

پس از کشف یک رخنه چه باید کرد؟
نخستین اقدامات ضروری پس از کشف نفوذ چیست؟ جلوگیری از ادامه نفوذ، کاهش زیان و اقدامات امنیتی لازم

برخورد نزدیک از نوع امن!
استاد امنیت اطلاعات آموزشگاه سایبرتک از جدیدترین فناوری های امنیتی و دغدغه های مرتبط می گوید

چگونه باید یک متخصص امنیت اطلاعات شد؟
معرفی کامل دوره های امنیت اطلاعات

+ پوستر نقشه راه دوره های سیسکو

سایبرنامه

www.CyberTech.ir
No.4, September 2015

CyberTech
The Leader in IT & Training
پیشرو در ارائه آموزش های تخصصی IT

ماهنامه خبری آموزشگاه مهندسی سایبرتک
دوره جدید، شماره چهارم، شهریورماه ۱۳۹۴

دوره های حرفه ای امنیت اطلاعات در سایبرتک

چهره ای در تاریکی!

چگونه سازمان خود را از گزند هکرها
در امان نگه داریم؟

وبسایت جدید سایبر تک افشاح شد!

نظرات و پیشنهادات خود را برای ما بفرستید

www.cybertech.ir

- جدیدترین اخبار و گزارش‌های دنیای فناوری و آموزش
- آشنایی با کلاس‌ها و اساتید سایبر تک
- تقویم آموزش و ثبت‌نام آنلاین
- اطلاع از آخرین تخفیف‌ها، مسابقات و جوایز
- ثبت‌نام در سمینارها و نشست‌های تخصصی
- ...و...



سخن مدیرعامل



دکتر هوشنگ کاظمی

در حال حاضر امنیت اطلاعات موضوعی بسیار مهم برای مطالعه و تحقیق است. این دانش به صورت یک نیاز اصلی هم‌سوی دیگر مباحث فناوری اطلاعات و چه بسا گاهی در مرکزیت این مباحث می‌درخشد. در سال‌های اخیر امنیت اطلاعات مورد توجه جوامع علمی و در راس آن جامعه دانشگاهی قرار گرفته. در این راستا، طراحی و درخشش بحث معماری امنیت توانسته مفاهیم بسیط و مختلف حوزه‌ی فناوری اطلاعات را زینت بخشد و جایگاه و خاستگاه آن‌ها را معین کند. امروز مشاهده می‌کنیم؛ رشد روزافزون این مبحث به علاوه پراکندگی‌اش، آن‌چنان پیش‌رفته که متأسفانه جز در مواردی خاص و خیلی محدود، این دانش به‌طور بنیادین در کشورمان وجود ندارد. به همین دلیل پیچیدگی علم امنیت اطلاعات، آموزش آن را بسیار حساس و پیچیده کرده است. این جاست که باید در کشورمان به آموزش و پژوهش آکادمیک این رشته توجه‌ای ویژه کنیم و بستر خودکفایی این فناوری را در دستور کار خود قرار دهیم. حالا دیگر می‌دانیم که این دانش بسیار حساس و باارزش است و با وجود تهدیدهای مختلف در زمینه‌ی امنیت اطلاعات، راه برای پژوهش و صنعت برای آن بسیار هموار است. اکنون آموزشی‌ترین نگاه می‌کنیم و توجه‌مان را به مدرک CISSP قرار دهیم، که هدف آن ایجاد یک سطح مهارت حرفه‌ای و عملی در زمینه امنیت اطلاعات برای افراد علاقمند است. مدرک CISSP بر خلاف سایر مدارک امنیتی، وابسته به محصولات هیچ شرکتی نبوده و به متخصصان امنیت اطلاعات، مهارت لازم را در طرح و پیاده‌سازی سیاست‌های کلان امنیتی اعطا می‌کند. سایبرتک در جایگاه ارایه دهنده آموزش تخصصی دوره‌های آی‌تی، در مبحث امنیت این دوره را مدت‌هاست در دستور کار خود قرار داده است... و حالا این‌گونه اندیشه کنیم تا امنیت اطلاعات خود را رویین‌تر کنیم و عرصه را بر نفوذگران تنگ‌تر!

خبر و گزارش

۱۴

گفت‌وگو: گفت‌وگوی اختصاصی سایبرنامه با روزبه نوروزی

۱۱

پوستر نقشه دوره‌های سیسکو

۱۰

اقدامات ضروری پس از کشف نفوذ

۱۲

معرفی دوره‌های امنیت

۱۶

تقویم آموزشی ماه

۱۸

سخن ماه

«چنان زندگی کن که انگار فردا می‌میری. چنان یاد بگیر که انگار تا ابد زنده‌ای.»

ماهاتما گاندی

“Live as if you were to die tomorrow. Learn as if you were to live forever.”

Mahatma Gandhi

Cybernameh

Cybertech's Monthly Bulletin

No.4, September 2015

License Holder:

Cybertech Institute

Managing Director:

Hassan Etemadi

Editor in Chief:

Ahmadreza Farzan Jam

Social Networks Manager:

Hossein Eftekhari Yekta

Content, Graphic Design, and Layout:

Digital Marketing Group

Address: No 33, Mir Emad Street, Motahari Avenue, Tehran

Tel: +9821 86 76 5000 Fax: +9821 86 76 5900

ماهنامه خبری داخلی آموزشگاه مهندسی سایبرتک

دوره جدید، شماره چهارم، شهریورماه هزار و سی صد و نود و چهار

صاحب امتیاز: آموزشگاه مهندسی فراتر از رایانه (سایبرتک)

مدیرمسئول: مهندس حسن اعتمادی

سرمدیر: احمدرضا فرزانه جم

مدیر شبکه‌های اجتماعی: حسین افتخاری یکتا

تأمین محتوا، طراحی و صفحه‌آرایی: گروه دیجیتال مارکتینگ سایبرتک

همکاران این شماره: روزبه نوروزی، کاوه اصلاحی و محمدرضا کاظمی

نشانی: تهران، خیابان مطهری، خیابان میرعماد

روبه‌روی سفارت هند، ساختمان شماره ۳۳

شماره تماس: ۸۶۷۶۵۰۰۰ فکس: ۸۶۷۶۵۹۰۰

سیستم CRM را برشمرد. وی با تاکید بر تجربه و دانش خوبی که در مجموعه سایبر تک برای انجام پروژه‌های مجازی سازی (Citrix و VMware) وجود دارد، آمادگی واحد خود را جهت ارائه هرگونه مشاوره و انجام پروژه اعلام کرد. سایبر تک تاکنون برای بیش از ۸۰ مشتری بزرگ و کوچک پروژه طراحی و پیاده سازی با استفاده از محصولات سیتریکس را انجام داده است. که از آن جمله می توان به شرکت ایران خودرو، ایران خودرو دیزل، سایپو، شرکت البرز، انرژی پاسارگاد، شرکت دنون سحر، بازرگانی موسی خانی، قوای محرکه، شرکت دلونگی، شرکت تدبیر، سیمان هرمزگان و ... اشاره کرد.

شماره تماس دپارتمان سیتریکس سایبر تک: ۸۶۷۶۵۱۲۱ و ۸۶۷۶۵۰۰۰

در راستای به کارگیری راه حل های مبتنی بر سیستم های جدید و پیشرفته، سایبر تک با نصب و راه اندازی نرم افزار XenApp 7.6 از سری محصولات مجازی سازی شرکت سیتریکس در مجموعه خود امکان ارائه و دردسترس قراردادن کلیه نرم افزارهای مورد نیاز پرسنل و کارشناسان خود را فراهم کرده است.

مهندس محمدرضا کاظمی مدیر بخش پروژه ها و کارشناس سیتریکس سایبر تک در این خصوص مزایای استفاده از این سیستم امکان مدیریت متمرکز، ایجاد بستر امن و سریع جهت دسترسی راحت به تمامی نرم افزارهای شرکت از جمله



سمینار CISCO VPN TECHNOLOGIES در سایبر تک

سمینار آشنایی با CISCO VPN TECHNOLOGIES با سخنرانی مهندس کاوه اصلاحی در آموزشگاه مهندسی سایبر تک برگزار شد. اهداف مهم این سمینار بر پایه معرفی کلی از سیستم های انتقال WAN در لایه های Service provider و معایب استفاده از این زیر ساخت ها بدون مکانیزم های VPN، ارائه راه کارها Cisco برای پیاده سازی مکانیزم های VPN، معرفی مکانیزم های ارتباطی در سطوح Enterprise مشتمل بر مکانیزم های Point-to-Point، Point-to-multipoint و Spoke-to-Spoke، معرفی مکانیزم های امنیتی روی ساختارهای VPN، ساختارهای ایزوله مبتنی بر VRF بود. در این سمینار حدود ۴۵ نفر از علاقمندان این موضوع جذاب شرکت داشتند. در پایان سمینار از علاقمندان پذیرایی به عمل آمد و شماره های گذشته سایبر نامه و پکیج های آموزشی در اختیارشان قرار داده شد.



