

وضعیت فعلی امنیت فضای تبادل اطلاعات در کشور

مهدی برنجکوب

رئیس هیات مدیره شرکت پیام پرداز - رییس مرکز تخصصی آفا دانشگاه صنعتی اصفهان

عضو هیات علمی دانشگاه صنعتی اصفهان

bmjkb@cc.iut.ac.ir

دیماه ۱۳۸۸



فهرست مطالب

- مقدمه
- نگاهی گذرا به روند جهانی
- آشنایی با وضعیت داخل کشور
 - مروری بر اهم وقایع دهه اخیر
 - فهرست اهم اقدامات اساسی لازم الاجرا
 - تحلیل نقاط ضعف و قدرت
 - نقش سازمان های تأثیرگذار
 - توصیفی از وضعیت امنیتی سازمانهای استان

فهرست مطالب

مقدمه

نگاهی گذرا به روند جهانی

آشنایی با وضعیت داخل کشور

- مروری بر اهم وقایع دهه اخیر

- فهرست اهم اقدامات اساسی لازم الاجرا

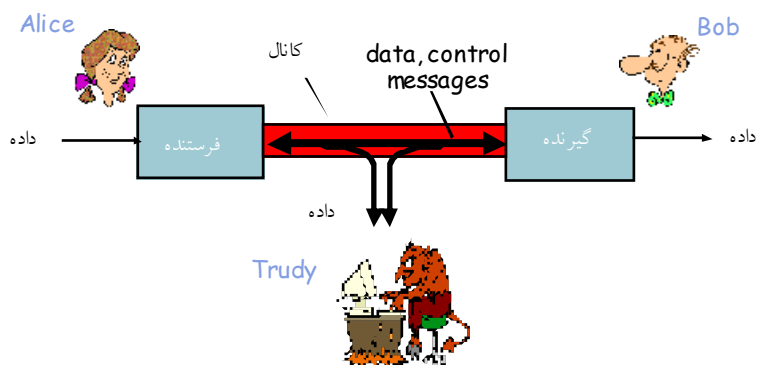
- تحلیل نقاط ضعف و قدرت

- نقش سازمان های تأثیرگذار

- توصیفی از وضعیت امنیتی سازمانهای استان

مؤلفه های امنیت

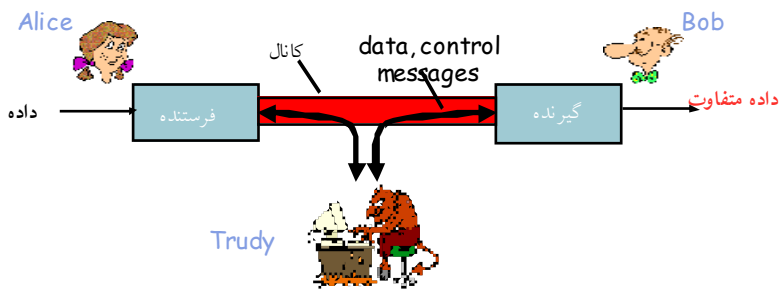
حفظ محرمانگی: مقابله با حملات غیر فعال



مقدمه: تعریف امنیت فضای تولید و تبادل اطلاعات

مؤلفه های امنیت

حفظ یکپارچگی: مقابله با حملات فعال



www.payampardaz.net

مقدمه: تعریف امنیت فضای تولید و تبادل اطلاعات

یک راه حل ساده برای امن سازی

حذف تمامی اتصالات و ارتباطات شبکه با سایرین

قراردادن سیستمها در اتاقهای محافظت شده

قراردادن یک محافظ در درب هر اتاق



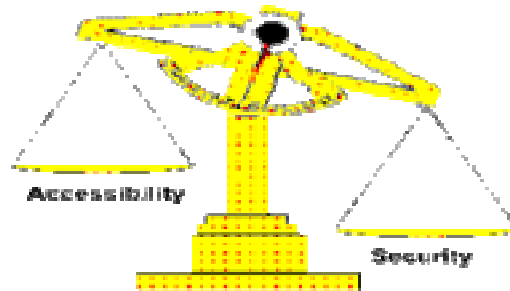
حذف بسیاری از دستاوردهای شبکه ها

www.payampardaz.net



مقدمه: تعریف امنیت فضای تولید و تبادل اطلاعات

➤ عدم کفایت راهکارهای سنتی دستیابی به امنیت



➤ امنیت همزمان با وجود دسترسی های کافی

