بررسی وضعیت امنیت شبکه و سامانه ها ی

دانشگاه امام صادق (ع)

نوع سند: محرمانه و غیر قابل انتشار

تاریخ تهیه : تیر ماه ۱۳۹۷

فهرست

۱- مقدمه..... ۱

۲- هدف..... ۲

۳- نحوه جمع آوری اطلاعات..... ۲

٤- آسیب شناسی حمله و نفوذ صورت گرفته..... ۲

٥- وضعیت فعلی..... ۳

٦- اقدامات ضروری جهت ایمن سازی مورد نیاز..... ٥

۷- الزامات و توصیه های عمومی..... ۱۱

۸- خلاصه و نتیجه گیری..... ۱۳

بررسی وضعیت امنیت شبکه و سامانه ها

دانشگاه امام صادق (ع)

تاریخ تهیه: تیر ماه ۹۷

نوع سند: محرمانه و غیر قابل انتشار

۱ - مقدمه:

تهدیدهای متنوع و پیچیده سایبری در دنیای امروز دغدغه همه کسب و کارها شده است. اگر چه تصور بر این بوده که موضوع امنیت سایبری و ریسک های امنیت اطلاعات چالشی محدود به واحد فناوری اطلاعات است، اما این دیدگاه امروزه تغییر کرده است. ریسک های سایبری می توانند همانند ریسک های سنتی، کل کسب و کار را تحت تاثیر قرار دهند. رشد تعداد و پیچیدگی حملات از یک طرف و اثرات مخرب آن بر کسب و کار از طرف دیگر موجب شده که بسیاری از سازمان ها موضوع مدیریت ریسک های امنیت سایبری را مانند دیگر ریسک های کسب و کار در سطح مدیریت ارشد سازمان دنبال نمایند.

همچنین با توجه به گسترش فناوری های مجازی، موبایل و اینترنتی به عنوان بستر ارائه خدمات و با نگاه به روند جهانی فناوری اطلاعات و امنیت، افزایش تعداد و ابعاد حوادث در سال های آتی قابل پیش بینی است. در ایران هم در سال های اخیر نمونه هایی از خسارات وارده به سازمان ها و مشتریان آنها ناشی از حملات و سوء استفاد های سایبری گزارش شده هر چند آمار دقیقی از اینگونه حوادث داخل کشور در دسترس نیست اما بدون شک تعداد و گستره آنها در چند سال گذشته رشد داشته و افزایش ابعاد آن در آینده نیز مانند دیگر روندهای جهانی فناوری اطلاعات قابل پیش بینی است.

لذا سازمان با پذیرش این واقعیت باید به سمت تقویت امکانات و محدودسازی تهدیدها حرکت کند. سازمانی موفق است که تا آنجا که ممکن است در جهت پیشگیری از تهدید ها حرکت کرده و در خصوص باقی تهدید ها بتواند در زمان مناسب، عکس العمل مناسب را در جهت محدودسازی و رفع اثرات مخرب آن به کار بندد.

۲- هدف:

هدف از این گزارش بررسی وضعیت امنیت شبکه و سامانه های دانشگاه امام صادق (ع) به منظور شناسایی آسیب پذیری ها و نقاط ضعف سامانه ها با رویکرد بهبود و ارتقاء وضعیت فعلی به سطح متعارفی از امنیت به منظور پیشگیری از بروز و تکرار حملات و رخدادهای شناسایی شده، محدود سازی دامنه حملات و آسیب ها و حفظ دارایی های مادی و معنوی سازمان می باشد.

بدیهی است امنیت امری نسبی است که همواره احتمال جزئی مبنی بر بروز رخدادهای امنیتی وجود دارد ولیکن همواره با رعایت استانداردها و اجرای مداوم فرآیندهای مربوطه وضعیت امنیت سازمان ها در بالاترین سطح حفظ می گردد و احتمال بروز خسارات ناشی از حملات را کاهش می دهیم.

۳- نحوه جمع آوری اطلاعات:

- مصاحبه با کارشناسان بخش فناوری اطلاعات دانشگاه
- بررسی میدانی مرکز داده (Data Center) دانشگاه
- بررسی تنظیمات تجهیزات، سرور ها و سامانه ها
- تست وب سایت ها با استفاده از ابزارها

٤- آسیب شناسی حمله و نفوذ صورت گرفته:

در تاریخ ۵ اسفند سال ۱۳۹۶ ساعت ۴ بامداد سازمان تحت حمله و نفوذ باج افزاری با نام Crypto Night قرار گرفته که منجر به رمزنگاری اطلاعات سامانه های حیاتی گردیده و با تلاش بخش فناوری اطلاعات تا پایان فروردین ماه سال ۱۳۹۷ بخشی از داده ها رمزگشایی گردیده است.

با توجه به بررسی های بعمل آمده، احتمال حمله مزبور از طریق سرور ایمیل به دلیل عدم کنترل و مدیریت صحیح پورت های باز از طریق پروتکل RDP (Remote Desktop Protocol) وجود دارد که به علت ضعف استراتژی تهیه پشتیبان و عدم وجود Zone بندی بین سرورها، پس از وقوع حمله نسخ پشتیبان نیز مورد نفوذ قرارگرفته و بلااستفاده گردیده اند.

۵- وضعیت فعلی:

وضعیت شبکه، ارتباطات و سامانه های دانشگاه با برگزاری جلسات حضوری و بر اساس اظهارات آقایان مهندس عبداللهی و آذرنگ مورد بررسی قرار گرفته که به شرح ذیل می باشد:

۵-۱- تیم فناوری اطلاعات سازمان شامل ۹ نفر بوده که از این تعداد ۶ نفر به صورت تمام وقت و ۳ نفر به صورت پاره وقت با سازمان همکاری می نمایند.

۵-۲- دیتا سنتر سازمان دارای سیستم اعلام و اطفاء حریق با گاز FM200، کولینگ های In Row، کف کاذب، Access Control به منظور کنترل دسترسی فیزیکی و دو دستگاه UPS با توان ۸۰ KVA است. همچنین طبق اظهار کارشناسان بخش فناوری اطلاعات، دانشگاه دارای ژنراتور مجزا برای تجهیزات بخش فناوری اطلاعات می باشد که امکان بازدید آن فراهم نگردید.