خبرهای سایبر تک



برگزاری دوره ها و کمپ های مختلف سازمانی سایبر تک

برگزاری کمپ SQL Server در شرکت خطوط لوله مخابرات نفت
برگزاری دوره ITIL در شرکت ملی مهندسی ساختمان نفت
برگزاری دوره کامل ICDL در پارک علم و فناوری پردیس
برگزاری دوره CCNA برای شرکت ناک در شهرستان کرج
برگزاری دوره CCNA Security در سازمان فناوری اطلاعات

با توجه به روند رو به رشد آموزشگاه مهندسی سایبر تک در ارائه آموزش های تخصصی و اعتماد متقابل سازمان ها در اجرای برگزاری دوره ها و کمپ ها توسط سایبر تک که توانسته نیازهای آنان را برآورده کند، در ماه جاری دوره هایی در سازمان های مختلف برگزار شد که تعدادی به این شرح است:



آمریکایی هیچ نمایندگی در ایران نداشته‌اند، بنابراین مشخص است که با رفع برخی تحریم‌ها، همکاری با این موسسات به شرایط دیگری از جمله رفع تحریم‌های آمریکا مرتبط می‌شود. فریب‌ها مه‌دیون با بیان این‌که سازمان نظام‌صن‌فی رایانه‌ای تهران از طریق سازوکارهای نظارتی خود به تخلف این



آموزشگاه‌ها به دلیل طرح ادعای جعلی دریافت نمایندگی رسمی موسسات آمریکایی فوق رسیدگی خواهد کرد، گفت: سازمان نظام‌صن‌فی رایانه‌ای از طریق ابزار نظارتی خود و با هماهنگی نهادهای متولی این حوزه تخلف این آموزشگاه‌ها را مورد پی‌گیری و رسیدگی قرار می‌دهد. او در این رابطه تاکید کرد: متاسفانه بازار فناوری اطلاعات گاهی اوقات شاهد اغراق‌ها و مطالبی خلاف واقع از سوی برخی فعالان متخلف این حوزه می‌شود که علاوه بر رواج بی‌اعتمادی مخاطبان و افکار عمومی در بازار، به کسب و کار دیگر اعضای صنف لطمه‌ای جبران‌ناپذیر وارد می‌کند.

مسوول کمیسیون آموزش و پژوهش سازمان نظام‌صن‌فی رایانه‌ای تهران با اشاره به لزوم اطلاع‌رسانی سازمان درخصوص ادعای خلاف واقع و تخلف این شرکت‌ها گفت: تمامی مراجعه‌کنندگان و کاربرانی که برای حضور در این دوره‌ها براساس ادعای خلاف واقع شرکت‌های آموزشی ثبت‌نام کرده‌اند، می‌توانند موضوع را برای پی‌گیری به دبیرخانه سازمان نظام‌صن‌فی رایانه‌ای تهران اطلاع دهند تا سازمان براساس ضوابط قانونی موضوع را پی‌گیری کند.

نماینده‌گی جعلی برخی شرکت‌های آموزش فاوا برای برگزاری آزمون‌های بین‌المللی مایکروسافت و سیسکو در ایران کمیسیون آموزش و پژوهش سازمان نظام‌صن‌فی رایانه‌ای تهران نسبت به فعالیت برخی شرکت‌های آموزشی حوزه IT که ادعای نمایندگی رسمی و برگزاری آزمون‌های بین‌المللی سیسکو و مایکروسافت در کشور را دارند، هشدار داد.

به گزارش روابط عمومی سازمان نظام‌صن‌فی رایانه‌ای تهران، خانم مهندس فریبا مه‌دیون، عضو هیات مدیره و مسوول کمیسیون آموزش و پژوهش سازمان با اعلام این خبر گفت: پیروی درج اخبار و تبلیغات برخی شرکت‌های آموزشی حوزه فناوری اطلاعات مبنی بر برگزاری رسمی آزمون‌های بین‌المللی مایکروسافت و سیسکو در ایران، کمیسیون آموزش تحقیقات خود در رابطه با صحت اخذ این نمایندگی‌ها را آغاز کرد و پس از بررسی‌های مختلف مشخص شد برخلاف ادعای جعلی این شرکت‌ها هیچ یک، دارای نمایندگی رسمی جهت برگزاری آزمون‌های بین‌المللی مایکروسافت و سیسکو در ایران نیستند. خانم مه‌دیون با تاکید بر ضرورت آگاهی کاربران و مخاطبان برگزاری این دوره‌های آموزشی در ایران گفت: براساس تحقیقات و پیگیری‌های به‌عمل آمده از سوی کمیسیون آموزش و پژوهش سازمان، هیچ یک از مراکز بین‌المللی برگزاری این دوره‌ها همچون موسسات VUE تاکنون هیچ‌گونه نمایندگی به شرکت‌های ایرانی واگذار نکرده‌اند و شرکت‌های مدعی برگزاری این آزمون‌ها در تبلیغات خود ادعای خلاف واقع را مطرح می‌کنند. این موضوع درحالی است که تاکنون موسسات بین‌المللی فوق هیچ‌گونه قولی مبنی بر واگذاری نمایندگی این دوره‌ها به شرکت‌های ایرانی نداده‌اند. او درخصوص تخلف برخی آموزشگاه‌های IT به منظور جلب مخاطبان بیشتر و بدون ارائه اسناد معتبر در برگزاری آزمون‌های بین‌المللی سیسکو و مایکروسافت گفت: براساس اعلام این موسسات بین‌المللی، تنها شرط اخذ نمایندگی رسمی یا انحصاری این است که شرکت‌ها و آموزشگاه‌های متقاضی بتوانند استانداردهای آموزشی مختلف این مراکز را طی یک فرایند زمانی مشخص کسب کنند که براساس اعلام رسمی این موسسات، تاکنون هیچ آموزشگاه IT در ایران موفق به دریافت این نمایندگی رسمی از سوی شرکت‌های VUE نشده‌اند. مسوول کمیسیون آموزش و پژوهش سازمان نظام‌صن‌فی رایانه‌ای تهران در این رابطه ادامه داد: در طی سالیان متمادی گذشته و حتی قبل از بحث توافق هسته‌ای، این موسسات



برای دانش‌پذیران مزایای اقتصادی جالبی را دربردارد. در این پکیج مهم آموزشی سرفصل‌ها بهینه‌سازی شده و به این شکل که سرفصل دوره‌ها به صورت عادی ۱۶۰ ساعت است اما در این پکیج ۳۰ ساعت مطالب تکراری حذف و دوره در ۱۳۰ ساعت ارائه می‌شود.

Security Pack (SSCP CEH & CISSP)

کاربردترین دوره‌های امنیت شامل دوره‌های CEH، SCP و CISSP است که به صورت جداگانه مشتمل بر ۱۲۵ ساعت خواهد بود. در این پکیج که شامل سه دوره اساسی امنیت است ۱۲۰ ساعت در نظر گرفته شده و این خود از ۱۰۰ ساعت آموزش مفاهیم، عملیات و فرایندهای امنیت شبکه و ۲۰ ساعت کارگاه اجرای سناریوهای واقعی امنیت خواهد بود. ضمن این که این پکیج از نظر اقتصادی برای دانش‌پذیران مقرون به صرفه است.

آموزشگاه سایبرتک به تازگی دوره‌های جدیدی را در حوزه سیسکو طراحی و برگزار کرده که در ادامه به معرفی آن‌ها می‌پردازیم:

Cisco Advanced Technologies

این دوره (پکیج ارائه شده توسط سایبرتک) تخصصی سیسکو، پُرکاربردترین سرفصل‌های CCIE و CCNP Route و CCNP Switch را دارا است. سرفصل‌های این پکیج آموزشی منطبق با بازار کار و براساس تجربه استادان آموزشگاه تهیه و تعریف شده است. سرفصل‌های موجود در این دوره به طور دقیق نیازها و مطالب اصلی متخصصان در سازمان‌ها را پوشش داده.

Routing & switching Pack

این دوره یکی از مهم‌ترین کورس‌های سیسکو است. شامل ۱۱۰ ساعت آموزش عملی و ۲۰ ساعت کارگاه اجرای سناریوی واقعی. ارائه این پک در سایبرتک

گزارش



سمینار بررسی اشکالات فعلی امنیت اطلاعات در ایران - چهارم شهریور در سایبرتک

مرتبط اقدام کرده‌اند. در ایران هم سالیانی است برخی از این دوره‌ها تدریس می‌شود. در این سمینار که با حضور مهندس روزبه نوروزی استاد دوره‌های امنیت سایبرتک در تاریخ چهارم شهریور ماه برگزار شد، به اشکالات مبحث امنیت اطلاعات در ایران مختص دوره‌های فوق، پرداخته شد و راهکارهای گریز از مشکل کنونی به بحث و بررسی گذاشته شد. در این سمینار به سوال‌های زیادی نیز پاسخ داده شد که نشان از استقبال خوبی از این سمینار دارد. همچنین قابل ذکر است که به زودی سمینار دیگری در راستای امنیت اطلاعات



برحسب اهمیت روز افزون امنیت اطلاعات در جهان، تربیت متخصص و نیروی کار در این رشته اولویت بالایی یافته است. در این راستا با توجه به نیاز بازار و تجربه‌های سالیان قبل، دوره‌هایی در جهان توسط تعدادی ارائه دهنده، تدوین شده است که گواهی‌نامه‌هایی نیز به قبول شدگان در امتحان مربوطه اعطا می‌شود تا سطح صلاحیت برای مشاغل امنیت اطلاعات احراز بشود. دریافت این گواهی‌نامه‌ها منوط به داشتن تجربه و دانش مرتبط

است و در این مسیر آموزشگاه‌ها نیز نسبت به برگزاری دوره‌های توسط مهندس روزبه نوروزی برگزار خواهد شد.