www.payampardaz.net



مقدمه: تعریف امنیت فضای تولید و تبادل اطلاعات

□ مؤلفه های امنیت

- حفظ قابلیت دسترسی: مقابله با حملات منع سرویس
- انکار ناپذیری: مقابله با سلب مسئولیت خودی ها
- حفظ حریم خصوصی: مقابله با ورود به حریم خصوصی اشخاص
- حفظ قابلیت حسابرسی: مقابله با مخدوش کردن سوابق و ردیابی آنها در سیستم

www.payampardaz.net

فهرست مطالب

مقدمه

نگاهی گذرا به روند جهانی

آشنایی با وضعیت داخل کشور

- مروری بر اهم وقایع دهه اخیر

- فهرست اهم اقدامات اساسی لازم الاجرا

- تحلیل نقاط ضعف و قدرت

- نقش سازمان های تأثیرگذار

- توصیفی از وضعیت امنیتی سازمانهای استان

www.payampardaz.net

نگاهی گذرا به روند جهانی

دهه ۱۹۶۰ میلادی:

شروع به کار شبکه آرپا (وزارت دفاع امریکا)

دهه ۱۹۷۰ میلادی:

استاندارد سازی الگوریتم DES، ابداع رمزنگاری کلید عمومی

دهه ۱۹۸۰ میلادی:

ایجاد مکانیزم کربرس، معرفی پروتکل X.509

دهه ۱۹۹۰ میلادی:

ورود اینترنت به عرصه کسب و کار، تشکیل IETF

www.payampardaz.net

نگاهی گذرا به روند جهانی

□ برآورد حجم بازار جهانی IT (بیلیون دلار) [IDC-2005]

۲۰۰۸	۲۰۰۷	۲۰۰۶	۲۰۰۵	
۳۵۴.۵۸	۳۳۹.۶۴	۳۲۵.۳۳	۳۱۲.۲۱	اروپا
۳۷۳.۴۶	۳۵۶.۶۹	۳۴۰.۰۳	۳۲۵.۰۸	آمریکا
۱۳۳.۵۲	۱۳۱.۸۰	۱۳۰.۵۰	۱۲۷.۰۷	ژاپن
۱۴۵.۰۱	۱۳۳.۷۴	۱۲۳.۱۵	۱۱۲.۶۷	سایر
۱۰۰۷.۰۶	۹۶۱.۸۷	۹۱۹.۰۰	۸۷۷.۰۲	جهان

نرخ رشد متوسط: ۵%

www.payampardaz.net

نگاهی گذرا به روند جهانی

□ برآورد حجم بازار جهانی افتا (بیلیون دلار) [IDC-2004]

۲۰۰۶	۲۰۰۳	۲۰۰۲	۲۰۰۱	
۱۲.۴	۸.۱	۷		نرم افزار
۸.۹	۴.۷	۳.۶		سخت افزار
۲۳.۲	۱۲	۹.۷		خدمات
۴۴.۵	۲۴.۸	۲۰.۳	۱۶.۹	جمع