۵-۳- کلیه کاربران درونی و بیرونی سازمان برای دسترسی به کلیه سامانه های مورد نیاز می بایست از UTM موجود سازمان عبور نمایند که پس از آن سرورهای مربوطه به صورت Zone بندی نشده قرار گرفته اند.

۵-۴- بر اساس بررسی تنظیمات UTM منصوب، دسترسی به سامانه ها و تجهیزات از بیرون سازمان از طریق پروتکل های Telnet و SSH همچنین پروتکل SMB ویندوز نیز مسدود گردیده است.

۵-۵- وضعیت آنتی ویروس های منصوب در سازمان به شرح ذیل می باشد:

- سرور ها آنتی ویروس F-Secure لایسنس دار
- کلاینت ها آنتی ویروس کسپرسکی لایسنس دار
- سرور ایمیل آنتی ویروس سیمانتک بدون لایسنس

۵-۶- اینترنت سامانه ها و کاربران داخلی از طریق دو POP Site شرکت رسپینا با مجموع پهنای باند ۱۳۰ مگابیت تا ساعت ۱۷ و ۱۶۰ مگابایت از این ساعت تا صبح روز بعد تامین می گردد.

این پهنای باند بیشتر چه نیازی را برآورده می کند

۷-۵- Active Directory در سازمان فعال می باشد که برای اعمال سیاست ها، دسترسی ها و بروز رسانی ها مورد استفاد قرار می گیرد.

۸-۵- سازمان دارای مجوز بهره برداری SSL تا سال ۲۰۲۰ از موسسه Certum می باشد که در سایت های تحت وب مورد استفاده قرار گرفته و بر اساس تست ها و بررسی های انجام شده در حال حاضر تنظیمات مربوطه به منظور پیشگیری از حملات به درستی انجام پذیرفته است که نتیجه برخی تست ها توسط ابزار مرکز محترم ماهر مطابق ۱۰ برگ پیوست گزارش تقدیم می گردد که بر اساس تست صورت گرفته دامنه isu.ac.ir و زیر دامنه های آن متعلق به دانشگاه تا تاریخ تست نسبت به حمله های Man in the middle، ROBOT، Drown، POODLE آسیب پذیر نمی باشد و Cipher Suite های تنظیم شده و پروتکل های رمز نگاری در حالت بهینه تنظیم گردیده اند. ولیکن دامنه دانشگاه از قابلیت Strict Transport Security پشتیبانی نمی کند که به دلیل وجود زیر دامنه های HTTP برای دامنه فوق الاشاره اجتناب ناپذیر است.

۹-۵- پشتیبان لحظه ای (Mirror) کلیه سامانه های اصلی بر روی دیسک تهیه می گردد و هر یک ساعت پشتیبان برروی دیسک هایی در Zone مجزا گرفته می شود و پشتیبان بر روی Tape به صورت ماهانه گرفته می شود که توصیه می گردد به صورت هفتگی یا حداکثر هر دو هفته یکبار اخذ گردد. برای هر سامانه حداقل آخرین سه نسخه قبلی بر روی دیسک و Tape نگهداری می شود.

لازم به ذکر است که قبل وقوع حمله وضعیت پشتیبان گیری سامانه ها به شرح فوق نبوده است و این بهبود پس از حمله ایجاد گردیده است.

۱۰-۵- بر اساس فرم های تکمیل شده "شناسنامه سیستم های نرم افزاری و سرویس ها" که در اختیار بخش انفورماتیک سازمان قرار داده شد، هیچ یک از سامانه ها با یکدیگر از طریق وب سرویس یا سوکت ارتباط نداشته و کلیه سامانه ها به صورت مستقل عمل می نمایند.

خاطر نشان می سازد که در صورت استفاده از وب سرویس ها در هر زمان می بایست الگوهای امنیتی مربوطه لحاظ گردد.

٦- اقدامات ضروری جهت ایمن سازی مورد نیاز:

با توجه به وضعیت موجود به منظور ارتقاء و بهبود وضعیت امنیت انجام و توجه به موارد ذیل ضروری می باشد:

۱-۶- با توجه به اینکه کلیه سامانه های آن سازمان تحت وب می باشد و دسترسی کلیه کاربران از طریق اینترنت به این سامانه ها صورت می پذیرد لذا تهیه، نصب و راه اندازی یک دستگاه WAF (Web Application Firewall) مورد تاکید می باشد.

در حال حاضر در معماری امنیتی شبکه آن سازمان فقط یک دستگاه UTM جهت انجام کلیه موارد مربوطه در نظر گرفته شده است که در آن IPS/IDS و آنتی ویروس بروزرسانی شده فعال می باشد ولیکن جهت تقسیم کارهای انجام شده توسط UTM و به منظور انجام دفاع در عمق با لایه های بیشتر علاوه بر تهیه یک دستگاه WAF مورد اشاره بکارگیری یک دستگاه فایروال نیز پیشنهاد می گردد.

همچنین با بررسی تنظیمات UTM فعلی مشخص گردید دسترسی رژیم اشغالگر قدس و کشور بحرین به سامانه های آن مجموعه مسدود نگردیده است که با توجه به شرایط موجود و وجود حملات سایبری متعدد از طریق کشورهای مزبور انسداد آن ضروری می باشد.

کلیه تجهیزات امنیتی و فعال شبکه (سوئیچ، روتر، فایروال و ...) و لاگ های مربوطه می بایست به صورت دوره ای در بازه های زمانی مشخص بصورت مستند توسط راهبر یا مسئول شبکه مورد بازرسی، بازبینی و بروزرسانی قرار گرفته و هرگونه رفتار مشکوک به دقت بررسی گردد که این فرآیند در حال حاضر به صورت مدون و دوره ای انجام نمی پذیرد.

نکته: همچنین لازم به ذکر است که انجام تنظیمات صحیح، بهینه و بروزرسانی مستمر با مجوزهای استفاده معتبر در کلیه دستگاه های امنیتی بسیار حائز اهمیت و ضروری می باشد.

در صورت صلاحدید سازمان و به منظور افزایش دسترس پذیری و تقسیم بار میتوان برای هر یک از تجهیزات فوق الذکر، تجهیزات پشتیبان آنلاین تهیه و راه اندازی نمود.

۲-۶- از آنجا که ایستگاه های کاری امکان اتصال همزمان به شبکه داخلی دانشگاه و اینترنت را دارند لذا اعمال سیاست های امنیتی لازم از طریق تجهیزات فوق الاشاره باید به صورت یکسان برای شبکه های داخلی و بیرونی به منظور پیشگیری از هرگونه حمله، نفوذ یا هک صورت پذیرد.