برخورد نزدیک از نوع امن!

گفت‌وگوی سایبرنامه با مهندس روزبه نوروزی، استاد دوره‌های امنیت آموزشگاه مهندسی سایبر تک

با توجه به این که شماره پیش‌روی سایبرنامه درباره امنیت اطلاعات است، به سراغ مهندس روزبه نوروزی استاد دوره‌های امنیت آموزشگاه مهندسی سایبر تک رفتیم و گپ و گفتی دوستانه با ایشان انجام دادیم. مصاحبه‌ای که می‌خوانید شرح و احوال گفت و گوی ما با ایشان است.

امنیت من را به شعله تبدیل کردند که مهم‌ترین آن‌ها «امضای دیجیتال» کاری از انتشارات اورلی بود که برایم مشوق بزرگی در این مسیر بوده است.

• از دیدگاه شما امنیت اطلاعات چیست؟

ه باید ببینیم اطلاعات چیست؟! اطلاعات مجموعه‌ای از دارایی‌ها است که ارزش‌های متفاوتی دارند و به تبع آن بایستی برای آن‌ها سطح حفاظت متناسب در نظر گرفت. این سطح حفاظت متناسب وابسته به ارزش دارایی و میزان ریسک مرتبط بر آن است. همچنین بایستی اطلاعات به هر نحو ممکن در موقع

روزبه نوروزی - متولد ۱۳۵۷ تهران. دانش‌آموخته‌ی کارشناسی ارشد مهندسی ژئودزی و ژئوماتیک از دانشگاه صنعتی خواجه نصیرالدین طوسی تهران در سال ۱۳۸۳ با پایان‌نامه‌ای در زمینه معماری سیستم‌های توزیع شده عامل پایه.

بیش از ۱۵ سال در حوزه فناوری سیستم‌های اطلاعاتی و امنیت مشغول به فعالیت است و نزدیک ۹ سال در این حوزه‌ها تدریس می‌کند. شغل‌هایی که داشته‌اند؛ در چندین موسسه و سازمان دولتی و خصوصی به صورت تمام‌وقت کارشناس ارشد و مدیر بوده‌اند. در برخی موارد نیز به صورت مشاوره‌ای در حوزه‌های فناوری اطلاعات و امنیت بوده که دامنه وسیعی از سازمان‌ها را شامل شده که می‌توان از وزارت راه و ترابری و شیلات ایران تا انواع موسسات مالی و بانک‌ها که در سال‌های اخیر بر بحث تحقیق و کشف و پیگرد جرایم رایانه‌ای متمرکزتر شده‌اند، اشاره کرد. سه سال قبل مدیر امنیت شبکه موسسه اعتباری ثامن بوده و اکنون به عنوان مدیر مرکز عملیات امنیت (SOC) موسسه اعتباری ثامن و مدیر پروژه‌های این مراکز در شرکت ثامن ارتباط عصر مشغول به کار هستند. در کنار کار روزانه، برای پی‌گیری علاقه و همچنین تغییر برخی ناهنجاری‌ها در تدریس امنیت اطلاعات در ایران همچنین ترویج علم امنیت اطلاعات در بدنه کشور، با موسسات آموزشی کشور در این زمینه همکاری دارند. ایشان کتاب مقدمه‌ای بر مراکز عملیات امنیت را تالیف کرده‌اند و همچنین نیز در مجلات بانکداری الکترونیک و برخی از روزنامه‌ها، مقالات امنیت اطلاعات و مدیریت پروژه را به چاپ رسانده‌اند.

• نخست بفرمایید که چگونه وارد عرصه فناوری

اطلاعات و امنیت اطلاعات، قدم نهادید؟

ه دغدغه امنیت از ضروریات یک متخصص امنیت اطلاعات است. بدین سبب از دوران تحصیلات کارشناسی که تجربه برنامه‌نویسی داشتم دغدغه‌های امنیتی برایم بسیار مهم بود و باعث می‌شد علاوه بر این که در حوزه برنامه‌نویسی به دنبال مسایل امنیتی باشم در سایر امور زندگی نیز این موضوع را رعایت کنم. به طوری که در هر دوره برنامه‌نویسی که شرکت می‌کردم اساتید از حجم سوالات من در حوزه امنیت نرم افزار به مرز کلافگی می‌رسیدند! اما چندین کتاب جرقه‌های ذهنی

تولید، انتقال و ذخیره سازی لایه های مختلف اعم از فیزیکی، شبکه، نرم افزاری و ... حفاظت شوند و این یعنی دیگر روش های حفاظتی نیز برای آن ها اندیشیده شود. حفاظت در لایه فرآیندها و پرسنل نیز از مقوله هایی است که کمتر به آن ها پرداخته می شود. پس امنیت اطلاعات، حفاظت متناسب و به جا و درخور از اطلاعات در تمام لایه های ممکن به نحوی که جامعیت، در دسترس بودن و محرمانگی آن ها حفظ شود.

به آسیب پذیری های جهانی و سازمان داشته باشند و بتوانند با تلفیق داده های موجود از هزاران دستگاه سیستم اطلاعاتی شما و با بهره گیری از ابزارهای اتوماتیک سازی تلفیق، نفوذ را شناسایی، گزارش و برای حل آن راهکار بدهند و همچنین کنترل بحران را هم به نحو مطلوب به سرانجام برسانند. متخصصان تطابق سنجی بایستی با بازرسی دوره ای سازمان تطابق کنترل های امنیتی را با قوانین و اهداف سازمان را بسنجند.

• آیا استاندارد یا روش خاصی برای این فناوری در نظر گرفته شده؟

در جهان استانداردها و بهینه روش های متعددی برای پیاده سازی امنیت اطلاعات ابداع شده. از این دست می توان به ISO ۲۷۰۰۱ و قوانینی چون FISMA اشاره کرد. برای استانداردهای موجود، دستگاه ها و نرم افزارهایی وجود دارد که متخصصان تطابق سنجی و مدیران امنیت باید دوره های آشنایی با آن ها را بگذرانند.

• نقش آموزش و یادگیری این مهارت را در دنیای کنونی توضیح دهید؟ آیا در کشورمان به این مقوله درست پرداخته شده؟

علاقه مند امنیت اطلاعات اولاً باید یک شاخه از امنیت را شروع، بعد با کسب تجربه و گذراندن دوره های مختلف دانش خود را در سایر شاخه ها گسترش دهد اما باید دانست دانش زیرساخت هر فناوری امنیتی نیز برای متخصص امنیت اطلاعات ضروری است. برای مثال متخصص امنیت شبکه اول باید در زیرساخت شبکه به دانش و مهارت مورد نیاز برسد تا بتواند متخصص امنیت ماهر در حوزه شبکه باشد. با توجه به این که آموزش های دانشگاهی به هیچ عنوان کفایت نیاز بازار کار را نمی دهد، باید هر شخص برای قدم گذاشتن در وادی امنیت اطلاعات دوره های لازم را متناسب با نقشه مسیری که برای آینده خود در نظر گرفته است، بگذراند. امروزه نیاز به متخصص امنیت اطلاعات در ایران بسیار بالا است و دانش آموختگان صاحب تخصص به راحتی جذب بازار کار می شوند. حالا آیا در ایران درست پرداخته شده یا نه، باید بگوییم؛ متأسفانه در ایران از دو جهت امنیت اطلاعات مهجور مانده. نخست از لحاظ ساختارها و قوانین؛ و دوم از لحاظ آموزش صحیح بحث ساختارها و قوانین... که سپس بیان می کنم. اما در بحث آموزش باید گفت متأسفانه بنا به دلایل متعدد کیفیت آموزش امنیت اطلاعات در برخی آموزشگاه ها در سال های اخیر اُفت پیدا کرده و این به واسطه عدم گذراندن پیش نیازها توسط دانشجو، عدم تدریس مطابق سرفصل ها و از همه مهم تر به روز نبودن و مدرک نداشتن مدرسان این دانش به وجود آمده است. یک متخصص امنیت اطلاعات باید دانش محکم و چند رشته ای را داشته باشد تا بتواند با احاطه کامل در مسایل ورود کند.

• جایگاه دانش امنیت اطلاعات در جوامع امروزی چگونه است؟

با توجه به این که از سالیان قبل مهاجرت از دنیای کاغذ به دیجیتال در کشورهای پیشرفته انجام شده، آن کشورها از مبانی حفاظت از آن داده ها گذشته و اکنون با موارد جدیدی که به واسطه باز تولید داده از داده نمود پیدا کرده است درگیر هستند. مباحثی چون Big data از این قبیل اند و دیگر موارد تهدیدات نسل جدید امنیتی که بسیار پیچیده اند هم می شود اشاره کرد. این تهدیدات کشورها را برای تولید نسل جدید تجهیزات امنیت و نسل های نوین مراکز عملیات امنیت ترغیب کرده اند. همان طور که گفتم بر اساس آمار منتشر شده، دیده می شود نیاز به متخصص امنیت اطلاعات بسیار بالاست.

