لایحه وظایف پست‌های خدمات ملکی

معلومات کلی پست

شماره اعلان پست:	
عنوان وظیفه:	تحلیلگر حملات سایبری
بست:	۴
وزارت یا اداره:	مخابرات وتکنالوژی معلوماتی
بخش مربوطه:	ریاست عمومی زیربنا های تکنالوژی معلوماتی
موقعیت پست:	مرکز
تعداد پست:	۲
گزارشده به:	ریاست امنیت سایبری
گزارش‌گیر از:	ندارد
کد:	
تاریخ بازنگری:	

هدف وظیفه: شناسایی، تحلیل و بررسی نقاط آسیب پذیر و رفع مشکلات امنیتی به منظور داشتن یک سیستم مطمین در کشور .

صلاحیت و مسئولیت های وظیفوی:

وظایف تخصصی

۱. تحلیل حالت فعلی و شناسایی نقاط ضعف سیستم و شبکه کمپیوتری وزارت مخابرات و تهیه راپور جامع از آن.
۲. راه اندازی و پیشبرد فعالیت های پاسخگویی به حوادث کمپیوتری (Computer Incident Response Team) .
۳. اجرای تست خلا امنیتی (Penetration Testing) و Security Assessment بالا ی منابع آنلاین دولتی و کمپنی های خصوصی جهت جمع آوری نقاط آسیب پذیر سایبری ورسیدگی به موقع جهت رفع آن.
۴. کشف جدید ترین نقاط آسیب پذیر امنیتی شبکه و تحت وب و رسیدگی به موقع جهت رفع آنها.
۵. ایجاد پلان، راه اندازی سیستم های مدرن و نوآوری در عرصه تآمین امنیت سایبری و جدید سازی سیستم ها.
۶. نظارت دوامدار از فضای سایبری کشور جهت جلوگیری از حملات سایبری (حملات سایبری Dos، DDOS، ransomware، malwares وغیره) .
۷. همکاری در پروسه تفتیش وضعیت سایبری در کشور جهت شناسایی خلا های موجود در زیربنای سیستم های تکنالوژی معلوماتی .
۸. همکاری در قسمت ترتیب پالیسی ها، طرزالعمل ها و رهنمود های تحقیق جرایم سایبری و تحلیل در مطابقت با استندرد های بین المللی.
۹. تحقیق و تحلیل تهدیدات سایبری و ارایه رهنمود های محافظتی جهت آگاهی دهی عامه و درج آن در پلتفورم آگاهی دهی .
۱۰. مطالعه ، دریافت و نشر معلومات نوین در باره خطرات سایبری در کشور.

۱۱. تحقیق و اطلاع رسانی جدیدترین آسیب پذیری های امنیتی و نشر قوانین و پالیسی های امنیت و جرایم سایبری کشور.

وظایف مدیریتی:

۱. ترتیب پلان کاری ماهوار، ربعوار و سالانه در مطابقت با پلان عمومی، بمنظور رسیدن به اهداف تعیین شده اداره.
۲. ارائه گزارش ماهوار، ربعوار، سالانه و عندالضرورت از فعالیت ها و دست آورد های مربوطه، بمنظور مطلع ساختن رهبری وزارت/اداره.
۳. ترتیب راپور تحلیلی حملات سایبری سیستم های الکترونیکی به امریت تیم عکس العمل سریع سایبر.
۴. اجرای سایر وظایف که از طرف مقامات ذیصلاح مطابق قوانین، مقررات و اهداف وزارت/ اداره مربوطه سپرده میشود.

وظایف هماهنگی

۱. هماهنگی با ادارات جهت شناسایی ، کشف نقاط ضعف، تحلیل و ارایه راهکار های مناسب برای رفع خلا های امنیتی سیستم های زیربنای تکنالوژی معلوماتی.
۲. هماهنگی با ادارات کشور های منطقه و بین المللی جهت ارتقای ظرفیت و دریافت راهکار های جدید تحقیق و استفاده وسایل و ابزار ها مورد نیاز.
۳. همکاری در زمینه ترتیب و انکشاف استراتیژی امنیت سایبری و قوانین سایبری با ادارات دولتی و خصوصی.

(شرایط استخدام (سطح تحصیل و تجربه کاری):

۴. این لایحهٔ وظایف با در نظر داشت مواد ۷، ۸و ۳۴ قانون کارکنان خدمات ملکی با حد اقل شرایط و معیارهای ذیل ترتیب گردیده است:
۵. داشتن حداقل سند تحصیلی لیسانس در یکی از رشته های: کمپیوتر ساینس ، تکنالوژی معلوماتی و سایبر سکیورتی و سایر رشته های مرتبط و به درجه تحصیلی بالاتر در رشته های متذکره ارجحیت داده میشود.
۶. تجربه کاری مرتبط یک سال
۷. تسلط به یکی از زبان های رسمی(پشتو یا دری)و (تحریر و تکلم) با زبان انگلیسی.

۱- مهارت های مسلکی:

- ✓ مهارت عالی در نوشتن گزارش استندرد (Vulnerability Report) از خلاء ها و نقاط آسیب پذیر
- ✓ مهارت و توانمندی عالی در ساختن پلان و پالیسی (Penetration Testing)
- ✓ آشنایی با سافت ویر های تست خلاء امنیتی (Penetration Test)
- ✓ آشنایی با ابزار های مختلف تحلیل حملات سایبری (ویب، شبکه و موبایل)
- ✓ بلدیت کامل با سیستم های عامل لینوکس خاصتا Kali Linux، Parrot و غیره
- ✓ آشنایی با استندرد های امنیت سایبری ISO, Offensive Security، SANS ، PCI-DSS ، e-learn Security
- ✓ آشنایی با Port Scanner، Vulnerability Scanner و Application Scanner
- ✓ توانایی در تهیه راپور از اجرای تست امنیتی مطابق استندرد های بین المللی