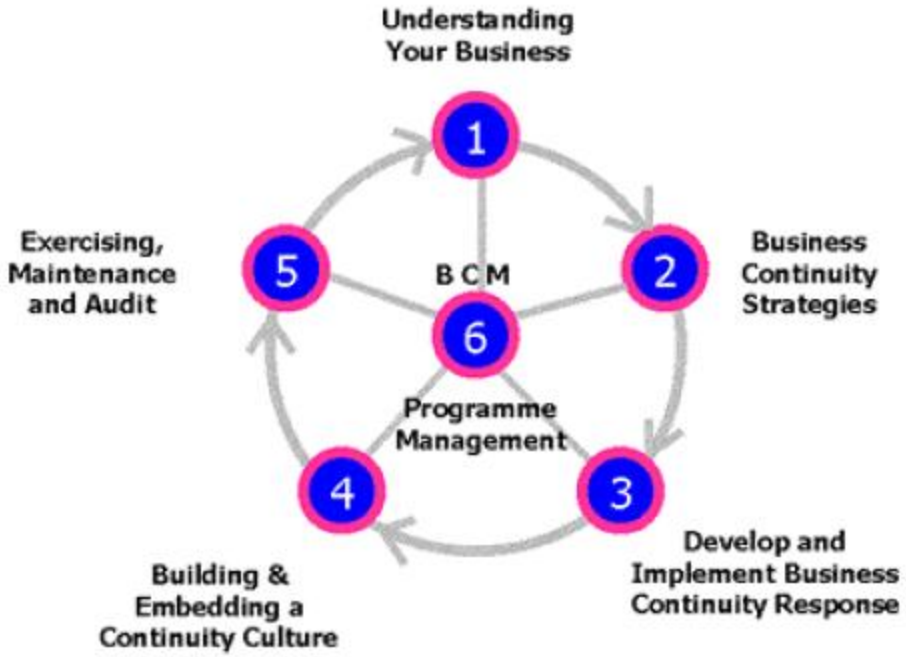
تست کردن –جزئیات پیکر بندی دستگاه کاوش و تسـتها شـامل تسـت نفـوز هـا و اجرا کـردن مرتـب قابلیـت آسـیب پـذیری بـوده .همچنـین در بـر داشـتن سـناریو پیرامون تمرینها در انتخاب ،برای مثال طرح یک واکنش به هنگامیکـه خطـری نـرم افزاری و سخت افزاری کمپانی ها را تهدید می کند .

لیست گرفتن از پیشنهادات امنیتی همواره به شـکل دادن ایـن بخـش در جهـت بـر ونداد ارزیابی امنیت ،تجریه کردن تدلیس مدنی و دوام فعالیـت تجـارت .آنهـا مـی توانند بسته به طرز علمی و رویه ، رده بندی کنند ،فیزیکی ،صنعتی یا باز گو کـردن مجموعه کارمندان یک اداره .

پیوستگی مدیریت تجارت

مدیریت پیوستگی تجارت (BCM) تنها جهت تاسیس کردن طرح ریـزی تجـارت پیوستگی و بازیافت حادثه بد نیست ، اما همچنان انتظام در جهـت بحـران مـدیریت ،ریسک مدیریت اسـت .مـدیریت امکانـات ،بهبـودی و ایمنـی ف امنیـت ،مـدیریت کیفیت و تحویل دادن زنجیره مدیریت .قسمت سوم آن چیز مانند مجموعه کارهای مفید در جهت پردازش مدیریت امنیت می باشد .

(BCM) نمایش پردازش تقسیم شده درون ششطبقه پیکره و آشکار نگـاه داشـتن طبقه پایین میباشد .