• امنیت اطلاعات براساس چه برنامه هایی و توسط چه کسانی باید پیاده سازی شود؟

تصور غلطی که در برخی موارد جاری شده این است که امنیت اطلاعات را با امنیت شبکه برابر می دانند. در صورتی که امنیت شبکه تنها یکی از ۵ شاخه امنیت اطلاعات است. امنیت اطلاعات شامل امنیت شبکه، امنیت سیستم ها، ارزیابی و ممیزی، تطابق سنجی و تحلیل وقایع امنیتی است. این پکیج بایستی توسط متخصصان امنیت اطلاعات که هر کدام در شاخه های خود فوق تخصص دارند در تعامل با یکدیگر پیاده سازی شوند. البته همکاری سایر بخش های مجموعه فناوری اطلاعات سازمان، نظیر زیرساخت شبکه و سیستم ها برای پیاده سازی امنیت اطلاعات، لازم و حیاتی است و باید رابطه بسیار محکم و حسنه ای بین این بخش ها برقرار باشد. مطابق زیرشاخه های امنیت اطلاعات که در بالا بیان شد، متخصصان امنیت شبکه بایستی توانایی طراحی امن شبکه و جانمایی و پیاده سازی دستگاه های امنیتی را داشته باشند. متخصصان امنیت سیستم ها باید بتوانند انواع تهدیدهای مرتبط بر سیستم های عامل و زیرساخت های مرتبط را رفع کنند. متخصصان ارزیابی و ممیزی نیز باید بتوانند با آنالیز ریسک و انجام تست های نفوذ موردی، سطح امنیتی سیستم ها را استخراج و برای به سازی وضع موجود راهکار ارائه دهند. متخصصان تحلیل وقایع امنیتی باید دیدی جامع

• به نظر شما جایگاه سایبرتک در ارایه این دانش چگونه بوده؟

آموزشگاه سایبرتک با توجه به قدمتی که دارد توانسته در خیل مخاطبان این رشته برای خود نامی نیک در زمینه آموزش فناوری اطلاعات برجای بگذارد و با توجه به آفق کاری که جناب دکتر کاظمی تبیین کرده‌اند، می‌توان دید در حوزه امنیت اطلاعات و فناوری‌های مربوطه با سرمایه‌گذاری‌هایی که شده بتوان سطح دانش علاقمندان این مرزو بوم را به میزان قابل ملاحظه‌ای ارتقا داد، چرا که همان کیفیت سابق در حوزه امنیت هم در حال پی‌گیری است و به نحوی که تغییرات سریع در حوزه امنیت اطلاعات که متغیرترین آن است خللی در کیفیت آموزش پیش نیاورد و نیز فرآیندهایی که آموزشگاه در نظر گرفته، اساتید همیشه به دانش و فن روز مسلط باشند. درضمن سعی هم می‌شود ارایه دوره‌ها با کیفیت و استاندارد اصلی و به‌روز قابل ارایه باشند.

• در پایان پیشنهاد، راه‌کار و هر مطلبی که باعث تشویق و ترغیب علاقه‌مندان این حوزه دارید، بفرمایید؟

عوامل مشوق برای هرکس تفاوت دارد اما دواعمل برای بسیاری جزو مشوق‌های بزرگ هستند، یکی آینده شغلی و درآمد - دیگری تنوع و هیجان انگیز بودن آن.

درخصوص این دو عامل باید بگویم در خارج از کشور براساس نظرسنجی و آمارگیری مراکز معتبری چون Forrester، کمبود متخصص امنیت اطلاعات از دوسال قبل شروع شده و پیش‌بینی‌ها نشان می‌دهد که این کمبود در سال‌های آینده جدی‌تر شود. به همین دلیل سازمان‌های تحقیقاتی در حال بررسی چگونگی حل این موضوع هستند. با توجه به هزینه بسیار پایین آموزش در ایران نسبت به خارج از کشور می‌توانند آینده خوبی را برای خود متصور باشند چرا که پرداخت‌ها در این حوزه‌ها نیز براساس آمار خوب است. در ایران با توجه به نبود اطلاعات آماری در این زمینه، بنده تجربه شخصی خود را عرض می‌کنم. با توجه به این‌که چندین سال است در حوزه مصاحبه و جذب نیروی انسانی امنیت اطلاعات سازمان‌ها و نهادهای مختلف و از طرفی طراحی ساختار سازمانی آن‌ها در حال فعالیت هستم، می‌بینم که اکنون مقوله امنیت اطلاعات در ایران در عنوان جوانی است. نیروی متخصص کاربلد برای پست‌ها پیدا نمی‌شود، به نحوی که سازمان‌ها در برخی موارد مجبور شده‌اند نیروهایی با سطح دانش کمتر استخدام کنند و خود وظیفه آموزش آن‌ها را برعهده بگیرند. در سال‌های آینده با توجه به رشد بسیار زیاد که صنعت امنیت اطلاعات در ایران خواهد داشت من پیش‌بینی می‌کنم اگر برای تامین و آموزش متخصص امنیت اطلاعات کاری نشود در این حوزه دچار مشکل بزرگی خواهیم شد. درست است که دانشگاه‌هایی در کشور در حال تربیت متخصص امنیت اطلاعات، حتی تا درجه‌ی دکترا هستند اما با توجه به این‌که در کشور ما حوزه خدمات امنیت اطلاعات رشد کرده و نیازمندی در این حوزه بالا است، آموزش‌های

دانشگاهی درصد بسیار کمی از نیاز بازار را تامین می‌کنند. به جرات می‌گویم حتی برای دانش‌آموخته دکترای امنیت اطلاعات از دانشگاه معتبر در ایران نمی‌توان جایابی شغلی کرد مگر این‌که دوره‌های آموزشی در آموزشگاه‌های تخصصی آی‌تی (امنیت اطلاعات) را گذرانده و مدارک بین‌المللی را اخذ کنند تا شغل در مقام و اعتبارشان بتوان در نظر گرفت.

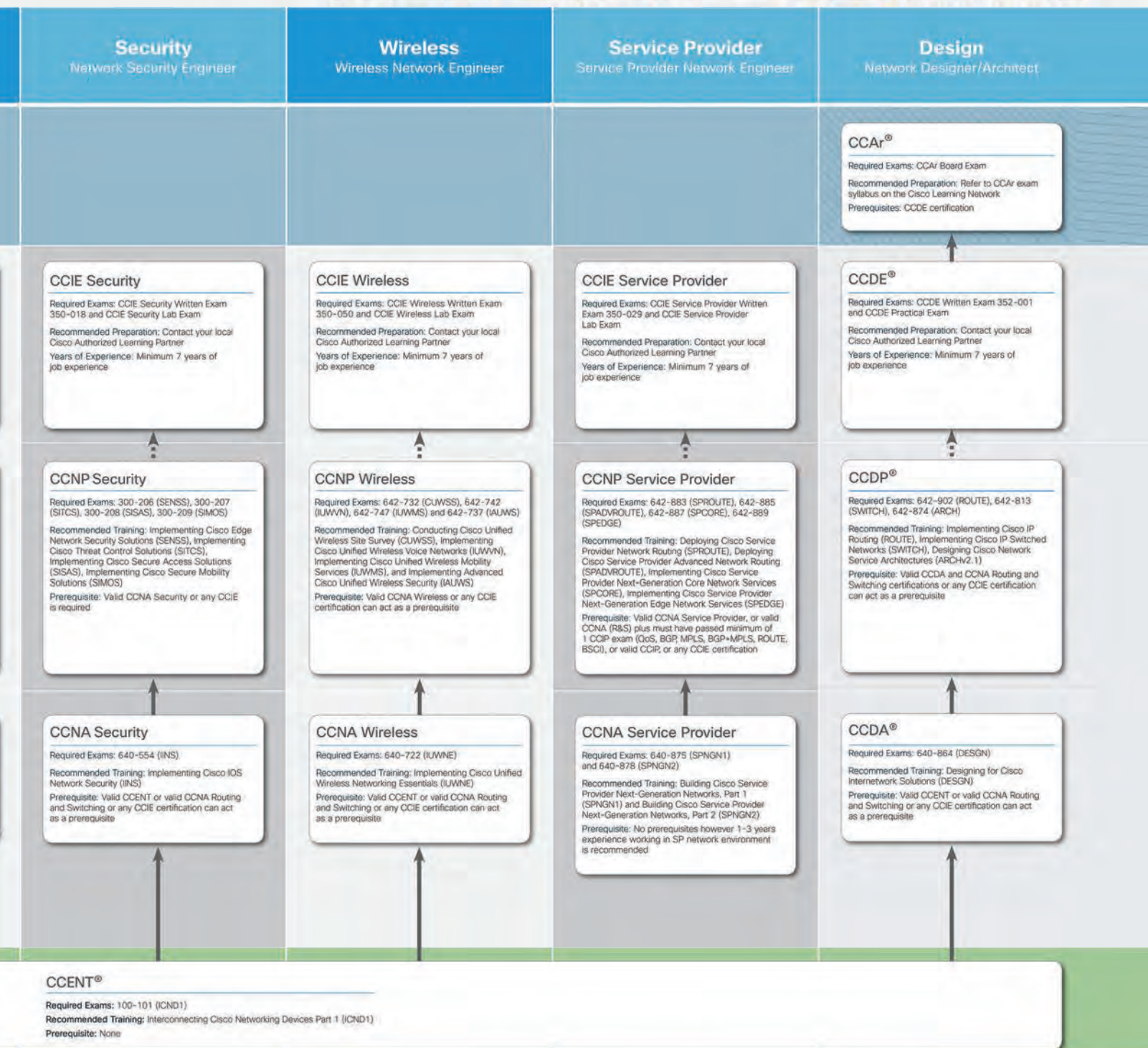
• جناب مهندس اگر در این راستا مطالب دیگری به ذهن‌تان رسیده، ارایه بفرمایید؟