بازرسی دسترسی ها

۳-۶- وضعیت حملات بر روی تجهیزات مورد اشاره در بند ۱-۶ از طریق ابزارهای مربوطه مورد پایش قرار گرفته و اقدامات مرتبط در هر زمان بسته به وضعیت انجام پذیرد. آدرس هایی که دسترسی های بیش از حد نرمال درخواست می نمایند پس از بررسی بلاک شوند یا در زمان های بروز حملات گسترده ارتباطات و دسترسی از سایر کشور ها بغیر از ایران به سامانه های دانشگاه تا زمان رفع حملات مسدود گردد.

تنظیم دسترسی ها

۴-۶- پس از بروز حمله، دسترسی شرکت ها از بیرون سازمان از طریق VPN با رمزنگاری IPSEC و IP Address مشخص و ثابت صورت می پذیرد و پروتکل RDP غیرفعال گردیده ولیکن در بررسی تنظیمات UTM مشخص گردید همچنان شرکت نوپرداز از طریق پروتکل RDP به سامانه های تحت پوشش خود دسترسی دارد که این موضوع می بایست در اسرع وقت اصلاح گردد. همچنین می بایست دسترسی از راه دور شرکت ها با راه اندازی سامانه احراز هویت از طریق توکن فیزیکی یا مجازی با رعایت موارد امنیتی مربوطه صورت پذیرد.

تنظیم

۵-۶- به منظور افزایش امنیت، معماری سرورهای سازمان که اکنون به صورت یکپارچه است می بایست به صورت Zone بندی شده با سیاست قرارگرفتن سرورهای سامانه های با خصوصیت مشابه در یک Zone تغییر یابد. همچنین سرور ایمیل می بایست در یک Zone مجزا از سایر سرورها قرار گیرد.

خرید نرم افزار اوریجینال

۶-۶- سرویس دهنده ایمیل یکی از سرورهای مهم و با درجه آسیب پذیری بالا می باشد لذا علاوه بر رعایت کلیه نکات امنیتی به منظور پیشگیری از ورود ایمیل های مخرب به آدرس ایمیل کاربران از جمله حصول اطمینان از بروز رسانی آنتی ویروس و آنتی اسپم می بایست سازمان نسبت به تهیه نرم افزار کنترل ورودی های سرور مزبور بعد از تجهیزات امنیتی و قبل از ارسال ایمیل ها به آدرس کاربران اقدام نموده و سیاست امنیتی SPF (Sender Policy Framework) و Demarc توسط راهبر سیستم تنظیم و در بازه های زمانی مشخص بروزرسانی گردد.

طبق بررسی ها آنتی ویروس سرور ایمیل در تاریخ ۹۷/۴/۵ سیمانتک ورژن ۷,۵,۶,۱۵۲ بوده است که در تاریخ مزبور نسخه جدیدتر آنتی ویروس مذکور نیز ارائه شده بود ولیکن بروزرسانی مربوطه انجام نپذیرفته است و نسخه فعلی منصوب از نوع Trial می باشد که می بایست حتما نسخه اورجینال تهیه و نصب گردد. همچنین پیشنهاد می گردد از آنتی ویروس های شرکت های امریکایی در مجموعه استفاده نگردد.

لازم به ذکر است که آنتی ویروس سرور ایمیل در زمان بروز حمله ازنوع F- Secure بوده که پس از آن توسط بخش فناوری اطلاعات به سیمانتک تغییر یافته است.

۷-۶- با بررسی سوئیچ های شبکه قابل مدیریت مارک سیسکو سازمان مشخص گردید نسخه IOS سوئیچ های مذکور ۱۲,۲ می باشد که می بایست در اسرع وقت به آخرین نسخه موجود بروزرسانی گردد و به منظور مدیریت اتصال تجهیزات به شبکه سازمان می بایست Port Security پس از اطلاع رسانی به کاربران، جمع آوری نیاز ها و درخواست های واحد ها و پس از بررسی آنها بر روی کلیه پورت های سوئیچ ها فعال گردد که این موضوع فقط برروی Vlan بخش فناوری اطلاعات مشاهده گردید.

۸-۶- در حال حاضر بخش فناوری اطلاعات سازمان به دلیل عدم تمرکز در خصوص سامانه های منصوب، نحوه اعمال تغییرات، دسترسی ها، پورتها و IP آدرس های فعال مورد استفاده و بلا استفاده، کاربران در سطوح مختلف (سیستم عامل، پایگاه داده و برنامه کاربردی) و ... اطلاعات کاملی ندارد که این موضوع می تواند موجب آسیب پذیری و ضعف های امنیتی می گردد لذا ایجاد تمرکز، مدیریت و حاکمیت واحد و یکپارچه مورد تاکید می باشد.

۹-۶- بستن دستگاه های ورودی و خروجی و کلیه پورت های فیزیکی و منطقی بلااستفاده در ایستگاه های کاری انجام پذیرفته و فرآیند نحوه باز کردن پورت های مزبور تدوین و عملیاتی گردد.

۱۰-۶- سامانه های مدیریت محتوای (CMS) مورد استفاده در پرتال داخلی تهیه شده از شرکت یکتا وب می بایست به صورت دوره های و در بازه های زمانی مشخص بروزرسانی گردد.

۱۱-۶- نصب کارت SNMP بر روی دستگاه های UPS و انجام تنظیمات مربوطه به منظور پایش و کنترل لحظه ای وضعیت دستگاه های مزبور جهت حصول اطمینان از صحت وضعیت دستگاه های مذکور صورت پذیرد.

شرح وظیفه ای

۱۲-۶- برگزاری مانور در بازه های زمانی مشخص بر اساس استاندارد های مربوطه جهت حصول اطمینان از عملکرد صحیح کلیه سیستم های پشتیبان و پشتیبان های گرفته شده از سامانه ها صورت پذیرد که در حال حاضر این موضوع به صورت برنامه ریزی شده انجام نمی پذیرد. همچنین برگزاری مانور تجهیزات تامین کننده برق اضطراری از جمله تابلوها، UPSها و ژنراتور هر سه ماه یکبار می بایست صورت پذیرد.

