راهنمای امنیتی

Security guideline

نکات امنیتی دورکاری کارکنان در سازمان ها

2020 (۱۳۹۹)

Version 1.0

www.ojan.org

Security guideline

شرکت مهندسی اوژن تدبیر پارس
Pars OJAN Counsel Eng. Co
www.ojan.org

راهنمای امنیتی

نکات امنیتی دورکاری کارکنان در سازمان‌ها

قبل از مطالعه بدانید

در این راهنما به درست/نادرست بودن دورکاری اشاره ای نگردیده، زیرا که سیاست‌ها و نیازهای سازمان‌ها متفاوت است. پس با فرض اینکه به این نتیجه رسیده اید که دورکاری در شرکت یا سازمان شما انجام گردد، می‌توانید از این راهنما در خصوص افزایش امنیت انجام دورکاری استفاده بفرمایید.

یادآوری: این مستند بروز می‌شود.

مخاطبین

+ مدیران و کارشناسان فناوری اطلاعات
+ مدیران و کارشناسان امنیت اطلاعات
+ مدیران و کارشناسان حراست

ضرورت نیاز به دورکاری

امروزه بسیاری از سازمان‌ها و شرکت‌های دولتی و خصوصی در ایران به دلیل گسترش بیماری واگیردار کرونا و همچنین با هدف حفظ سلامت نیروی انسانی و پیشگیری از همه‌گیر شدن این بیماری در کشور، به کارکنان خود اجازه داده اند تا مسئولیت ها و وظایف محوله خود را در خانه و به صورت دورکاری انجام دهند.

چالش های امنیتی دورکاری

انجام دورکاری مستلزم اجرا و تامین پاره‌ای از الزامات امنیت سایبری از سوی کارکنان می‌باشد که در این مستند به‌بیان این الزامات در حوزه‌های زیر پرداخته شده است:

- کلان امنیت سایبری
- کاربران مجاز
- ایمیل های فیشینگ
- حریم خصوصی
- جلسات و تماس های آنلاین
- رسیدگی به رخداد و حملات سایبری
- پشتیبان گیری

جهت سهولت مطالعه مخاطبین عزیز، الزامات امنیتی بصورت چک لیست تهیه و ارائه می‌گردد.

کلان امنیت سایبری

- اطمینان حاصل شود که لپ‌تاپ‌ها/ تجهیزات، دارای رمزگذاری سخت‌افزاری می‌باشد.

- در صورت امکان، از کارکنان خواسته شود که از فیلترهای صفحه‌نمایش [1] به‌منظور سخت‌تر کردن حملات Shoulder-Surfing [2] استفاده شود و یا اینکه دقت نمایند در محیطی که فعالیت می‌کنند، فردی به صفحه نمایش آنها اشراف نداشته باشد. (تحت هیچ عنوان تصویری از صفحه نمایش خود در حال کارکردن در فضای مجازی منتشر ننمایند.)

- می‌بایست در صورت امکان برای تمام کارکنانی که دورکاری می‌کنند، احراز هویت ۲ عاملی اجباری گردد (به خصوص در دسترسی به مواردی از قبیل ایمیل و سیستم‌ها و برنامه‌های کاربردی حیاتی). چنانچه از قبل تدابیری اندیشیده نشده، اکنون بهترین زمان برای انجام این کار است.

- کارمندان را تشویق کنید که از ابزارهای مدیریت رمز عبور بر روی دستگاه‌های خود استفاده نمایند.

- به کارمندان تاکید گردد که حتما از سیاست های رمز عبور پیچیده برای تعیین رمزهای عبور خود استفاده نمایند.

- به کارمندان تذکر داده شود که در صورت مشاهده لینک‌ها و مستندات مرتبط با کروناویروس بر روی سیستم و ایمیل خود، به هیچ عنوان اقدام به باز نمودن آن نکرده و مراتب را هر چه سریعتر به سازمان گزارش دهند.

- در خصوص محرمانه بودن اطلاعات سازمان و همچنین لزوم حفظ محرمانگی آنها به کارکنان تذکرات لازم داده شود. همچنین بیان گردد که مسئولیت حفظ محرمانگی این اطلاعات برعهده کارکنان بوده و در صورت قصور در انجام آن ، می‌بایست پاسخگو باشند.

- از کارمندان خواسته شود تا به روزرسانی‌های مهم نرم‌افزاری سیستم خود را به تعویق نیاندازند و همواره سیستم خود را بروز نگهدارند.