بله! اگر اجازه بدهید دو نکته قابل ذکر است که بیان کنم. یکی در حوزه آموزش امنیت اطلاعات و دیگری در حوزه قانون‌گذاری؛ نکته اول: در بحث امنیت اطلاعات تقریباً همه هشیار شده‌اند، نمی‌گویم آگاه!! چرا که آگاه شدن نیازمند آموزش با توجه به سطح دانش و نیازمندی مخاطب است که در ایران با جدیت دنبال نمی‌شود. این هشیار بودن خوب است و همه دنبال عقد قراردادهای امنیتی هستند، بدون توجه به اصول پایه‌ای امنیت اطلاعات در زمینه اسکپ‌کار، آنالیز ریسک و ساختار سازمانی یا حتی عقد قرارداد. این مهم به چند دلیل بروز کرده است، نخست برای این‌که ساختارهای امنیت اطلاعات در سازمان‌ها و نهادهای به‌درستی شکل نگرفته است، بدنه کارشناسی از دانش بالایی برخوردار نیست و مدیریت‌ها هم که بایستی مطابق با اصول امنیت اطلاعات به‌مبانی مدیریت این حوزه‌ها واقف باشند به‌طور ناقص دوره‌ها را گذرانده‌اند. پس تنها چیزی که من می‌بینم تعدادی هکر جوان و باعلاقه هستند که در گوشه گوشه‌های کشور در حال کار بوده و بدنه کارشناسی و سطوح مدیریتی ما یا دوره‌های امنیت اطلاعات را نگذرانده‌اند یا اگر حتی گذرانده باشند در صورت اخذ امتحان نمره بسیار پایینی خواهند گرفت. چندی پیش یکی از دوستان که مدیر مرکز مهم امنیت است بیان می‌کرد که کارشناسان ما تمام دوره‌ها را رفته‌اند اما تغییری را در سیستم خود مشاهده نمی‌کنم!! پس ما نیازمند طراحی متدهای آموزشی و آموزش مجدد کارشناسان و مدیران امنیت اطلاعات سازمان‌ها هستیم. نکته بعدی: درست است که همه در ایران در خصوص امنیت اطلاعات هشیار شده‌اند اما پیاده‌سازی امنیت سلیقه‌ای نیست و باید بر اساس اصول مرتبط باشد و مسایل قانونی آن حل شود. پیاده‌سازی صحیح امنیت اطلاعات ضمانت قانونی می‌خواهد، قانون‌هایی که برای هر حرفه و حوزه کاری به دقت و تخصصی تدوین شده‌اند، به عنوان مثال: HIPPA، SOX و ... در ایران با توجه به تدوین قانون جرایم رایانه‌ای، دیده می‌شود که این حوزه برای اعمال حاکمیت، نیاز به تدوین قوانین جزئی و مخصوص به حرفه‌ای بودن را دارد. با قوانین تخصصی و نظارت بر آن می‌توان هم به رشد امنیت اطلاعات امید بست هم به پیاده‌سازی صحیح آن.

جناب مهندس، با سپاس فراوان از شما بابت زمانی که قرار دادید تا منجر به چنین گفت‌وگوی نرباری شود!!

Networking

Working career.
and financial rewards.

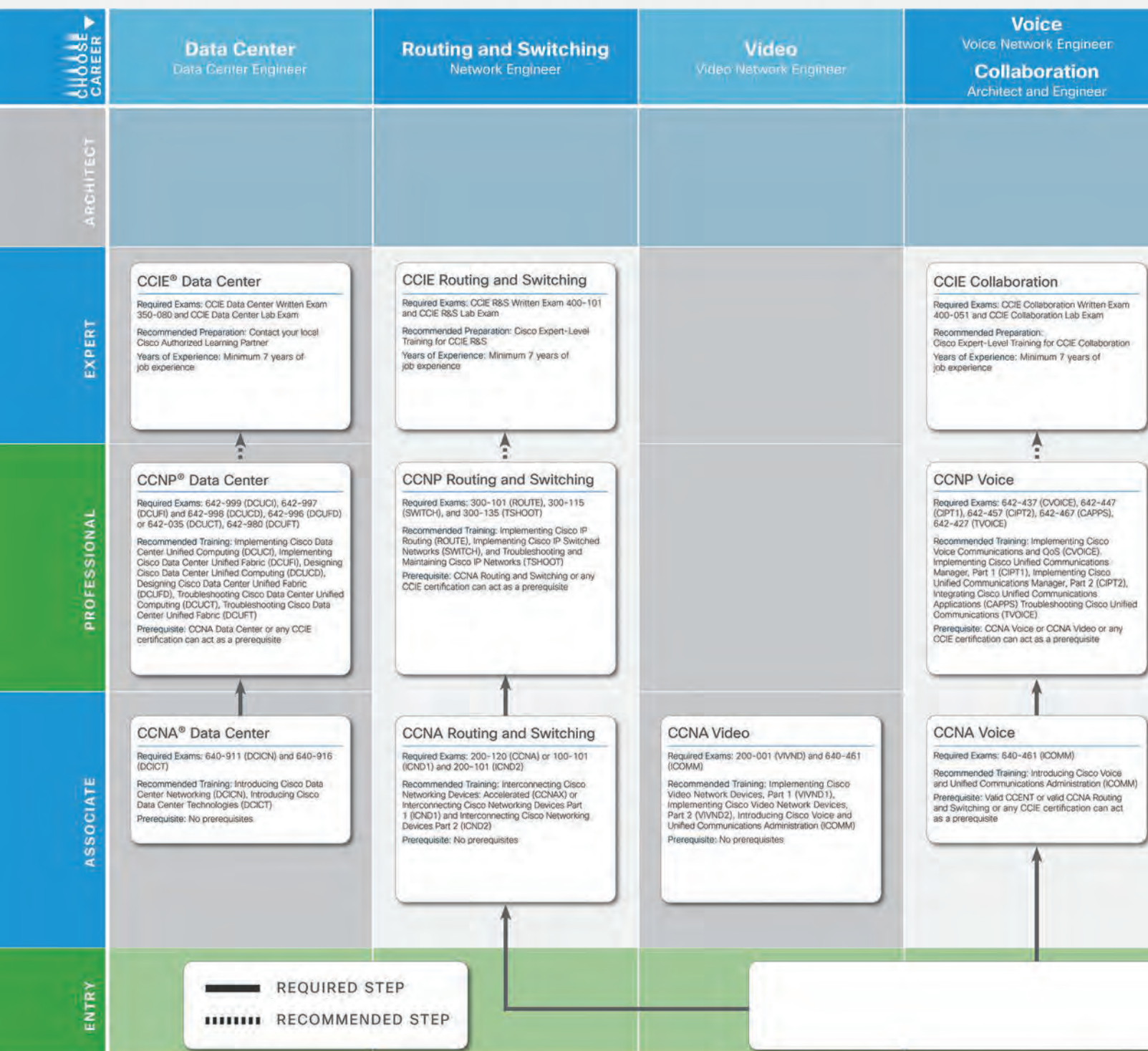


Enhance Your Core Knowledge with Specialist Certifications

- [Data Center](#)
- [Security](#)
- [Operating System Software](#)
- [Video](#)
- [Virtual Classroom Instruction](#)
- [Enterprise IT Business](#)
- [Internet of Things](#)
- [Network Programmability](#)
- [Service Provider](#)



Cisco Certifications help you launch and advance your IT Network career. Choose a career path that meets your goals for professional and personal growth.



Make the Next Move

To learn more about Cisco Certifications training and exam requirements, visit the Cisco Learning Network at ciscolearningnetwork.com.



اقدامات ضروری پس از کشف نفوذ

اگر شرکت یا سازمان شما قربانی نفوذ شده، اقداماتی لازم است تا آسیب نبینید.