بازرسی

۱۳-۶- در سازمان تاکنون تست نفوذ رسمی صورت نپذیرفته است لذا به منظور شناسایی آسیب پذیری های سامانه های موجود، سازمان می بایست در اسرع وقت نسبت به انجام تست نفوذ بر روی شبکه و کلیه سامانه ها توسط شرکت های واجد شرایط و مورد تائید مراکز ذیصلاح (مرکز مدیریت راهبردی افتا) در مرحله اول به صورت Black Box با استفاده از استانداردهای مربوطه و قرارداد NDA (Non-disclosure Agreement) اقدام نماید.

پس از شناسایی آسیب پذیری های موجود نسبت به اعلام آن به پیمانکاران و رفع مشکلات بر اساس درجه آسیب پذیری اقدام نموده و تست مجدد (Retest) به منظور حصول اطمینان از رفع کلیه ضعف های امنیتی صورت پذیرد. تست نفوذ می بایست به صورت فرآیندی سالیانه برای کلیه سامانه ها انجام پذیرد.

در قرارداد های کلیه پیمانکاران می بایست بندهایی به منظور همکاری پیمانکاران جهت رفع مشکلات شناسایی شده در تست نفوذ انجام شده توسط سازمان، زمانبندی رفع اشکالات اعلام شده با توجه به درجه اهمیت آنها و تعهد مبنی بر عدم مشاهده مشکلات اعلام و رفع شده قبلی در تست های نفوذ سال های آتی درج گردد.

در هنگام خرید یا توسعه سامانه ها از شرکت های پیمانکار نتایج تست نفوذ به عنوان یکی از مدارک مورد نیاز و ضروری اخذ گردد.

ارتباطی

۱۴-۶- قرارداد NDA و رعایت موارد امنیتی جهت پیشگیری از دسترسی های غیر مجاز کارشناسان شرکت با شرکت های تامین کننده با توجه به حساسیت و اهمیت سامانه ها منعقد گردد یا بندهای مربوطه در قرارداد های جاری لحاظ گردد.

مدیریتی / خرید تجهیزات

۱۵-۶- حضور کشیک شبانه روزی به منظور پایش و کنترل وضعیت سامانه های ۲۴ ساعته و در صورت عدم امکان در شرایط حاضر استفاده از سامانه های مانیتورینگ، پایش و اطلاع رسانی وضعیت سامانه ها، شرایط و فاکتور های فیزیکی محیط در کلیه ساعات اداری و غیر اداری و تعطیل از طریق پیامک مورد تاکید می باشد.

ارتباطی

۱۶-۶- تیم بخش فناوری اطلاعات سازمان مشترک هیچ یک از مراکز اطلاع رسانی امنیتی کشور (مرکز ماهر یا ...) نبوده لذا اطلاع از موارد امنیتی، باج افزار ها، ویروس ها و حملات جدید و اعمال سیاست های مربوطه هر یک در تجهیزات، سیستم ها و سامانه های سازمان با سرعت مناسب صورت نمی پذیرد که این موضوع خود ریسک امنیتی سازمان را بالا می برد لذا توصیه می گردد این موضوع به صورت رسمی با شرح مسئولیت های مربوطه جهت دریافت اطلاعات و انجام اقدامات در هر یک از موارد که در خصوص تجهیزات یا سامانه های دانشگاه صدق می نماید انجام پذیرد.

مدیریتی / ساختاری

۱۷-۶- ایجاد کمیته بحران، تعیین شرح وظایف، مسئولیت ها، سمت ها، نحوه تشکیل و تصمیم گیری در زمان های بروز حوادث امنیتی به منظور انجام تصمیم گیری های لازم جهت کنترل و مدیریت بحران ضروری می باشد.

مدیریتی / سیاستگذاری

۱۸-۶- تدوین، تصویب و ابلاغ مجموعه خط مشی های امنیت فناوری اطلاعات سازمان از جمله موارد ذیل تاکنون انجام نشده و توصیه می گردد در اسرع صورت پذیرد.

- خط مشی گذرواژه
- خط مشی کاربر مجاز سامانه های فناوری اطلاعات
- خط مشی امنیت برون سپاری سامانه ها
- خط مشی مدیریت مجوز دسترسی
- خط مشی تداوم کسب و کار فناوری اطلاعات
- خط مشی توسعه امن سامانه ها
- خط مشی امنیتی دسترسی از راه دور
- خط مشی ارزیابی امنیتی و تست نفوذ سامانه ها
- خط مشی امنیتی وب سایت
- خط مشی امنیتی دسترسی به ایمیل
- خط مشی امنیتی امحاء اطلاعات
- خط مشی امنیتی تجهیزات همراه

- خط مشی سرویس اینترنت برای پرسنل سازمان
- خط مشی امنیت ارتباطات بی سیم
- خط مشی مدیریت نسخه های پشتیبان

۱۹-۶- با توجه به بررسی های صورت گرفته فرآیند مدون و مستندی در هیچ موضوعی جهت انجام امور امنیتی، بروز رسانی ها، ایجاد و کنترل دسترسی ها، باز و بستن پورت ها، پشتیبان گیری، برگزاری مانور ها و ... در سازمان مشاهده نگردید و برخی از این موارد با تصمیم پرسنل در مقاطعی انجام می پذیرد لذا پس از تدوین خط مشی ها به منظور ارتقاء و بهبود امنیت، پیشگیری و به حداقل رساندن حوزه تخریب حملات، ایجاد فرآیند ها، روال ها، فرم های مربوطه و کنترل های آن بر اساس استاندارد های مربوطه توسط شخص مسئول مورد تاکید می باشد.

۲۰-۶- به منظور افزایش دسترس پذیری سامانه های تحت اینترنت پیشنهاد می گردد اینترنت سازمان از دو شرکت تامین کننده اینترنت با پهنای باند یکسان تامین گردد تا در صورت اختلال در زیرساخت داخلی یکی از شرکت ها کلیه سامانه های مجموعه از دسترس به صورت کامل خارج نشود و با مدیریت بخش فناوری اطلاعات و هماهنگی با سایر بخش های سازمان در چنین زمان هایی سامانه های با اولویت کمتر از ارائه سرویس خارج گردند تا سایر سامانه های حیاتی با سرعت مناسب سرویس لازم را ارائه نمایند.