نرخ رشد متوسط: ۲۰%

www.payampardaz.net

نگاهی گذرا به روند جهانی

□ برآورد سهم افتا از بازار جهانی IT

2008	2006	2004
%6.5	%4.9	%3.6

اولویت دوم از نظر کسب و کار

اولویت اول از نظر تکنولوژی

www.payampardaz.net

فهرست مطالب

□ مقدمه

□ نگاهی گذرا به روند جهانی

□ **آشنایی با وضعیت داخل کشور**

- مروری بر اهم وقایع دهه اخیر

- فهرست اهم اقدامات اساسی لازم الاجرا

- تحلیل نقاط ضعف و قدرت

- نقش سازمان های تأثیرگذار

- توصیفی از وضعیت امنیتی سازمانهای استان

www.payampardaz.net

گام به گام با تحولات دهه اخیر در کشور

سال ۱۳۷۹: □

تشکیل انجمن رمز ایران

سال ۱۳۸۰: □

تشکیل مرکز صنایع نوین

سال ۱۳۸۱: □

تصویب قانون تجارت الکترونیک

سال ۱۳۸۲: □

ابلاغ سند چشم انداز ۲۰ ساله کشور به قوای سه گانه

www.payampardaz.net

گام به گام با تحولات دهه اخیر در کشور

سال ۱۳۸۳: □

تشکیل شورای عالی افتا/ صدور بخشنامه الزام سازمان ها به برنامه ریزی
برای مدیریت امنیت/ ابلاغ برنامه ۵ ساله چهارم توسعه کشور

سال ۱۳۸۴: □

تصویب سند ملی افتا در هیأت دولت

سال ۱۳۸۵: □

فعال سازی کمیسیون افتای شورای عالی امنیت ملی / ایده نقش آفرینی
کمیسیون امنیت شورای عالی فناوری اطلاعات

سال ۱۳۸۶: □

تشکیل مرکز پدافند غیرعامل/ فعال سازی مرکز صنایع نوین دفاعی

www.payampardaz.net

گام به گام با تحولات دهه اخیر در کشور

□ سال ۱۳۸۷:

تصویب مجدد و ابلاغ سند راهبردی افتا/ ابلاغ سیاست های کلی برنامه پنجم توسعه به قوای سه گانه

- ایجاد سامانه یکپارچه نرم افزاری اطلاعاتی، ارتقاء سطح حفاظت از اطلاعات رایانه ای، توسط علوم و فناوری های مرتبط با حفظ امنیت سامانه های اطلاعاتی و ارتباطی به منظور صیانت از فضای تبادل اطلاعات، تقویت فنی برای مقابله با تخلفات در فضاهای رایانه ای و صیانت از حریم فردی و عمومی

□ سال ۱۳۸۸:

تصویب و ابلاغ قانون جرایم رایانه ای/ ارائه لایحه برنامه ۵ ساله پنجم توسعه به مجلس شورای اسلامی

www.payampardaz.net

نگاهی دقیق تر به سند راهبردی افتا

□ چشم انداز

تأمین امنیت فضای تولید و تبادل اطلاعات کشور، عدم بروز اختلال در زیرساخت های حیاتی کشور و اعتماد و آسودگی خاطر آحاد شهروندان جامعه برای انجام تمامی امور قانونی از جمله فعالیت های اقتصادی، اجتماعی و فرهنگی به منظور صیانت از حاکمیت و اقتدار ملی در افق ۱۴۰۴

□ اهداف کلان

- صیانت از هویت دینی، ملی و ارزش های انسانی جامعه در افتا.
- حفظ حریم خصوصی و آزادی های مشروع در افتا.
- صیانت از منافع، اسرار و اقتدار ملی در افتا.
- حفظ زیرساخت های حیاتی کشور در مقابل حملات الکترونیکی.
- حفظ سرمایه های مادی و معنوی، اسرار کسب و کار و مالکیت خصوصی در افتا

www.payampardaz.net

نگاهی دقیق تر به سند راهبردی افتا

□ راهبردها و اهم اقدامات

راهبرد اول: امن سازی زیرساخت های حیاتی

- امن سازی زیرساخت های حیاتی کشور و منابع ملی در قبال حملات الکترونیکی

راهبرد دوم: ایجاد و توسعه نظام های فنی فرابخشی افتا

- استقرار سیستم مدیریت امنیت اطلاعات در دستگاه ها
- اعتبار سنجی محصولات، خدمات و مدیریت افتا
- استقرار نظام پیشگیری، مقابله و امداد افتا
- استقرار نظام تصدیق هویت رایانه ای
- استقرار نظام مقابله با جرایم افتا

www.payampardaz.net

نگاهی دقیق تر به سند راهبردی افتا

راهبرد سوم: تأمین سلامت و جلوگیری از مخاطرات ناشی از محتوا در افتا

- استقرار نظام سلامت محتوا
- استقرار مراکز عملیات امنیت

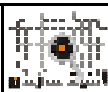
راهبرد چهارم: تقویت صنعت و توسعه محصولات و خدمات افتا