شرکت Heartland Payment Systems که یکی از بزرگ‌ترین شرکت‌های ارائه خدمات مالی در دنیاست، در سال ۲۰۰۹ اعلام کرد که قربانی یک حمله نفوذی ویرانگر شده: اطلاعات کامل ۱۳۴ میلیون کارت اعتباری در اختیار افراد نفوذگر قرار گرفته بود. این حمله با استفاده از نصب جاسوس افزار روی سیستم‌های ذخیره داده هارتلند، از طریق حمله SQL Injection انجام شده بود. این شرکت، مسوول پردازش تراکنش‌های انواع کارت‌های اعتباری، پرداخت‌های آنلاین، سرویس‌های پرداخت حقوق و چک‌های بانکی است. هارتلند در زمان کشف حمله، ماهیانه ۱۰۰ میلیون تراکنش را برای ۱۷۵ هزار مشتری از شرکت‌های کوچک تا رده متوسط انجام می‌داد. طبق گزارش‌های خبری، کامپیوترهایی که در هارتلند برای پردازش پرداخت‌ها و تراکنش‌ها مورد استفاده قرار می‌گرفتند، در سال ۲۰۰۸ تحت نفوذ قرار گرفته‌اند. داده‌ها نیز شامل تمامی اطلاعات مورد نیاز برای ساخت کارت‌های تقلبی می‌شدند، از جمله داده‌های رمزنگاری شده روی نوار مغناطیسی کارت.

طبق گفته‌های کوین جاج، از سایت امنیتی کومودو، رخنه مذکور وقتی کشف شد که شرکت «ویزا» و «مسترکارد» متوجه تراکنش‌های مشکوکی در حساب‌های تحت پردازش هارتلند شدند. سپس، هارتلند یک جاسوس افزار پیدا کرد که توسط هکرها کارگذاری شده بود و در یک دوره چندماهه در سال ۲۰۰۸، به دزدی داده‌ها پرداخته بود. جاج می‌گوید: «در حقیقت، رخنه یک حرکت برنامه‌ریزی شده بسیار آهسته بود. این رخنه با یک حمله SQL Injection در اواخر سال ۲۰۰۷ آغاز شده که مرکز داده آن‌ها را در معرض خطر قرار داده است. یک حمله SQL Injection فرمان‌های مرکز داده را ضمیمه کدهای موجود در اسکریپت وب می‌کند. هارتلند دریافت که کد دست‌کاری شده در یک صفحه وب لاگین وجود دارد که هشت سال پیش از کشف، در آن جا پیاده‌سازی شده است. اما این برای نخستین بار بود که نقطه آسیب‌پذیر مذکور مورد سوءاستفاده قرار گرفته بود.» طبق گفته‌های جاج، هکرها پس از آن هشت ماه را صرف دست‌یابی به سیستم پردازش پرداخت کردند و همزمان، اقدام‌هایی برای مخفی ماندن از دید چندین راه‌کار ضد ویروس مختلف در سیستم‌های هارتلند، انجام دادند. آن‌ها در نهایت نوعی از جاسوس افزار را در سیستم نصب کردند که «اسنیفر» خوانده می‌شود. این ابزار همزمان با پردازش پرداخت‌ها، به ثبت داده‌های کارت می‌پردازد. برنامه‌های اسنیفر برای نظارت بر ترافیک شبکه جهت تجزیه و تحلیل و حل مشکلات کاربرد دارند. متأسفانه، کاربرد دیگر آن‌ها نیز ثبت داده برای اهداف

تبه‌کارانه است. در این مورد، داده‌های مسروقه همه اطلاعات مورد نیاز برای ساخت کارت تقلبی هستند. عواقب

این ضعف امنیتی بسیار شدید بود. هارتلند به‌طور موقت صلاحیت خود را در PCI DSS از دست داد. علاوه بر این، هارتلند موظف شد ۱۴۵ میلیون دلار بابت پرداخت‌های جعلی خسارت پرداخت کند. در سال ۲۰۰۹ نیز، سه نفر بابت رخنه امنیتی هارتلند مورد تعقیب قرار گرفتند.

حدود ۹ ماه پس از رخنه، جان آر ساوث به‌عنوان مدیر ارشد امنیتی به هارتلند پیوست؛ یعنی زمانی که شرکت هنوز در دوره نقاهت پس از حمله به سر می‌برد.

او پیش از این، در چندین شرکت بزرگ بین‌المللی مدیر امنیت اطلاعات بود. ساوث به‌عنوان CSO مسوول رهبری و نظارت بر برنامه‌های اصلی شرکت است که حفاظت از اطلاعات حساس شرکت را در بر می‌گیرد. او یک فرایند شبیه‌سازی ریسک و حمله را در دستور کار قرار داده و همچنین بر رعایت تعهدات سازمانی و قانونی نظارت می‌کند.

ساوث پیش از این، عضو هیات مدیره مرکز FS-ISAC بوده که انجمن اصلی صنعت برای تعاملات اعضا، درباره حمله‌های بحرانی امنیتی به حساب می‌آید؛ حمله‌هایی که بخش خدمات مالی صنعت را تهدید می‌کنند. او همچنین عضو هیات مشاوران مرکز PCI SSC بوده و وظیفه‌اش قدرت بخشیدن به استانداردهای امنیتی و حفاظت از داده‌های کارت‌ها در مقابل تهدیدهای جهانی بوده است.

علاوه بر این‌ها، ساوث استاد دانشگاه دالاس در مباحث امنیتی، مشاور چندین

قربانی‌های بزرگ

یک پژوهش جدید از موسسه پوینمون نشان می‌دهد هزینه متوسط تبهکاری سایبری برای فروشگاه‌های زنجیره‌ای در آمریکا از سال ۲۰۱۳ به بیش از دو برابر، یعنی رقم ۸,۶ میلیون دلار برای هر شرکت رسیده است. هزینه متوسط سالانه حمله‌های سایبری موفقیت‌آمیز در صنایع مختلف نیز، برای هر شرکت به این ترتیب است: ۲۰,۸ (خدمات مالی)، ۱۴,۵ (در بخش فناوری) و ۱۲,۷ میلیون دلار در صنایع ارتباطی.

جداً از هزینه‌های مالی فوق، رخنه‌های حایز اهمیت نیز در میان شرکت‌ها در سال ۲۰۱۴ رخ داد که به حسن شهرت شرکت آسیب وارد کرد:

* Target. در ژانویه ۲۰۱۴ تارگت اعلام کرد که اطلاعات شخصی ۷۰ میلیون نفر دیگر طی یک نفوذ در دسامبر ۲۰۱۳ دزدیده شده که در میان آن‌ها اطلاعات کارت اعتباری ۴۰ میلیون مشتری نیز موجود بوده است.

* Neiman Marcus. بین ژوئیه و اکتبر ۲۰۱۳، اطلاعات کارت اعتباری ۳۵۰ هزار نفر دزدیده شد و بیش از ۹۰۰۰ کارت اعتباری مورد سوءاستفاده قرار گرفت.

* Michaels Stores. بین ماه مه ۲۰۱۳ تا ژانویه ۲۰۱۴، کارت خرید ۲,۶ میلیون نفر از مشتری‌ها دستکاری شد.

* eBay. حمله‌های سایبری در اواخر فوریه و اوایل مارس باعث به خطر افتادن اطلاعات لاگین کارکنان شرکت شد و در نهایت دسترسی به مشخصات و اطلاعات لاگین ۲۳۳ میلیون کاربر سایت برای نفوذگران فراهم شد.

* U.S. Investigations Services. این شرکت که یک پیمان‌کار برای بررسی پیشینه کارکنان فدرال است، قربانی یک رخنه اطلاعاتی شد که باعث به سرقت رفتن اطلاعات شخصی کارکنان شد.

* Community Health Services. بین ماه‌های آوریل تا ژوئن، اطلاعات شخصی ۴,۵ میلیون بیمار CHS در دسترس نفوذگران قرار گرفت.

* Home Depot. تبهکاران سایبری با استفاده از بدافزار اطلاعات شخصی ۵۶ میلیون خریدار را به دست آوردند.

* Google. طبق گزارش‌های غیررسمی، نام کاربری و رمز عبور ۵ میلیون کاربر مورد سوءاستفاده قرار گرفته است.

* Apple iCloud. طبق گزارش‌ها، هکرها با تaktیک‌های brute force و نرم‌افزارهای خاص، به داده‌های ذخیره‌شده کاربران اپل دست یافتند.

* Bartell Hotels. بین فوریه تا مه، اطلاعات ۵۵ هزار مشتری مورد سوءاستفاده قرار گرفت.



نهاد

امنیتی ملی و دارنده جوایزی

همچون ۲۰۱۱ ISE، مدیردهه ISE و صد مدیر برتر Computerworld Premier در سال ۲۰۱۲ نیز است.

بنابراین، او در حوزه امنیت فردی کهنه‌کار و آزموده است. با این حال، هنوز ممکن است این سوال پیش بیاید که چرا سمت CSO را در هارتلند پذیرفته، به خصوص پس از داستان رخنه امنیتی. آیا ارزش ریسک را داشته است؟ پاسخ او این است: «بدون شک! این برای من یک چالش بود. اما من می‌دانستم افرادی در شرکت هستند که برای جبران نفوذ کار می‌کردند و به مدیرعامل و گروه مدیریتی نیز اطمینان داشتم. بنابراین موقعیت مذکور را بیش از ریسک، یک فرصت می‌دیدم، برای انجام یک کار خوب.»