- کارکنان به هیچ‌وجه نباید از سایت‌هایی مانند وبسایت‌های فیلم غیرقانونی و همچنین حاوی مطالب غیر اخلاقی بازدید کنند زیرا ممکن است بر اثر آن، سیستم آنها به باج افزار و یا سایر نرم‌افزارهای مخرب آلوده گردد.

[1] Screen Filters

[۲] این حملات نوعی تکنیک مهندسی اجتماعی است که مهاجم برای بدست آوردن اطلاعاتی از قبیل شماره شناسایی شخصی (PIN)، گذرواژه‌ها و سایر اطلاعات محرمانه، اقدام به نشستن در کنار قربانی و تماشای بدون اجازه صفحه نمایش دستگاهی که قربانی درحال کار کردن با آن است، می کند.

- از کارمندان خواسته شود تحت هیچ عنوانی، رایانه‌ای را که برای دورکاری استفاده می‌نمایند در اختیار فرزندان و سایر اعضای خانواده (حتی برای چند لحظه) قرار ندهند.

- با توجه به اینکه دورکاری ممکن است منجر به اشتراک‌گذاری بیشتر رمزهای عبور گردد لذا می بایست بر اهمیت عدم به اشتراک‌گذاری رمز عبور با سایرین حتی اعضای خانواده، تاکید و پافشاری گردد.

- به کارکنان یادآوری شود که آنها مسئول رفع مشکلات فنی نیستند و نباید خودسرانه اقدام به رفع آن نمایند چرا که ممکن است مخاطرات بیشتری به همراه داشته باشد، لذا تنها کافی است به سازمان این موارد را اطلاع دهند.

- از کارکنان خواسته شود در صورت امکان از شبکه‌های سیمی برای برقراری ارتباطات اینترنتی استفاده نمایند. یا در صورت استفاده از شبکه WIFI حتما پیش از استفاده، اقدام به امن سازی آن نمایند (بهتر است در این خصوص راهنماهای امنیتی به کاربران ارائه شود).

- برای برقراری ارتباط راه‌دور با سیستم‌ها و شبکه‌های سازمانی، حتما از اتصالات VPN مورد تایید سازمان استفاده گردد و تحت هیچ عنوانی پورت های مدیریتی و راه دور از قبیل VNC، RDP و SSH به طور مستقیم از اینترنت قابل دسترس نباشد.

- از نصب آنتی ویروس و بروز بودن آن در رایانه ای را که برای دورکاری استفاده می‌نمایند، اطمینان حاصل بفرمایید.

کاربران مجاز

- اطمینان حاصل کنید که به تمام کاربران مجاز کسب و کار و فناوری اطلاعات سازمان تذکرات لازم داده شده است و :
  - **به کلیه کارکنان مسئولیت هایشان را یادآوری کنید.**
  - **از کارکنان بخواهید که برای انجام کارهای عادی روزمره خود، هیچ‌گاه از طریق کاربری با سطح دسترسی بالا در سیستم لاگین نکنند.**
  - **از کارکنان بخواهید تا تمامی خطاهای سیستمی و اشتباهات انسانی خود را فورا به سازمان گزارش نمایند.**
  - **لیست کاربران متصل به سرورها و استفاده‌کنندگان از پروتکل های ارتباط از راه دور، با لیست کاربران مجاز به صورت تصادفی چک شود. بهتر است لاگ کلیه اتصالات ذخیره گردد.**

ایمیل های فیشینگ

- به کارمندان یادآوری شود که هر شخصی ممکن است اشتباه کند و در صورتی که به هر دلیلی مرتکب یکی از کارهای زیر شده هرچه سریعتر موضوع را به اطلاع سازمان برساند:
  - **در صورتی که به صورت تصادفی بر روی یک لینک یا فایل مشکوک کلیک گردد.**
  - **یا یک فایل اکسل، PDF و یا ورد حاوی ماکرو باز گردید.**
- کارکنان می‌بایست بلافاصله آلودگی‌های بدافزاری/باج افزاری خود را گزارش نمایند.

