ارزیابی امنیتی حملات ممکن به شهر الکترونیکی

محمد مهدی درفشی
۸۵۱۶۱۴۰۲۲

آشنایی با شهر الکترونیکی

اهداف

راهبردها

بخش های مختلف

کلیت انواع حملات وارده به شهر الکترونیکی

بیمارستان الکترونیکی و پزشکی از راه دور

اهداف

انواع

کاربردها

کلیت انواع حملات وارده به بیمارستان الکترونیکی

دانشگاه الکترونیکی و آموزش مجازی

اهداف

سابقه

آینده ی آموزش مجازی

کلیت انواع حملات وارده به دانشگاه الکترونیکی

بانک داری الکترونیکی

چالش های بانک داری الکترونیکی در ایران

انواع سرویس ها

مزایا

کلیت انواع حملات وارده به بانک داری الکترونیکی

روش های نفوذ

حملاتی که وبسایت ما را مورد هدف قرار می دهد

حملاتی که برنامه های تحت سیستم عامل را مورد هدف قرار می دهد

حملاتی که شبکه ی ما را مورد هدف قرار می دهد

حملاتی که وبسایت ما را مورد هدف قرار می دهد

تزریق دستورات SQL :

این حملات برای دستکاری یا مشاهده ی اطلاعات درون بانک اطلاعاتی به کار می رود.

XSS :

سرقت هویت کاربران،سرقت کوکی ها، تزریق دستورات جاوا اسکریپت و ... .

تزریق دستورات SQL

آشنایی با SQL INJECTION

تشخیص

راه های مقابله

کد نویسی ایمن

به روز بودن

رمز نگاری

XSS

آشنایی با Cross Site Scripting

نحوه ی وقوع

بر اثر برنامه نویسی اشتباه

ضعف Application های تحت وب

محافظت

حملاتی که برنامه ی تحت سیستم عامل را مورد هدف قرار می دهد

ویروس ها

انتشار ویروس ها به کندی صورت می گیرید و کم خطر هستند

تروجان ها

برای مقاصد هدف دار و معمولا سرقت اطلاعات نوشته می شوند

کرم ها

صرفا برای آلوده سازی سیستم ها نوشته می شوند و سرعت رشد بسیار بالایی دارند.

ویروس ها و تروجان ها

مقدمه

عملکرد

آلوده سازی را انجام می دهند و معمولا توسط کاربرها به این سو و آن سو تکثیر می شوند.

پیش گیری

استفاده از نرم افزارهای ضد ویروس و تروجان

کرم ها

نحوه ی عملکرد و تکثیر کرم

آسیب پذیری چیست؟

آسیب پذیری یا BUG نقطه ضعفی قابل سو
استفاده در یک سیستم است.

کرم ها

نمونه ای از آسیب پذیری در زبان C/C++

```
#include <iostream>
using namespace std;
int main()
{
    char *str="%n%n%n%n";
    cout<<str;
    printf(str);
    return 0;
}
```

حملاتی که شبکه ما را مورد هدف قرار می دهد

عوامل انسانی

هر چقدر هم که امنیت رشد کند نمی توانیم بی دقتی عوامل انسانی را به صفر برسانیم

سرویس های فعال در هر سیستم

شناسایی سرویس های فعال در هر سیستم می تواند به ما کمک کند تا از وقوع برخی حملات جلوگیری کنیم.

انواع و تعریف حملات

برخی از انواع حملات در شبکه های کامپیوتری

DOS

Man In The Middle

Sniff

DNS Poisoning

تامین امنیت فیزیکی

نقش عوامل ساختمانی در امنیت مراکز داده

مراکزداده به دلیل وجود تجهیزات الکترونیکی و رایانه ای ارزشمند ، فرآیندهای اطلاعاتی پیچیده و حجیم ، انجام امور اجرایی ، اقتصادی ، اجتماعی و خدمات عمومی در سطوح ملی ، منطقه ای و محلی، دارای درجه اهمیت فراوانی خواهند بود که متناسب با سطح تأثیر گذاری بایستی مورد توجه قرار گیرند.

نقش عوامل ساختمانی در امنیت مراکز داده

Data Centerهای متفاوتی در نقاط مختلف دنیا وجود دارد که با توجه به نیاز و همچنین شرایط منطقه‌ای طراحی و ساخته شده‌اند.

ازنظرساختمان استاندارد خاصی برای یک Data Center وجود ندارد اما در اینجا سعی شده است به برخی از مشخصات دارای اهمیت یک مرکز داده اشاره شود.