۷- الزامات و توصیه های عمومی :

کنترل و رعایت موارد ذیل در سطوح اعلام شده در کلیه سامانه ها و زیرساخت های مربوطه فعلی و آتی ضروری است. لذا به منظور انجام این مهم ایجاد فرآیند لازم و متولی جهت کنترل موارد مزبور در مقاطع زمانی مشخص حداکثر شش ماهه به صورت مستند توسط سازمان ضروری می باشد.

۱-۷- سیستم عامل:

- تمامی سرویس های بلا استفاده در سیستم عامل های سرورها غیر فعال شود .
- مجوزهای کاربری در سیستم عامل به صورت مشخص و معینی تعریف شود .
- حسابهای کاربری مشخص و تعریف شده ای در هر سیستم عامل وجود دارد و تمامی حساب های پیش فرض در صورت امکان حذف یا غیر فعال شود .
- طول کلمات عبور حداقل ۱۰ کاراکتر بوده و ترکیبی از حروف بزرگ و کوچک، اعداد و کاراکترهای خاص باشد.
- تمامی آسیب پذیری های سیستم عامل توسط ابزارهای مناسب پویش آسیب پذیری کشف و رفع شود .
- تمامی وصله های امنیتی سیستم عامل اعمال شود .
- فایروال میزبان در سیستم عامل فعال شده و به گونه ای پیکر بندی شود که فقط ترافیک مجاز امکان عبور داشته باشد
- مکانیزم مناسب پشتیبان گیری و روال بازیابی مناسب برای آن باید تهیه و اجرایی گردد.
- ابزار مناسب ضد ویروس در سیستم عامل نصب شده ، فعال گردیده و به صورت دائمی به روزرسانی شود.
- تمام داده های لاگ در سیستم عامل شامل داده های لاگ خودش و دیگر برنامه ها مانند پایگاه داده ، وب سرور و .... را به سامانه های نگهداری و تحلیل داده های لاگ ارسال شده و حداقل به مدت ۶ ماه نگهداری شود .
- فرآیندهای سرویس دهنده وب و سرویس دهنده برنامه های کاربردی ، تحت مجوز کاربردی با سطح دسترسی محدود و کمتری اجرا شوند .
- سیستم عامل به گونه ای پیکر بندی شود که با یک سرور زمانی مرکزی همگام سازی شود .

۲-۷- پایگاه داده:

- جدا سازی برنامه کاربردی وب و پایگاه داده در دو سرور مجزا.
- کلیه مکانیزم های غیر ضروری در سیستم مدیریت پایگاه داده غیر فعال شود مانند: پروتکل های ارتباطی ، رویه های ذخیره شده ، کلاس ها و ....
- حساب های کاربری مشخص و تعریف شده ای در پایگاه داده وجود داشته باشد و تمامی حساب های پیش فرض حذف یا غیر فعال شود .
- کلمات عبور حداقل ۱۰ کاراکتر بوده و ترکیبی از حروف بزرگ و کوچک، اعداد و کاراکترهای خاص باشد.
- سیستم مدیریت پایگاه داده به آخرین نسخه به روز رسانی شود و همچنین آخرین وصله های امنیتی اعمال شود .
- دسترسی به پایگاه داده فقط از طریق برنامه کاربردی و مدیر سیستم پایگاه داده وجود داشته و هیچ نوع دسترسی مستقیم دیگری به پایگاه داده وجود نداشته باشد .
- حساب کاربری که توسط برنامه های کاربردی به منظور ارتباط با پایگاه داده مورد استفاده قرار میگیرد صرفاً محدود به مجوزهای لازم بوده و دسترسی آن فقط مربوط به پایگاه داده و جداول همان برنامه باشد .
- لاگ تمامی پرس و جوها و اطلاعات تراکنش ها در بخش خارج از پایگاه داده ذخیره شود.

۳-۷- سرویس زیر ساختی برنامه کاربردی:

- کلمات عبور حداقل ۱۰ کاراکتر بوده و ترکیبی از حروف بزرگ و کوچک، اعداد و کاراکترهای خاص باشد (در صورتی که سرویس زیر ساختی دارای مکانیزم احراز هویت مستقل مربوط به خودش است) .
- کلیه حسابهای کاربری پیش فرض حذف یا غیر فعال گردد (در صورتی که سرویس زیر ساختی دارای مکانیزم احراز هویت مستقل مربوط به خودش است).
- کلیه محتوای وب در یک مسیر جداگانه و مستقلی قرار گرفته و در پارتیشن متفاوتی از سیستم عامل قرار گیرد .
- سرویس زیر ساختی به گونه ای پیکر بندی شود که در صورت بروز خطا صفحه ی خاصی را نمایش دهد و اطلاعات خطا قابل مشاهده نباشد .
- سرویس زیر ساختی به گونه ای پیکر بندی شود که داده های لاگ را در محل مناسبی ذخیره کند .
- سرویس زیر ساختی به آخرین نسخه به روز رسانی شده و کلیه ی وصله های امنیتی آن نصب شود .

٤-۷- برنامه کاربردی:

- تمامی فایل های غیر ضروری از محتوای برنامه های کاربردی وب حذف شود .
- چنانچه در تولید برنامه کاربردی از چارچوب ها یا سیستم های مدیریت محتوای (CMS) آماده استفاده شده است ، این چارچوب ها و یا سیستم های مدیریت محتوا به آخرین نسخه به روز رسانی شود .
- تمامی کامپوننت ها و کتابخانه های مورد استفاده در برنامه به آخرین نسخه به روز رسانی شود .
- فرم های ورود کاربر از مکانیزم های جلوگیری از حملات Brute force مانند CAPTCHA پشتیبانی کند.
- کلمات عبور مدیریتی به منظور تغییر محتوا حداقل ۱۰ کاراکتر بوده و از ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکتر های خاص تشکیل شود .
- کلیه اطلاعات محرمانه مانند کلمات عبور به صورت امن (با استفاده از الگوریتم های رمز نگاری) ذخیره سازی شود
- صفحات حساس مدیریتی صرفاً از آدرس های خاص قابل مشاهده و دسترسی باشد .

۸- خلاصه و نتیجه گیری

پس از نفوذ صورت گرفته، با دستور و هماهنگی مدیریت عالی دانشگاه وضعیت امنیت سامانه های دانشگاه از طریق مراجعه حضوری طی خرداد و تیر ماه سالجاری، مصاحبه با کارشناسان بخش فناوری اطلاعات، بررسی میدانی مرکز داده و استفاده از ابزارها مورد ارزیابی قرار گرفت که نتایج حاصله حاکی از بروز آسیب به دلیل عدم رعایت حداقل موارد امنیتی می باشد.