- حمایت از تولید، پشتیبانی و بکارگیری محصولات داخلی
- حمایت از تشکیل و تقویت شرکت های مهندسی و حرفه ای
- حمایت از ایجاد آزمایشگاه های ارزیابی فنی

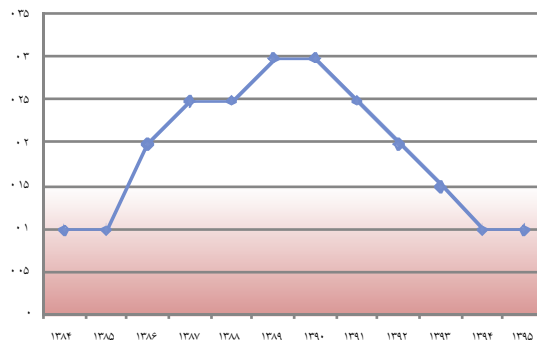
راهبرد پنجم: حمایت از تحقیق، ارتقای سطح آگاهی، دانش و مهارت های مرتبط با افتا

راهبرد ششم: ارتقای سطح همکاری های منطقه ای و بین المللی در زمینه افتا

www.payampardaz.net



پیش‌بینی نرخ رشد بازار امنیت اطلاعات در ایران



www.payampardaz.net



نگاه تحلیلی به وضعیت فعلی امنیت در کشور

□ نگاه تحلیلی به وضع موجود: نقاط ضعف

- عدم درک صحیح از نحوه دستیابی به امنیت شبکه
- عدم توسعه کافی دانش، فناوری و صنعت
- عدم هماهنگی و ارتباط نظام یافته (اقدامات پراکنده)
- عدم گردش و به اشتراک گذاری منابع (اطلاعات، دانش و تجربه)
- کمبود نیروی انسانی زبده پایدار
- عدم درک کافی از عمق ضرورت برقراری امنیت
- مشکلات فرهنگی (رقابت منفی، نقد ناپذیری و ارائه آمار و اطلاعات غیر واقعی).

www.payampardaz.net

نگاه تحلیلی به وضعیت فعلی امنیت در کشور

□ نگاه تحلیلی به وضع موجود: نقاط قوت

- برخورداری از فارغ التحصیلان مستعد و متخصص
- بستر آماده تشکیلاتی و قانونی برای حرکت به سوی وضعیت مطلوب
- وجود مراکز پشتیبان در سطوح مختلف (مرکز آبا، مرکز ماهر، مرکز پدافند غیر عامل، انجمن رمز ایران)
- وجود هسته ها و شرکت های فناوری

www.payampardaz.net

نگاه تحلیلی به وضعیت فعلی امنیت در کشور

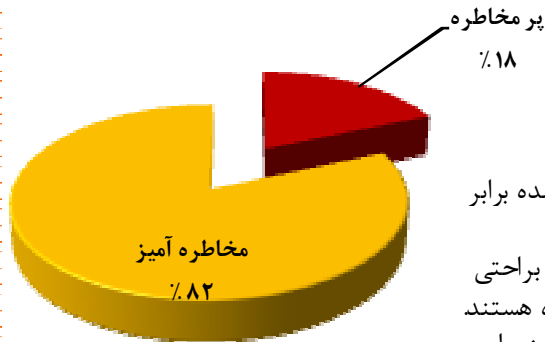
□ نقش سازمان های تأثیرگذار

سازمان	حوزه حاکمیت	حوزه تقاضا	حوزه عرضه
وزارت ارتباطات و فناوری اطلاعات	✓	✓	
وزارت صنایع و معادن	✓		
مرکز پدافند غیرعامل	✓		
سیستم بانکی		✓	
حوزه بازرگانی		✓	
دانشگاه ها و مراکز تحقیقاتی			✓
شرکت های فناوری (بخش خصوصی)			✓