نقش عوامل ساختمانی در امنیت مراکز داده

عوامل مورد بررسي در مکانیابی

عوامل مورد بررسي درطراحی معماری

تهدیدات مراکز داده در زمان بحران

بمب الکترو مغناطیسی (EMP)

درآغاز قرن جدید ، بسیاری از بانکها ، موسسات تجاری ، سیستم های مخابراتی و ... بدون وابستگی به سیستمهای الکترونیکی بی معنی شده اند . در پی این وابستگی ، تهاجم به مدارهای الکترونیکی نیز در برنامه های نظامی و استراتژیک قرار گرفته است

در تخریب و اختلال کلان در شبکه های IT و مدارات الکترونیکی استفاده از انرژی الکترومغناطیسی در مرحله اول قراردارد.

EMP

یک بمب الکترو مغناطیسی سلاحی است که از وابستگی عمیق انسان به برق بهره می برد و بر همین اساس طراحی شده است. با به کارگیری یک نمونه از این بمب های الکترومغناطیسی در یک منطقه ، ژنراتورها از کار خواهند افتاد ، موتور اتومبیل ها دیگر روشن نخواهند شدوحتی امکان برقراری ارتباط تلفنی نیز وجود نخواهد داشت،تمام کامپیوترها ازکارافتاده وتمام اطلاعات آنها ازبین رفته است.

استحکامات و سازه های امن :

ایجاد استحکامات و سازه های امن نقش بسیار اساسی درحفظ تأسیسات ، تجهیزات ، نیروی انسانی ، مراکز حیاتی ، حساس و مهم در زمان بروز بحران ایفاء نموده و می تواند تأثیرات بسیار چشمگیری در حفاظت ازتاسیسات ،اسناد ومدارک خاص در مراکزحیاتی، حساس ومهم کشور داشته باشد

کف های طبقات باید دارای شیب بندی مناسب و زهکش باشند تا در صورت نفوذ یا نشت آب به محوطه سیستم های رایانه ای، آب موجود به خارج از فضا هدایت و زهکش گردد.

بالای کف بتنی سازه ای و در ارتفاع حدود یک متری از آن، برای عبور کابل ها و تجهیزات ارتباطی ، بهتر است از یک کف کاذب که در مقابل وزن کلیه تجهیزات رایانه ای (بیش از ۵۰۰kg/m2) مقاوم باشد، استفاده گردد.

حداقل ضوابط مقاومت در برابر آتش :

ستون ها باید در مقابل ۳ ساعت آتش سوزی، کف ها وبام در مقابل ۲ ساعت و دیوارهای خارجی باید در مقابل ۴ ساعت آتش سوزی مقاوم باشند

بررسی سیستم های تأسیسات الکتریکی مرکز داده :

در صورتیکه قطع برق شبکه طولانی باشد، به یک نیروگاه برق اضطراری نیاز میباشد. ظرفیت این نیروگاه بستگی به وسعت مرکز دارد و بایستی توسط مهندسین مشاور محاسبه و مشخص شود. در صورتیکه ظرفیت و تعداد دیزل ها مناسب انتخاب شوند می تواند صرفه جویی زیادی در هزینه ها داشته باشد. همزمان به تعداد زیادی UPS با ظرفیت مشابه نیاز است تا بتواند تا زمانیکه دیزل ژنراتورها وارد مدار نشده اند برق اضطراری را تأمین کند(حدود ۲۰ ثانیه).

در صورتیکه این مرکز در محل مناسب انتخاب شود می توان برق شبکه را از دو سو به این مرکز آورد تا امکان قطع برق کمتر شود. چنانچه این مرکز در درجه بندی اهمیت کار دارای درجه متوسط یا کم باشد میتوان قطعی برق شبکه را مدت کوتاهی تحمل کرد. اما برای مراکز با درجه اهمیت بالا بایستی امکان بهره برداری از حداقل دو سیستم موازی پیش بینی شود.(N + ۱)

تابلوها،کلیدها و اتاق برق

یک طراحی ضعیف باعث می شود که با کوچکترین مشکلی که در سیستم برق پیش آید کل برق مرکز قطع شود. با توجه به اینکه تغذیه برق از مسیرهای کلیدها و فیوزها می گذردلذا بایستی طراحی و اجرا با کیفیت بالا باشد.

برابر تخمین مصرف برق یک مرکز دیتا می توان برای هر ۱/۰مترمربع ۲۰۰ وات در نظر گرفت. بنابراین برای یک مرکز ۲۰۰۰ مترمربعی حدوداً ۴مگاوات ساعت برق مورد نیاز است. همچنین توسعه مرکز نیز بایستی در نظر گرفته شود. تأمین برق بایستی سه برابر آنچه که در حال حاضر درخواست می شود پیش بینی شود.

مهمترین بخش این مرکز سیستم اتصال زمین آن است که قابلیت اطمینان کار را تا حدود بسیار زیادی بالا می برد. اگر

Patch panel درست چیدمان شود حدود ۳۶ ٪ صرفه جویی در فضای مورد نیاز پیش بینی می شود.