لذا در این گزارش رهنمود های ضروری فوری از قبیل نصب WAF ، فایروال، مدیریت پروتکل ها و پورت ها، ایجاد استراتژی، فرآیندها، کنترل ها و ... و نکات عمومی که حسب صلاحدید مدیریت ارشد دانشگاه جهت انجام در مراحل بعدی می تواند در دستور کار قرار داده شود ارائه گردیده است.

ابزار ارزیابی : sslcheck.certcc.ir

نتایج ارزیابی SSL/TLS

نام دامنه مورد ارزیابی	isu.ac.ir(77.104.103.15:443)

اطلاعات تحلیل

زمان ارزیابی	۱۳۹۷ / ۴ / ۱۲ - ۲۲:۰۴:۲۱
آدرس IP، شماره پورت و نام میزبان	isu.ac.ir(77.104.103.15:443)

اطلاعات گواهی دیجیتال

نام دامنه‌های پشتیبانی شده	*.isu.ac.ir
سایر دامنه‌های پشتیبانی شده	*.isu.ac.ir isu.ac.ir
زمان شروع اعتبار	2017-01-15 06:15:39
زمان اتمام اعتبار	2020-01-15 06:15:39
تاریخ گواهی اعتبار دارد؟	بله
نوع رمزنگاری نامتقارن و اندازه کلید	rsaEncryption (2048 bit)
مرکز صدور گواهی	Certum Domain Validation CA SHA2 (Unizeto Technologies S.A. from PL)
الگوریتم امضاء رقمی	sha256WithRSAEncryption
نوع گواهی	wildcard

توضیحات:
از نظر تعداد دامنه های تحت پوشش ، 3 نوع گواهی وجود دارد:
Single Domain: تنها یک دامنه یا زیردامنه را در بر می‌گیرد.
Wildcard: یک دامنه و تعداد نامحدودی از زیردامنه‌های آن را پوشش می‌دهد.
Multi-Domain: چندین دامنه را پوشش می‌دهد.
در صورتی که می‌خواهید تنها یک زیردامنه خاص را مجهز به سرویس SSL نمایید، از گواهی‌های Single Domain استفاده نمایید که هزینه کمتری دارد.
در صورتی که سازمان شما چندین زیردامنه دارد که می‌خواهید سرویس SSL را برای همه آنها فعال کنید، می‌توانید از یک گواهی Wildcard استفاده کنید. در این حالت کلیدهای رمزنگاری یکسانی در تمامی سرویس‌دهنده‌های شما مورد استفاده قرار خواهد گرفت.
برای شرایطی که امنیت بالاتری مد نظر است و قصد به اشتراک گذاری کلید خصوصی بین سرویس‌دهنده‌های مختلف را ندارید، می‌توانید در کنار گواهینامه Wildcard، برای برخی از زیردامنه‌ها گواهی مجزا از نوع Single تهیه نمایید.

نوع اعتبارسنجی گواهی

توضیحات:
سطح اعتبار گواهی‌ها دارای دسته های زیر است:
DV (Domain Validated): این سطح حداقل هزینه را دارد و اعتبارسنجی‌های پایه را پوشش می‌دهد. در این حالت صدورگواهی بر این مبنا صورت می‌گیرد که مرکزصدور گواهی اطمینان حاصل می‌کند که کلیدعمومی موجود در گواهی، توسط مالک دامنه ساخته شده است (ولذا کلید خصوصی آن تنها در اختیار مالک دامنه است و نه فرد دیگری). گرفتن این گواهی ممکن است چند دقیقه تا چند ساعت طول بکشد.
OV (Organization Validation): علاوه بر اعتبارسنجی مربوط به مالکیت دامنه، جزئیات خاصی از مالک (مثل نام و آدرس) هم تصدیق اصالت می‌شود. گرفتن این گواهی ممکن است چند ساعت الی چند روز طور بکشد.
EV (Extended Validation): این مورد بالاترین درجه از امنیت را فراهم می‌آورد زیرا قبل از صدور این گواهی، بررسی‌های کاملی روی آن انجام شده است و مورد تایید است. گرفتن این گواهی معمولا بین چند روز الی چند هفته طول می‌کشد.

آیا گواهی برای دامنه بدون پیشوند https://isu.ac.ir (https://isu.ac.ir) معتبر است؟ بله

توضیحات:
در مرحله صدور گواهی، در هنگام تهیه CSR یا Certificate Signing Request، برای دامنه‌های wildcard مانند domain.ir.* دقت کنید که بهتر است حتماً فیلد SAN یا SubjectAlternateName را هم پرکرده و دامنه بدون پیشوند خود (یعنی domain.ir) را در آن قرار دهید. این کار سبب می‌شود که گواهی صادرشده برای نام دامنه بدون پیشوند هم معتبر باشد (برای خود domain.ir). در این حالت پس از نصب و فعال‌سازی SSL، با واردکردن آدرس https://domain.ir در مرورگر فایرفاکس یا IE خطای گواهی نخواهید داشت.

آیا گواهی برای میزبان مورد نظر (isu.ac.ir) معتبر است؟ **بله**

توضیحات:
اعتبار یک گواهی برای یک میزبان سه شرط دارد:
1. انطباق نام میزبان با دامنه های مشخص شده در گواهی (در فیلدهای Common Name یا Subject Alternative Name).
2. گواهی از نظر زمان منقضی نشده باشد.
3. امضا کننده گواهی جزء مراکز صدور گواهی معتبر باشد یا با سلسله مراتبی به یکی از این مراکز برسد.

زنجیره گواهی‌ها

1 - گواهی میزبان	IR (*.isu.ac.ir)
صادر کننده	Certum Certification Authority (Certum Domain Validation CA SHA2)
2 - گواهی ریشه	Certum Certification Authority (Certum Domain Validation CA SHA2)
صادر کننده	Certum Certification Authority (Certum Trusted Network CA)

صادر کننده ریشه در مجموعه گواهی‌های قابل اعتماد است

پشتیبانی از خانواده پروتکل‌های TLS/SSL

TLS 1.2 — پشتیبانی می‌شود (مناسب) ✔

توضیحات:
TLS1.2 جدیدترین و امن ترین نسخه از پروتکل TLS است. این پروتکل حتما می بایست در سرویس دهنده فعال باشد.