حریم خصوصی

- به کلیه کارکنان در خصوص مسئولیت خود در قبال حفظ حریم خصوصی مشتریان و کارکنان سازمان تذکرات لازم داده شود.
- به واحدهای فناوری اطلاعات و امنیت سایبری اطلاع داده شود تا بر روی فعالیت های مخرب احتمالی بر روی حساب های کاربری بسیار هوشیار باشند.
- به کارکنان اعلام شود که از ارسال اطلاعات سازمان از طریق ایمیل شخصی و یا ذخیره آنها در فضاهایی که مورد تایید نمی باشند، اجتناب کنند.
- از کارکنان خواسته شود که از بکارگیری ابزارهای ارتباطی از قبیل، Telegram، Whatsapp Linkedin یا هر ابزار ارتباطی شخصی برای دورکاری و تبادل اطلاعات سازمان اجتناب گردد و تنها از ابزارهای مورد تایید سازمان برای این منظور استفاده شود.
- ممکن است کارکنان نیاز به تبادل شماره تلفن یا ایمیل با همدیگر داشته باشند. از کارکنان خواسته شود که حتی الامکان از این کار بپرهیزید یا اینکه از آنها بخواهید عبارت "بعدا پاک شود" را در ابتدای نام آنها اضافه کنند البته اگر جزییات را ذخیره می نمایند.

جلسات وتماس های آنلاین

- به کارکنان یادآوری شود که زمانیکه در یک تماس کنفرانسی صحبت نمی‌کنند، میکروفون خود را قطع کنند.
- می‌بایست به تمامی کارکنان آموزش داده شود تا این اطمینان حاصل گردد که تمامی وب‌کم ها به صورت پیش فرض مسدود شده اند (این کار می تواند بصورت فیزیکی و با یک برچسب صورت پذیرد).

- می‌بایست به تمامی کارکنان گفته شود که سیستم های باز و لاگین شده خود را خصوصا در زمان تماس و یا مشاهده مستندات مهم، به هیچ عنوان ترک نکنند و پیش از ترک، سیستم خود را قفل[1] نمایند.

- از کارکنان خواسته شود که یک مکان مستقل برای انجام دورکاری خود انتخاب نموده و از اماکن عمومی و کافی‌شاپ ها به خصوص در زمان برقراری تماس محرمانه و یا کار بر روی اسناد محرمانه، اقدام به دورکاری ننمایند.

۱ Lock

رسیدگی به رخداد و حملات سایبری

- دائما به کارکنان یادآوری کنید که نسبت به ایمیل فیشینگ و سایر تلاش ها برای به خطر انداختن/سرقت اطلاعات حساب کاربری خود هوشیار باشند.

- به کارکنان تاکید گردد که در صورت مشاهده این ایمیل ها و فعالیت های مخرب بلافاصله مراتب را گزارش نمایند. به منظور اطلاع می بایست راهکار مناسب ایمیل یا شماره تلفن در اختیار کارکنان قرار گیرد.

- از کارکنان خواسته شود تا در صورت نیاز با ذی نفعان و واحدهای مربوطه سازمان تماس بگیرند.

- کارکنان واحدهای امنیت سایبری سازمان می بایست هوشیار بوده و به طور فعال به دنبال فعالیت های مشکوک باشند (با توجه به عادت های کار کردن از راه دور کاربران ممکن است این فعالیت از نظر عملیاتی برای سازمان گران باشد).

- از پرسنل و کارکنان واحد فناوری اطلاعات و امنیت سایبری سازمان خواسته شود که اگر موضوعی مهم می باشد به جای آنکه تنها به ایمیل اکتفا کنند، تلفن را انتخاب کرده و تماس بگیرند.

- به کارکنان تذکر داده شود که در زمان دورکاری، دیگر واحدهای سازمانی در کنار شما حضور ندارند، بنابراین می بایست هرگونه درخواست برای به اشتراک گذاشتن داده های محرمانه یا انتقال وجوه را حتی در صورتی که از طریق ایمیل نیز ارسال شده باشد، پیش از انجام با درخواست کننده تماس گرفته و تاییدیه ایشان دریافت شود.

- از کارکنان خواسته شود تا یک نسخه چاپی از روال ها و چک لیست های خود در منزل به همراه داشته باشند و مطمئن باشند که این مستندات در دسترس دیگران قرار ندارد.

- به تمامی کارکنان یادآوری شود که بروز اشتباهاتی از قبیل ارسال ایمیل به گیرندگان اشتباه، کلیک بر روی لینک های مخرب و مواردی از این دست، ممکن است برای همه اتفاق بیافتد و آنها باید بلافاصله بروز این اشتباهات را به سازمان اطلاع بدهند. همچنین تاکید گردد که در صورت گزارش فوری، در اکثر موارد عواقب ناگواری برای آنها به همراه نخواهد داشت.

- سازمان ها می بایست اقدام به مانیتورینگ کلیه اتصالات و دسترسی های راه دور خود نمایند.