بررسی سیستم های تأسیسات مکانیکی مراکزداده :

یکی از مهمترین عوامل پشتیبانی کننده مراکز دیتا (Date Centers) ، تأسیسات مکانیکی تأمین کننده نیازمندیهای شرایط محیطی ، ملزومات ، تجهیزات و در نتیجه فرآیندهای جمع آوری و پردازش داده ها می باشد.

این مراکز نیازمند سیستم های پیچیده تأسیسات مکانیکی از جمله موارد ذیل خواهند بود :

- تأمین هوا (Make up air)
- تهویه و تجدید هوا (Ventilation & Air change)
- فیلتراسیون و تصفیه هوا (Air Filtration)
- سرمایش و دفع حرارت های زائد (Air cooling & Heat rejection)
- تنظیم و کنترل درجه حرارت و رطوبت فضا (Temprature & Humidity control)
- سیستم های اطفاء حریق (Fire protection systems)
- ذخیره سازی آب (Water storage tank)
- سیستم های آب خنک کن (Cooling water systems)
- ذخیره سازی سوخت (Fuel storage system)

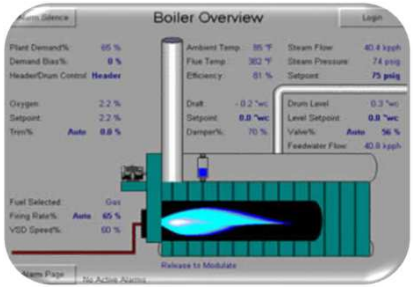
محدوده عملکرد و فعالیت مجاز تجهیزات الکترونیکی ویژه مراکز دیتا به لحاظ درجه حرارت ، رطوبت و پاکیزگی مناسب هوا ، با رجوع به استاندارد ASHRAE Handbook Application عبارتند از :

محدوده درجه حرارت فضا (Temp.) = 22+ 1c (72+2 F)

محدوده رطوبت نسبی مجاز فضا (R.H.) = 50 + 5%

کیفیت فیلتراسیون هوا برای فیلترهای با بستر خشک = 45% , minimum 20%

لذا یکی از مهمترین عوامل محدود کننده فعالیت سیستم این مراکز ، نیاز به سامانه های تأسیساتی فوق الذکر خواهد بود.



- در پاره ای از موارد سامانه های این مراکز به دلیل حجم بالای پردازش و تبادل دیتا نیازمند سیستم آب خنک کن (Cooling water) خواهد بود. تولید این آب نیازمند سیستم های سرمایشی با قابلیت فعالیت در فصول مختلف سال (زمستان و تابستان) ، کیفیت آب جریانی به صورت خاص و سایر پارامترهای مؤثر می باشد.
- در این سامانه ها بحث نشت یابی و تعادل فشار در سیستم فشار آب از اهمیت بسزایی برخوردار است.

- سیستم های تهویه مطبوع و بطور کلی سیستم های تأسیسات مکانیکی به لحاظ حساسیت عملکرد و خدمات پشتیبانی از مراکز دیتا بلحاظ تعدد تجهیزات و بروز شرایط بحرانی دارای(N + □)دستگاه خواهند بود.

استفاده از Shock Isolator جهت کاهش صدمات ناشی از لرزش زمین :

- مکان یابی مناسب فضاهای تأمین تأسیسات مکانیکی مانند موتورخانه های استقرار تجهیزات HVAC (تهویه مطبوع) چیلر و ... ، هواسازها ، مخازن ذخیره سوخت مصرفی دیزل ژنراتور ها و غیره در مراکز دیتا ، چه بلحاظ حفظ ایمنی داخل مرکز و چه بلحاظ رعایت نکات امنیتی از اهمیت بسزایی برخوردار است.
- مانند استفاده از زیرزمین ها ، استحکامات ، ایزولاتورهای شوک (Shock Isolator) ناشی از زلزله یا انفجارات در نصب و استقرار تجهیزات و رعایت نکات ایمنی مندرج در استانداردها ضروری خواهد بود.

A diesel engine operated shelter ventilation unit mounted on VTV2G/35-3000 A shock isolators

- استفاده از سوخت های متنوع یا سیستم های دوگانه سوز برای دیزل ژنراتورها و سیستم گرمایش حرارت مرکزی فضاهای پشتیبانی مراکز دیتا به منظور مقابله با شرایط بحران قابل توصیه است.

- به منظور اجرای کانال کشی مناسب و هوارسانی رفت و برگشت هوای خنک کننده به فضاهای خاص مرکز دیتا ، استفاده از پلنوم (Plenum) کف کاذب یا پلنوم سقف کاذب اجتناب ناپذیر است که در طراحی معماری ، سازه و برق رسانی این فضا تأثیر مستقیم خواهد داشت.

ژنراتور استفاده شده در یک سازه مقاوم که مجهز به سیستم Shock Isolation میباشد

با تشکر از توجه شما