TLS 1.1 — پشتیبانی می‌شود (مناسب) ✔

توضیحات:
به دلیل سازگاری با مرورگرها و سیستم عامل های قدیمی تر توصیه می شود TSL 1.1 بر روی سرویس دهنده ها فعال باشد.

TLS 1.0 — پشتیبانی می‌شود (مناسب) ✔

توضیحات:
به دلیل سازگاری با مرورگرها و سیستم عامل های قدیمی تر توصیه می شود TSL 1.0 بر روی سرویس دهنده ها فعال باشد.

SSL v3.0 — پشتیبانی نمی‌شود (مناسب) ✔

توضیحات:
پروتکل SSLv3 دارای آسیب پذیری های امنیتی متعدد است و می بایست غیرفعال گردد.

SSL v2.0 — پشتیبانی نمی‌شود (مناسب) ✔

توضیحات:
پروتکل SSLv2 دارای آسیب پذیری های امنیتی متعدد است و می بایست غیرفعال گردد.

نتایج تحلیل آسیب‌پذیری

OpenSSL Padding Oracle (CVE-2016-2107) آسیب‌پذیر نیست.

توضیحات:
حمله کننده Man-in-the-middle با استفاده از این آسیب پذیری می تواند ترافیک را رمزگشایی کند، هنگامی که ارتباط از AES CBC استفاده می کند و سرور AES-NI را پشتیبانی میکند.

ROBOT (CVE-2017-13099) آسیب‌پذیر نیست.

توضیحات:
حمله ROBOT به مهاجم اجازه می‌دهد یک عملیات رمزگشایی و رمزنگاری RSA را با استفاده از کلید خصوصی پیکربندی‌شده بر روی سرورهای TLS آسیب‌پذیر انجام دهد

Drown (CVE-2016-0800) آسیب‌پذیر نیست.

توضیحات:
DROWN یک حمله‌ی بین پروتکلی است که از ضعف پیاده‌سازی SSLv2 استفاده می‌کند و می‌تواند نشست‌های TLS به‌دست‌آمده از کاربران را به‌صورت غیرفعال ترجمه کند.

POODLE (CVE-2014-3566) آسیب‌پذیر نیست.

توضیحات:
نوعی حمله Man-in-the-Middle است که با بهره‌برداری از آن حمله کننده می‌تواند با تعداد محدودی درخواست SSL/TLS قسمتی از یک پیام رمز شده را ترجمه کند.

RC4 (CVE-2013-2566, CVE-2015-2808) آسیب‌پذیر نیست.

توضیحات:
الگوریتم RC4 دارای نقاط ضعف قابل بهره برداری است. بنابراین بهتر است که از RC4 استفاده نشود.

Heartbleed (CVE-2014-0160) آسیب‌پذیر نیست.

توضیحات:
یک آسیب‌پذیری جدی در کتابخانه رمزنگاری OpenSSL است. این ضعف امکان سرقت داده‌های محافظت شده توسط SSL/TLS را ممکن می‌سازد. حمله کننده می‌تواند از طریق اینترنت حافظه سیستم‌های حفاظت شده توسط نسخه‌های آسیب‌پذیر نرم افزار OpenSSL را بخواند.

CCS (CVE-2014-0224) آسیب‌پذیر نیست.

توضیحات:
CCS امکان حمله man-in-the-middle به ارتباطات رمز شده را می دهد.

CRIME, TLS (CVE-2012-4929) آسیب‌پذیر نیست.

توضیحات:
CRIME یک بهره برداری امنیتی از کوکی های رمز ارتباط هایی است که از پروتکل های HTTPS و SPDY و همچنین از فشرده سازی داده استفاده می کنند. هنگام بازیابی محتوای کوکی های رمز شده تصدیق اصالت، به حمله کننده اجازه می دهد که session hijacking را بر روی یک نشست تصدیق شده وب، انجام دهد.

FREAK (CVE-2015-0204) آسیب‌پذیر نیست.

توضیحات:
FREAK یک بهره برداری امنیتی از ضعف رمزنگاری در پروتکل های SSL/TLS است.

Secure Renegotiation (CVE-2009-3555) آسیب‌پذیر نیست.

توضیحات:
این نقص به یک man-in-the-middle اجازه می دهد که در یک ارتباط بین کلاینت و سرور داده تزریق کند و دستوراتی با گواهی های یک کاربر غیرمجاز را اجرا کند. همچنین او می تواند گواهی های تصدیق اصالت یک کاربر مجاز را جمع آوری کند.

اطلاعات ابطال کلید

آدرس الکترونیکی لیست ابطال کلید http://crl.certum.pl/dvcasha2.crl

توضیحات:
Certificate Revocation List (CRL)

آدرس الکترونیکی OCSP http://dvcasha2.ocsp-certum.com

توضیحات:
Online Certificate Status Protocol (OCSP)

پشتیبانی از OCSP stapling خیر

توضیحات:
روشی برای بالا بردن سرعت در چک کردن لیست ابطال کلید برای گواهی است. با استفاده از OCSP Stapling نیاز نیست که سرویس گیرنده درخواستی را به سرور OCSP بدهد و با استفاده از اطلاعات مهیا شده همراه گواهی، می‌تواند از باطل نبودن گواهی اطمینان حاصل کند.

پروتکل تبادل کلید

پشتیبانی از Forward Secrecy فقط مرورگرهای جدید

توضیحات:
یک ویژگی در پروتکل‌های ارتباطی امن است. این خاصیت تضمین می‌کند که در صورت لو رفتن کلیدهای طولانی مدت، مهاجم نمی‌تواند به کلیدهای نشست گذشته دسترسی یابد.

بکار بردن دیفی-هلمن ناشناس — خیر (مناسب) ✓

توضیحات:
دیفی-هلمن ناشناس از پروتکل دیفی-هلمن بدون تصدیق اصالت استفاده می‌کند. از آنجایی که کلیدهای استفاده شده تصدیق اصالت نمی‌شوند، این نوع پیاده‌سازی از پروتکل مستعد حمله Man-in-the-Middle است.

استفاده از زوج کلیدهای دیفی-هلمن شناخته شده — خیر (مناسب) ✓

توضیحات:
در صورتی که زوج کلیدهای استفاده شده در پروتکل دیفی-هلمن شناخته شده باشد، مهاجم می‌تواند با استفاده از آنها کلیدهای جلسه توافق شده را بدست آورد.