پشتیبان گیری

- برای کارکنان، نرم افزاری برای اطمینان از پشتیبان گیری از اسناد مهم فراهم نمایید.

- از کارمندان بخواهید تا از داده های خود در یک دیسک سخت خارجی تأیید شده که به طور دائم به دستگاه متصل نیست، پشتیبان تهیه نمایند.

- از کارکنان خود بخواهید تا به هیچ عنوان از خدمات ذخیره ساز ابری خارجی ، استفاده نکنند.

- از کارکنان خواسته شود تا در مورد هر نوع ذخیره سازی ابری یا راهکارهای سرویس ابری که می‌خواهند از آنها استفاده کنند، پیش از استفاده از سازمان تاییدیه‌های لازم را دریافت نمایند و بدون دریافت تاییدیه به هیچ عنوان از آنها استفاده نکنند.

به عنوان گروهی توانمند در حوزه‌های خدمات فناوری اطلاعات و ارتباطات ایجاد شده است و با بهره گیری از ارتباطات گسترده بین المللی و تکیه بر دانش فنی بومی، از سال ۱۳۹۱ پا به عرصه فعالیت نهاده است و خدمات ارزنده ای را در زمینه‌های مختلف فناوری اطلاعات در سه حوزه امنیت اطلاعات، شبکه و آموزش ارائه نموده است.

خدمات شرکت

حوزه امنیت Security

حوزه شبکه Network

حوزه آموزش
Education

- شناسایی نقاط ضعف سیستم های آموزشی موجود و ارائه راهکار
- مشاوره صحیح و هدفمند در راستای آموزش افراد و تدوین مسیر راه آموزشی
- ارائه آموزش های در محل سازمان
- ارائه ارزیابی ۳۶۰ درجه
- برگزاری سمینارها، کارگاه ها وهمایش های علمی
- ارائه آموزش های ضمن خدمت متناسب با موقعیت شغلی
- ارائه بسته های آموزشی دیجیتال
- برگزاری تورهای آموزشی
- متخصص پروری و دانش افزایی در حوزه امنیت شبکه و اطلاعات
- سفارشی سازی دوره های آموزشی متناسب با نیاز سازمان ها

SANS EC-Council Microsoft Linux Professional Institute ISACA CISCO vmware MikroTik CompTIA

دوره های شبکه
- CompTIA (NET+,SEC+,...)
- Cisco (CCNA,CCNP,...)
- MikroTIK (MTCNA,MTCRE,...)
- Microsoft (MTA,MCSA,...)
- LPI (LPIC1,LPIC2,...)

دوره های برنامه نویسی
- Web Programming
- System Programming
- Database
- Mobile Programming
- Network Programming

دوره های امنیت
- EC-Council (CEH,CHFI,...)
- SANS (SEC511,SEC504,...)
- ISACA (CISM,CISA,...)
- OFFENSIVE Security (PWK,...)

دوره های فناوری نوین
- کلان داده
- اینترنت اشیاء
- بلاک چین

مجوزهای شرکت

- عضویت سازمان نظام صنفی رایانه‌ای استان تهران
- اخذ رتبه شورای عالی انفورماتیک
- اخذ مجوز افتا (سازمان فناوری و اطلاعات)
  - پیاده‌سازی مرکز عملیات امنیت و تیم پاسخ به رخداد
  - آزمون و ارزیابی امنیتی
  - خدمات آموزش افتا
- اخذ مجوز آموزش از سازمان پدافند غیرعامل (پدافند سایبری)
- اخذ مجوز سازمان برنامه و بودجه (آموزش)
- اخذ مجوز حراست نفت

امیدواریم در این ایام با حفظ مسائل امنیتی و رعایت کل نکات، بتوانید با خاطری آسوده به کسب و کار خود ادامه دهید.

واحد عملیات امنیت و مدیریت رخدادهای امنیتی شرکت اوژن تدبیر پارس در این ایام بصورت شبانه روزی در خدمت شماست تا در صورت نیاز به مشاوره و یا بروز مشکل در کنار شما باشد.

Cert@ojan.org

تماس با ما

021-22119220-22

Clickpro.ir

Info@ojan.org

www.Ojan.org
www.Csirtpro.ir
www.Clickpro.ir

دفتر مرکزی: تهران، سعادت آباد، انتهای خیابان ۲۵ (قره تپه ای) ، پلاک ۱۱۶ - طبقه ۳ (واحد ۴)