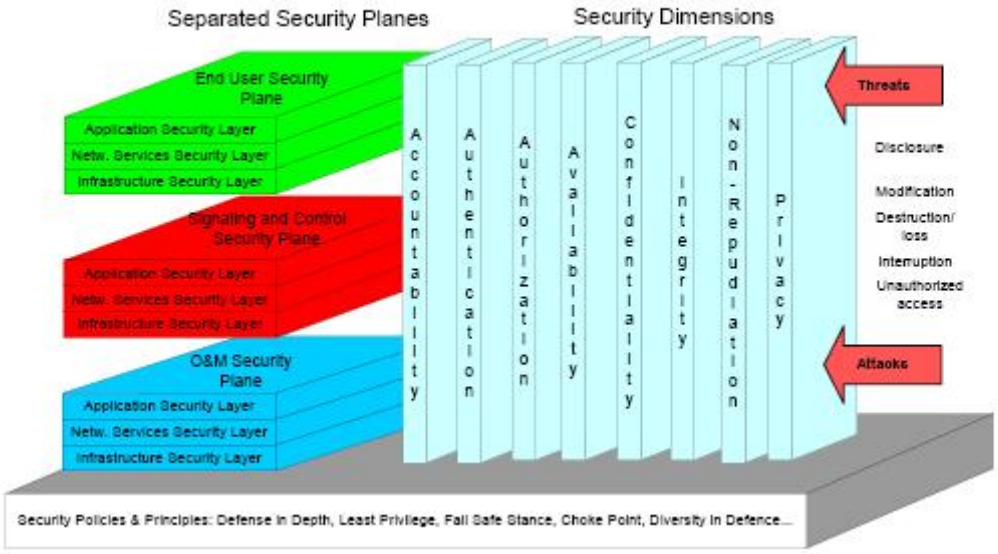


شش طبقه در جهت مدیریت پیوستگی تجارت را در ا در بالا می توان دید

MANAGING NETWORK SECURITY

Network Security Architecture Reference Model

To provide adequate security, it is important to be able to model the mobile network and analyze the threats to assets. The following three-plane architecture (based on the international standard X.805) provides a useful and simple way of capturing relevant information. This model consists of four architectural components: separate security planes, security layers, security services, and security policies & principles.
Figure 1. Network Security Architecture Model



3.2.1 Security Planes

Networks should be designed in such a way that events on one security plane are kept totally isolated from the other security planes. The concept of security planes provides the ability to differentiate and address security concerns independently.
The End-User Security Plane addresses security of access and use of the serviceprovider's network by customers. This plane also represents actual end-user data flows. *The Signaling and Control Security Plane* covers protection of the activities that enable the efficient delivery of information, services and applications across the network. *The O&M Security Plane* covers the protection of operation and maintenance functions.

3.2.2 Security Dimensions

The security dimensions are system aspects which run through all security solutions. However, security solutions and mechanisms are used for implementing the security dimensions. All security dimensions should be evaluated in each security plane/layer intersection point. The most common ones are:

• authentication

• authorization
• accountability
• availability
• confidentiality
• integrity
• non-repudiation and privacy

3.2.3 Security policies & principles

To enhance protection of the network, specific security principles and best practices are commonly used. Probably the most important one is the defense-in-depth principle: employ several security mechanisms and security layers to provide protection. If one of the mechanisms or layers fails, the other mechanisms and layers are still in place to provide sufficient protection. This principle is commonly used to protect the perimeter of a site, as depicted earlier in Figure 1.

The least privilege is another fundamental security principle. It means that an entity should only have the privileges it needs to perform its tasks. This is of utmost importance when considering node protection. The services running on a node should have only the privileges they need to provide the service and the node should not be running any unnecessary services.

Systems and nodes should also implement the fail-safe principle. This means that when the system or node fails, it should fail without harmful side effects.

Sometimes, the diversity-of-defense principle might also be useful. This principle is based on using different types of systems to provide a certain kind of protection. If one of the systems contains vulnerability, the other systems might not have that vulnerability and the impact of the vulnerability is thus mitigated.

A choke point forces attackers to use a narrow channel, which can be monitored and controlled. In network security the proper perimeter protection for the site is such a choke point; anyone attacking the site from the outside will have to go through that channel, which should be defended against such attacks.

4 Managing Security

4.1 Introduction

To be able to make sound security judgments, both the particular business context and the networking environment must be fully understood. To support the whole telecom system life cycle, from end-to-end, the following operations have to be undertaken:

- Business Continuity Management
- Network Security Design
- Network Configuration / Integration
- Network Security Audits
- Network Security Implementation
- Fraud Management.

4.2 Common Principles

The security operations address:

- Risk Management: all network operation implies a certain risk that must be accepted, avoided, reduced or transferred.
- Business Continuity: the operator’s critical processes and information should be protected from disclosure and/or disruption.
- Lowering operator costs: well thought-out security solutions provide a

payback in terms of reduced operating costs, reduced risk of fraud,
a reduced risk of critical security-related network outages and
potentially less churn.
The following chapter describes how the different sub-operations complement each other and fit into the “Security Wheel” concept, forming continuous security management.