ارزیابی استانداردهای رمزنگاری

Null Ciphers — خیر (مناسب) ✓

توضیحات:
در رمزهای Null هیچ نوع رمزنگاری انجام نمی‌شود. بنابراین به سادگی متن ورودی به خروجی منتقل می‌شود و در واقع هیچ تغییری بر روی آن اعمال نمی‌شود.

Anonymous Null Ciphers — خیر (مناسب) ✓

توضیحات:
رمزهای Null هستند که در پروتکل تبادل کلید تصدیق اصالت انجام نمی‌شود.

رمزهای ضعیف با طول کمتر از 64 بیت — خیر (مناسب) ✓

DES Ciphers — خیر (مناسب) ✓

توضیحات:
الگوریتم رمزنگاری متقارن

(Triple DES Ciphers (>=64 bit — خیر

توضیحات:
الگوریتم رمزنگاری متقارن است که، بلوک های داده را سه بار با الگوریتم DES رمز می کند.

دنباله رمزهای پشتیبانی شده

- دنباله رمز به ترتیب، الگوریتم رمزنگاری نامتقارن، متقارن و الگوریتم درهم ساز را نشان میدهد.
- دنباله رمزهای ضعیف با رنگ قرمز مشخص شده اند.
- الگوریتمی که دلیل ضعیف بودن دنباله رمز است، برجسته شده است.

پروتکل	پشتیبانی از FS	دنباله رمز
TLSv1	ECDH, P-256, 256 bits FS	خیلی قوی - TLS_ECDHE_RSA_WITH_ AES_256_CBC_SHA
TLSv1	ECDH, P-256, 256 bits FS	خیلی قوی - TLS_ECDHE_RSA_WITH_ AES_128_CBC_SHA
TLSv1.1	ECDH, P-256, 256 bits FS	خیلی قوی - TLS_ECDHE_RSA_WITH_ AES_256_CBC_SHA
TLSv1.1	ECDH, P-256, 256 bits FS	خیلی قوی - TLS_ECDHE_RSA_WITH_ AES_128_CBC_SHA
TLSv1.2	ECDH, P-256, 256 bits FS	خیلی قوی - TLS_ECDHE_RSA_WITH_ AES_256_CBC_SHA384
TLSv1.2	ECDH, P-256, 256 bits FS	خیلی قوی - TLS_ECDHE_RSA_WITH_ AES_256_CBC_SHA
TLSv1.2	ECDH, P-256, 256 bits FS	خیلی قوی - TLS_ECDHE_RSA_WITH_ AES_128_CBC_SHA256
TLSv1.2	ECDH, P-256, 256 bits FS	خیلی قوی - TLS_ECDHE_RSA_WITH_ AES_128_CBC_SHA

مکانیزم‌های امنیتی دیگر

پشتیبانی از Strict Transport Security

خیر (نامناسب)

توضیحات:
یک بهبود امنیتی برای برنامه‌های تحت وب است که از پروتکل HTTPS استفاده می‌کنند. این بهبود امنیتی سبب میشود مرورگر به صورت خودکار تمامی ارتباطات را به صورت https یا امن برقرار نماید و از برقراری ارتباط به صورت http (حتی در صورت درخواست کاربر) جلوگیری شود.

پشتیبانی از Heartbeat Extension

خیر

توضیحات:
افزونه ضربان قلب یک پروتکل جدید برای TLS/DTLS است که قابلیت زنده نگه داشتن ارتباط بدون انجام تعاملات اولیه را مهیا می‌کند.

جمع بندی مشکلات

پشتیبانی از پروتکل های امن

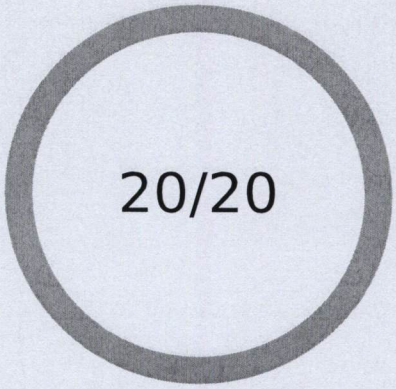
- پشتیبانی از Forward Secrecy فقط در مرورگر های جدید انجام می شود.

مستندات امن سازی
(HelpDoc-pe.php)

نمره وب سایت

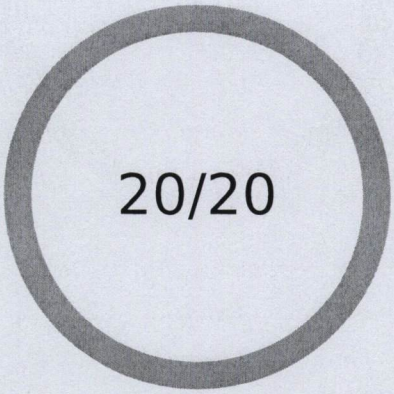
نمره وب سایت: 20 از 20

20



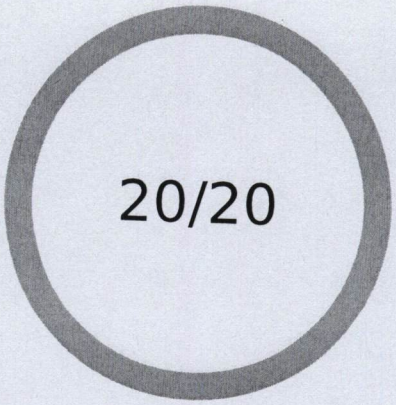
قدرت الگوریتم های رمزنگاری

20



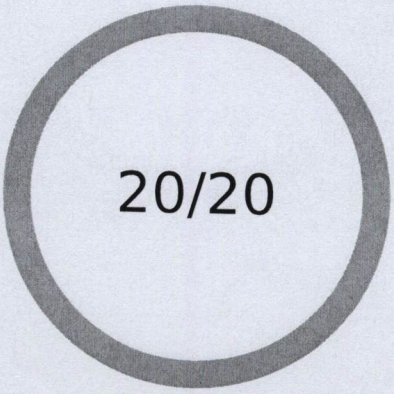
پشتیبانی از پروتکل های امن

20



مقاومت در برابر حملات شناخته شده

20



گواهی دیجیتال

جهت امن سازی به مستندات امن سازی (HelpDoc-pe.php) مراجعه نمایید.