طبق گفته ساوث، در زمان پیوستن او به مجموعه، بخش زیادی از مشکل جبران شده بود و برای انجام این کار در مدت کوتاه، تلاش و هزینه زیادی صرف شده بود. یکی از عوامل تبدیل مشکل به فرصت توسط ساوث، عملکرد مدیرعامل، یعنی رابرت اُکار بود. به عنوان، کار با مساله نفوذ بسیار باز برخورد کرد و اطلاعات زیادی را عمومی کرد تا شرکت‌های دیگر را نیز ترغیب کند که اطلاعات مربوط به حمله‌های امنیتی را منتشر کنند و با یکپارچگی بیشتر در مقابل بزه‌کاران سایبری بایستند. او همچنین مجمعی تشکیل داده تا شرکت‌ها بتوانند با سرعت و راحتی بیشتری به انتشار اطلاعات در میان رسانه‌ها بپردازند.

تمرکز ساوث از آن زمان تا کنون روی این بوده که همیشه جلوتر از نفوذگرها باشد. او این کار را با به‌کارگیری جدیدترین فناوری‌ها و افزایش تعامل با شرکت‌های همکار انجام می‌دهد.

طبق گفته ساوث، یکی از چالش‌های همیشگی او این است که در باید رخنه‌ها چگونه می‌توانند اتفاق بیفتند. او می‌گوید: «ما باید مطمئن شویم که محیط برنامه امن است. از درک مسایلی گرفته که از محیط مبتنی بر برنامه برمی‌خیزند تا زدودن مسایل پیش از عملی شدن، شامل این فرایند می‌شود.» او همچنین یکی از موارد مورد توجه را بهینه‌سازی روش‌های کدنویسی و آموزش درست کارکنان می‌داند تا باعث ایجاد خطا در محیط‌های مبتنی بر برنامه نشوند.

و معماران برنامه اطمینان یابند که محیط نرم افزاری امن است. مرحله بعدی آزمایش مداوم ساز و کار است که شامل تست کارایی، آسیب پذیری و تست نفوذ می شود.

آن طور که ساوث می گوید، برای دستیابی به تمام این اهداف به یک فناوری امنیتی نیاز است که امکان آزمایش موثر را فراهم کند و همچنین قادر باشد مسایل را در محیط شبیه سازی کند. او می گوید: «ما حجم انبوهی از داده های امنیتی را در طول یک روز جمع آوری می کنیم، بنابراین توانایی شبیه سازی کارآمد وقوع مسایل در محیط، باید حل شود. این امکان ما را تا حد امکان فعال می سازد تا اتفاق ها را قبل از وقوع پیش بینی و بحران را کاهش دهیم.»

علاوه بر این به یک گروه دانش نیاز است تا چرخه حیات داده را در محیط زیر نظر داشته باشد؛ داده وارد شده، پردازش و ذخیره می شود و در طول چرخه حیات داده، تعدهای امنیتی برای رعایت وجود دارد و گروه هایی که در زمان معین باید در موقعیت مشخص قرار گیرند. همچنین ملاحظاتی مانند دسترسی کاربر و امنیت فیزیکی نیز وجود دارد که باید به آن ها پرداخته شود. در مجموع، باید یک قدم از نفوذگر جلوتر باشید، مشکلات بالقوه را بررسی کنید و این که در صورت به خطر افتادن شبکه، این مشکلات چگونه پیش می آیند.

یک بخش کلیدی دیگر که ساوث آن را به استراتژی امنیتی هارتلند اضافه کرده توانایی گردآوری هوشمند است؛ این که در حمله های بالقوه اطلاعات را دریافت کرد و به اشتراک گذاشت.

ساوث می گوید: «اگر حمله ای را مشاهده کنم که به یک رقیب وارد شده و اطلاعات میان ما نیز مشترک باشد، باید پیش از وقوع حادثه آن را پیش بینی کنیم و شاخص های آن حمله شناسایی و با آن مقابله کنیم. این، خلاصه تجربه ای است که از رخنه به هارتلند حاصل شد. اگر ما پیش از وقوع، داده های مربوطه را دیده بودیم، شاید می توانستیم جلوی آن را بگیریم. امروز، می توانیم چنین پیش بینی داشته باشیم و این یک ابزار کارآمد است. توانایی ها در حال بهبود مستمر است و روابط خصوصی و عمومی نیز رو به افزایش است تا به جایی برسیم که بتوانیم داده ها را به اشتراک بگذاریم.»

گفت و گو

استیو چابینسکی مشاور ارشد و مدیر ارشد امنیت (مخاطرات) در شرکت کراود استرایک است. این شرکت در حوزه فناوری های امنیت سایبری فعال است و تخصص ویژه آن نیز نظارت مداوم و بی درنگ بر تهدیدها و حملات، گزارش دهی هوشمند، آزمایش نفوذ به شبکه و واکنش سریع به حادثه است. چابینسکی همچنین قائم مقام واحد سایبری اف بی آی بوده است و به شرکت های بزرگ درباره واکنش مناسب به حمله سایبری یا رخنه مشاوره می داده است. در ادامه شاهد گفت و گویی با چابینسکی خواهید بود که در آن به جدیدترین مسایل و ملاحظات امنیتی پرداخته ایم.

● نشریه سکیوریتی: اولین کسی که مدیر یا مسوول امنیت پس از کشف رخنه امنیتی باید با او تماس بگیرد، کیست؟

○ استیو چابینسکی: پس از اذمین سیستم ها و یکی از مدیران ارشد بخش امنیت IT، باید با واحد حقوقی تماس گرفته شود. اگر بخواهید یک ساز و کار سایبر درست داشته باشید که مشتری ها و کارکنان را تحت پوشش قرار دهد، باید ابزارهای اعلان دهی و هماهنگی کارآمد را در کنار بیمه مناسب، پیش بینی کنید و در این ساز و کار حتی قانون گذاران و سهام داران را نیز تحت پوشش قرار دهید. من همچنین مواردی را می بینم که مشاوره با عوامل خارج از شرکت به عنوان اولین تماس در نظر گرفته می شود. و نه فقط برای تخصص و تجربه بیشتر آن ها، بلکه برای مسایل حقوقی در طول دعوا. جالب است که به شکل فزاینده ای، پیش از آن که با شرکت های ارزیابی ارزش شرکت (برای ادعای خسارت) ارتباط گرفته شود، با شرکت های حقوقی تماس گرفته می شود. اگر این موضوع باعث تاخیر در گرفتن کمک مناسب نشود، اتفاق خوبی است.

● پس از اولین درخواست کمک، چه تعداد افراد درگیر می شوند؟

○ خُب: این بستگی به فاکتورهای مختلفی دارد. بسته به ارزیابی هایی که چه اتفاقی افتاده یا چه اتفاقی هنوز در حال وقوع است. نکته اصلی ای که به آن می رسیم این است که مقابله با یک حادثه نفوذ عمده، بسیار فراتر از آن است که به متخصصان بگوییم: «فقط این کامپیوترها را درست کنید و کار را زود تمام کنید.» گروه Incident Response Team ممکن است نیاز به برقراری ارتباط با بخش های مختلفی از شرکت را داشته باشند. شکی نیست که با هر بار پیدا شدن یک بدافزار، با مدیرعامل تماس گرفته نمی شود، اما در نهایت، اگر حادثه تحت کنترل نباشد یا ریسک شرکت در حال رشد باشد، گروه مدیریتی باید یک برنامه ای مُدون پیش بینی کرده باشند.

● چه مدارک و شواهدی باید حفظ شود و چگونه؟

○ بیشتر شواهد مورد نیاز به شکل لاگ شبکه ثبت خواهد شد. گروه واکنش به حادثه از تجهیزات اختصاصی برای کُپی، ذخیره و تجزیه و تحلیل اطلاعات مذکور استفاده می کنند. اما اطلاعات مورد بحث، یک فایل کوچک نیست. منظور حجم عظیمی از داده است که از منابع مختلفی حاصل می شود. کامپیوترها همانند معنادان شبکه های اجتماعی هستند. آن ها به طور مداوم می توانند بگویند چه کاری انجام داده اند، چه زمانی و با چه کسی انجام گرفته و حتی چه کسی را برای همراهی رد کرده اند. اما درک همه این موارد و این حجم داده، کار ساده ای نیست. موسسه فناوری و استانداردها (NIST) یک سند هفتاد صفحه ای دارد که فقط به رسیدگی لاگ امنیتی کامپیوتر اختصاص دارد. متأسفانه شرکت های زیادی را دیده ام که این بخش ماجرا را جدی نمی گیرند و حتی از ابتدا لاگی ذخیره نمی کنند. این موضوع مثل آن می ماند که دوربین های امنیتی نصب شده باشند، اما هیچ فیلمی ضبط نکنند.

• آیا کامپیوترها [در طول مقابله با حمله] خاموش می شوند یا روشن می مانند؟

• بیشتر متخصصان واکنش به حادثه پیشنهاد می کنند که کامپیوترها آماده به کار و روشن باشند، مگر این که گل داده نابود شده باشد. دلیل این امر، این است که خاموش کردن کامپیوتر باعث از بین رفتن اطلاعات موجود در حافظه موقت می شود که این اطلاعات می تواند به متخصصان امنیت، برای تحلیل بهتر حمله و جلوگیری از وقوع مجدد آن کمک کند. البته راه بهتر، محدود کردن ارتباط کامپیوترها با شبکه است. بهتر است که بعد از یک حمله امنیتی، دسترسی به اینترنت و ارتباط کامپیوترها با یکدیگر را محدود کنیم.