www.payampardaz.net

توصیفی از وضعیت امنیتی سازمانهای استان

□ توزیع آسیب پذیری های مهم یافت شده در سازمان های استان

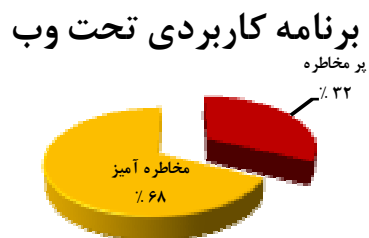
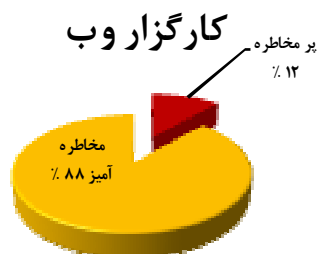


- تعداد آسیب پذیریهای یافت شده برابر با ۷۱۵ عدد بوده است.
- آسیب پذیری های پر مخاطره براحتی برای نفوذگران قابل سوء استفاده هستند
- آسیب پذیری های مخاطره آمیز برای سوء استفاده نیاز به تلاش بیشتری دارند

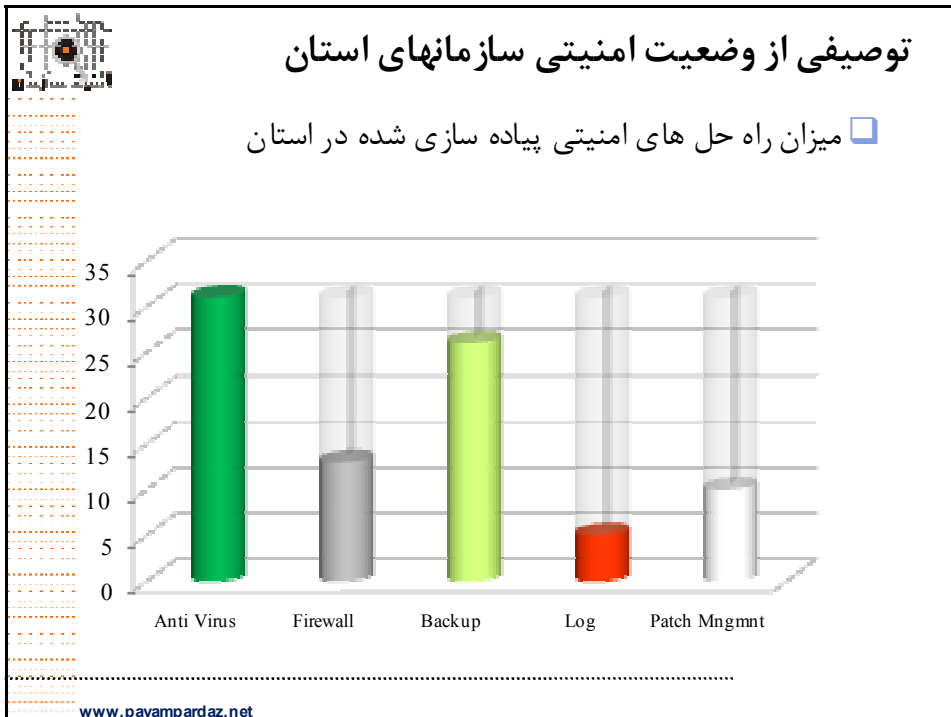
www.payampardaz.net

توصیفی از وضعیت امنیتی سازمانهای استان

□ تفکیک آسیب پذیری های برنامه های کاربردی تحت وب به همراه امنیت کارگزار وب آن:



www.payampardaz.net



مرور مطالب

- مقدمه
- نگاهی گذرا به روند جهانی
- آشنایی با وضعیت داخل کشور
- مروری بر اهم وقایع دهه اخیر
- فهرست اهم اقدامات اساسی لازم الاجرا
- تحلیل نقاط ضعف و قدرت
- نقش سازمان های تأثیرگذار
- توصیفی از وضعیت امنیتی سازمانهای استان

www.payampardaz.net