حفـظ امنیـت سـازمان، تنهـا بـر عهـده اداره کل امنیـت اطلاعـات نیسـت و هر کارمند بسـته به سـطح دسترسـی به دارایی های اطلاعاتی سـازمان و وظایف محول شده، مسئول حفظ امنیت اطلاعات تحت اختیار خود است.

حفظ امنیت، وظیفه همه کارکنان است

همه در برابر حفظ امنیت اطلاعات مسئولیم

اطلاعات

یک دارایی ارزشمند برای سازمان است و باید به شکلی مناسب محافظت شود.

لزوم برقراری امنیت برای سازمان

- جلوگیری از بروز زیان مالی و اختلال در کسب و کار
- حفظ اعتبار و شهرت سازمان
- افزایش اعتماد مشتریان و سرویس گیرندگان
- پیروزی در رقابت تجاری با رقبا
- مقابله با تهدیدات ملی و بین المللی

انواع دارایی های اطلاعات

انواع دارایی های اطلاعات

اطلاعـات دیجیتـال (ماننـد: بانـک هـای اطلاعاتـی، نـر م افزارهـا، سـامانه ها و سـایت هـای داخلـی اطلاعـات فایـل قراردادهـا با مشـتریان و پیمانـکاران، اطلاعـات ذخیـره شـده بـر روی رسـانه هـای قابل حمـل و ....)

اطلاعـات ملمـوس کاغـذی (ماننـد: نسـخه کاغـذی قراردادهـا بـا مشـتریان و پیمانـکاران، مشـخصات هویتـی و اطلاعات مشـتریان، نامه هـا و اطلاعیه های بانکـی و ...)

اطلاعـات غیرملمـوس (مانند: سـرمایه های فکری سـازمان، دانـش، تجربیات و مهـارت هـای کارکنان، حقـوق مالکیـت، برند سـازمان، اطلاعات اسـتراتژ ی ها، روند انجـام کارهـا و فرآیندها و...)

خطراتی که دارایی های اطلاعاتی را تهدید می کنند و را ه های پیشگیری از هر کدام

	تهدیدات	راه های مقابله با تهدیدات
	**جعل هویت (Spoofing)** تظاهـر کردن بـه هویت شـخصی دیگر	• استفاده از کلمه عبور پیچیده (ترکیبی از حروف بزرگ و کوچک، اعداد و کاراکترهای خاص) برای حسا ب های کاربری و تغییر مداوم آن در باز ه های زمانی مشخص • پاسخ ندادن به هرگونه پیام ناشناس و مشکوک در فضای مجازی، که از شما درخواست ورود اطلاعات شخصی یا مالی می کنند • محافظت از کلمه عبور و عدم افشاء و اشترا ک گذاری آن با دیگران
	**افشای اطلاعات (Information disclosure)** ارائـه اطلاعـات به شـخصی که مجاز به دسترسی به آن نیست	• محافظت از اسناد طبقه بندی شده و عدم افشاء و اشترا ک گذاری آن با افراد غیر مجاز
	**محرومیت از سرویس (Denial of service)** خـراب کـردن یـا اختـلال در سـرویس بـرای جلوگیـری از ارائـه خدمـات	• تهیه نسخه پشتیبان از دارایی های اطلاعاتی مهم • بروزرسانی سیستم عامل و برنامه های کاربردی • استفاده از نرم افزار آنتی ویروس و اطمینان از به روز بودن آن

آمارجرائم و رخدادهای سایبری

• تعداد حملات باج افزارها که منجربه رمز گذاری اطلاعات کاربران گردیده است: (Statista)

سال	تعداد حمله (اعداد به میلیون می باشد)
۲۰۱٤	۳/۲
۲۰۱۵	۳/۸
۲۰۱٦	٦۳۸
۲۰۱۷	۱۸٤
۲۰۱۸	۲۰٤/۲٤
۲۰۱۹	۱۸۷/۹

• پیش بینی می گردد که هزینه سالانه خسارت های جرائم سایبری از ۳ تریلیون دلار در سال ۲۰۱۵ به ٦ تریلیون دلار در سال ۲۰۲۱ افزایش خواهد یافت. (Cybersecurity Ventures)

• پیش بینی ها حاکی از آن است که در یک بازه زمانی ۵ ساله، از سال ۲۰۱۸ تا ۲۰۲۳، حدود ۱٤٦ میلیارد رکورد اطلاعاتی افشا خواهد شد و این میزان در سال ۲۰۲۳ از رشد ۱۷۵٪ در مقایسه با سال ۲۰۱۸ برخوردار خواهد بود. (میزان افشاء اطلاعات در سال ۲۰۱۸ برابر ۱۲ میلیارد رکورد اطلاعاتی بوده و پیش بینی می گردد در سال ۲۰۲۳ به ۳۳ میلیارد رکورد در سال افزایش یابد.) (Juniper)

• بنابر بررسی محققان دانشگاه مریلند در سال ۲۰۱۹، هکرها هر ۳۹ ثانیه یکبار از طریق اینترنت تلاش می کنند، که به رایانه های دیگران حمله کنند. (Security Magazine)

بانک ملت
bank mellat

تجربه ای متمایز