4.3 The Security Wheel

This industry-standard model has been chosen to illustrate where security management fits in, and how all security activities in a network must evolve around the security policy; see figure in chapter 4.4.
The concept sees network security as a continuing process built around a corporate security policy. This process is divided into the stages:
• Implement network security
• Monitor network and respond to incidents
• Test the security of the network
• Improve network security.
Implement network security – Security devices such as perimeter nodes,
VPN devices, firewalls, Intrusion Detection/Prevention Systems (IDS/IPS)
and authentication devices are planned, configured and integrated.
The purpose is to prevent activities that the policy has defined as threats.
Monitor/Respond – The implemented security policy is validated using intrusion detection, as well as log and other auditing techniques, to watch for violations.
Test – The effectiveness of the policy should be evaluated at regular intervals through security audits, vulnerability scanning and/or penetration tests.
Manage/Improve – Information gathered from previous steps is analyzed and used together with developments in the security market to improve the policy, moving around the circle to the first step again.

4.4 Security – A continuous process

Figure 2. The Security Wheel model
Security Policy – Is, together with the Risk Analysis, the most fundamental part of any company’s security/business continuity process. These can be checked and/or developed as a part of either the security assessment service or the business continuity service. Business Continuity also includes such aspects as, for example, crisis management, disaster recovery, and organization resiliency.
Risk Analysis and Readiness planning is of utmost importance in guaranteeing the safe launch of a new service.
Implement Network Security – Network Security Design ensures that security is implemented according to best telecom practices, and the level planned for in the security policy. Also, configuration and integration must be performed in the most secure manner possible, and according to plans.
Monitor/Respond – Network Management personnel monitor logs, while Intrusion Detection System real-time alarms detect any signs of attempted policy violations. Fraud-management processes and solutions instantly detect malicious end-user behavior. The network security organization must be continuously updated with the latest methodology to perform IDS/IPS tuning, log analysis and computer forensics.
- Business Continuity Management

- Nw Management
- Fraud Management
- Nw Security Assessment/Analysis
- Nw Security Design
- Nw Configuration/Integration
- Nw Security Analysis
(incl. penetration tests)

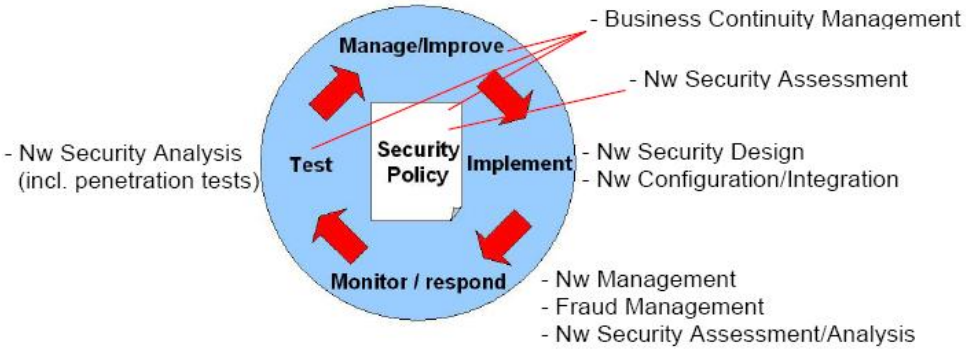


Figure 2. The Security Wheel model

- Nw Security Assessment
-
-

Test – Detailed system configuration analysis and tests, including penetration tests and vulnerability scanning must be performed on a regular basis. This also includes exercises around selected scenarios in, for example, a company's disaster recovery plan.

Manage/Improve – A list of suggested security improvements always form part of the output of a security Assessment, Analysis, Fraud or Business Continuity activity. They can be categorized as procedural, physical, technical or relate to the personnel.

4.5 Business Continuity Management

Business Continuity Management (BCM) incorporates not only business continuity planning and disaster recovery, but also the disciplines of crisis management, risk management, facilities management, health and safety, security, quality management and supply chain management. It can be seen as a super set of security management processes.

.

The BCM process is divided into six stages shown in Figure 3 and explained below
Test – Detailed system configuration analysis and tests, including penetration tests and vulnerability scanning must be performed on a regular basis. This also includes exercises around selected scenarios in, for example, a company's disaster recovery plan.Manage/Improve – A list of suggested security improvements always form part of the output of a security Assessment, Analysis, Fraud or Business Continuity activity.