• پس از کشف حمله، کارکنان را در خانه نگه می دارید یا در محل کار؟

• در محل کار! کسب و کار باید در طول مقابله با حمله ادامه داشته باشد و این یکی از وظایف ما به عنوان متخصصان امنیت است که ادامه جریان کار اطمینان حاصل کنیم. خوشبختانه، حمله های مخربی که گل زیرساخت یک شرکت را هدف قرار می دهند چندان مرسوم نیستند، بنابراین حتی در هنگام تحقیق و بازسازی، بیشتر کارکنان می توانند به کار همیشگی خود ادامه داده و نیازهای احتمالی آن ها نیز برآورده می شود.

• چه زمانی با اف بی آی یا «پلیس سایبری» تماس می گیرید و چه اطلاعاتی را باید در اختیار آن ها قرار گیرد؟

• اف بی آی برای حملات بزرگ انتخاب خوبی است. اما متأسفانه این نهاد یا هر نهاد مجری قانونی دیگر، منابعی برای کمک به موارد کوچک تر ندارند. پیشنهاد من ثبت مورد در سایت پلیس سایبری است تا آن ها ابتدا به بررسی و تجزیه و تحلیل آن مورد بپردازند. مجری قانون کاری به این ندارد که امنیت شبکه شما خوب بوده یا ضعف داشته؛ آن ها به دنبال اطلاعاتی درباره افراد شرور هستند، یعنی در اصل همان لاگ هایی که مورد بحث بوده. پس آن ها کمکی به جبران ضعف های امنیتی را حل مشکلات شبکه شما نمی کنند. اما آن ها می توانند اطلاعات بسیار دقیقی از جرم اتفاق افتاده فراهم کنند که می تواند برای جلوگیری از تکرار حادثه بسیار کارآمد باشد. نکته مهم دیگری که باید در نظر گرفت این است که در مواردی خاص، شرکت در نهایت قصد دارد اطلاعاتی را در اختیار عموم بگذارد، بسیار مهم است که ذکر شود: هر اقدام ممکن که برای کاهش زیان حادثه لازم بوده بلافاصله پس از کشف، انجام شده و همکاری لازم نیز با مجری قانون صورت گرفته است.

• چه اطلاعاتی را باید و چه مواردی را نباید به کارکنان منتقل کرد؟

• بسیار مهم است که در نظر داشته باشید، ارتباط با کل نیروهای سازمان برابر است با

فراهم کردن اطلاعات برای عموم و اگر این اتفاق پیش از مقابله کامل با حمله و ارزیابی دقیق نحوه ی نفوذ انجام شود، می تواند به حمله های بیشتر و زیان های بزرگ تر بیانجامد. بنابراین، من به این موضوع به عنوان یک نکته ضروری نگاه می کنم. اگر موارد لورفته، اطلاعات قابل شناسایی شخص خاصی موجود باشد، بهتر است کارکنان مربوطه مطلع شوند، اما ممکن است ضروری باشد که این مورد هم به تأخیر بیفتد. اگر رسانه ها داستان را دنبال می کنند و کارکنان می خواهند بدانند که حمله چگونه آن ها و کارشان را تحت تأثیر قرار داده و مدیران نیز باید اطمینان خاطر قانع کننده ای برای آن ها فراهم کنند. اما اگر تنها مشکل مشهود، مشکلات ارتباط در شبکه بوده باشد، به گمان من هر چه کمتر گفته شود، بهتر خواهد بود.

• چه اطلاعاتی را باید و چه مواردی را نباید به سهام داران منتقل کرد؟

• SEC نکات زیادی را در این باره در سایت خود منتشر کرده است. در اصل، طبق گفته SEC، اگر موضوع برای سهام داران یک مساله اساسی باشد، باید برای آن ها فاش شود. البته در نحوه فراهم کردن اطلاعات توسط شرکت، انعطاف زیادی وجود دارد. مثلاً نیازی نیست که یک شرکت نقاط آسیب پذیر خود را بیان کند و این اطلاعات در اختیار هکرها در نقاط مختلف دنیا قرار بگیرد. همه این ها مرا به نکته ای می رساند که پیش تر ذکر کردم و آن این است: آیا ابتدا با وکیل یا مشاور حقوقی خود تماس گرفته اید؟ به نظرم این پاسخ بهتری است.

• مهم ترین چیزی که پس از وقوع یک نفوذ باید برای آن آماده بود، چیست؟

• آماده بودن برای برخورد با حوادث سایبری به عنوان یک مشکل چندرشته ای، نه فقط به عنوان یک مشکل تکنیکی. پیش از وقوع حادثه، باید فهرستی از کارکنان در بخش های مختلف موجود باشد که می دانند ممکن است هدف ارتباط قرار گیرند و بسته به نوع حادثه از این فهرست استفاده شود و در هر زمان از شبانه روز، با افراد مورد نظر تماس گرفته شود.

با توجه به این که ممکن است امکان استفاده از کامپیوترها محدود شود، باید دو نسخه چاپی از فهرست مذکور و دستورالعمل واکنش به حادثه تهیه و در شرکت و خانه نگهداری شود. علاوه بر این، مدیران شرکت، پیش از وقوع هر حادثه ای باید با یک شرکت حقوقی با تخصص ویژه در نفوذ، در ارتباط باشد و یک قرارداد با شرکت های ارزیابی شبکه داشته باشند که در صورت وقوع حادثه، به سرعت درگیر شوند، البته پرداخت هزینه در این قرارداد، فقط در هنگام وقوع حادثه لازم خواهد بود. در نهایت، شکی نیست که آمادگی درست پیش از حادثه، تفاوت میان یک رویداد قابل مدیریت و مارپیچی از بحران را تعیین می کند.

دوره های حرفه ای امنیت اطلاعات

با کادر کارشناسان و اساتید متخصص

ویژه سازمان ها و شرکت ها

CyberTech
The Leader in IT & Training



آشنایی با دوره‌های امنیت، بخش اول



Systems Security
Certified Practitioner

دوره (SSCP) (Systems Security Certified Practitioner)

امروزه امنیت اطلاعات بسیار عمیق و گستره شده و دیگر امنیت شبکه تعبیر نمی‌شود. بدین دلیل برای ورود به این عرصه باید ابتدا بر پایه‌های این شاخه از فناوری مسلط شد تا بتوان برای مراحل بعد و انتخاب مسیر راه، اقدام کرد. دوره SSCP به عنوان سنگ بنای امنیت اطلاعات می‌باشد که با توجه به سرفصل آن، هر شخصی که به دنبال ورود به حرفه امنیت اطلاعات است باید آن را بگذراند. این دوره برای علاقمندان امنیت اطلاعات که در ابتدای راه هستند می‌تواند شروع خوبی باشد و افق‌های حرکت در این مسیر را برایشان روشن سازد. این دوره دربردارنده مفاهیمی است که مبانی امنیت اطلاعات را شامل شده و به‌زبانی نسبتاً روان و ساده این مفاهیم را آرایه می‌کند. به تجربه ثابت شده است که گذراندن این دوره به عنوان دوره پایه‌ای برای شروع در حوزه امنیت اطلاعات تضمین کننده حرکت مستقیم و درست به سمت هدف است چراکه در این دوره علاوه بر استحکام پایه‌های دانشی فرد در امنیت اطلاعات، توانایی انتخاب را نیز برای دانشجو فراهم می‌آورد که با توجه به نیاز و علاقمندی می‌تواند مسیر راه خود را در حوزه امنیت اطلاعات برگزیند. گذراندن یکی از دوره‌های MCITP (یا هم‌تراز لینوکس آن) و یا CCNA قبل از این دوره توصیه می‌شود. اما گذراندن Network+ اجباری است. تدریس این دوره در سایبرتک مطابق با آخرین سرفصل ISC2 که آرایه دهنده مدرک آن است توسط مدرسان متخصص امنیت انجام می‌پذیرد.

سرفصل دوره

- Access Controls
- Security Operations and Administration
- Risk Identification, Monitoring, and Analysis
- Incident Response and Recovery
- Cryptography
- Network and Communications Security
- Systems and Application Security



Certified Information
Systems Security Professional

دوره (CISSP) (Certified Information Systems Security Professional)

این دوره سرگُل یا به قولی دکترای امنیت اطلاعات است و اخذ آن از مزیت بالایی برخوردار می‌باشد. این دوره که توسط جامعه متخصصان امنیت اطلاعات ISC2 ارائه می‌شود، دریافت مدرک آن که بسیاری از جنبه‌های امنیت را در خود جای داده، مراحل سختی را در پی دارد. نظر ISC2 در آن بوده است که کلیه جنبه‌های امنیت را در این مدرک بین‌المللی گردهم بیاورد، به نحوی که در حوزه‌های مربوطه شخص یک صاحب نظر شود. در این دوره دانش‌پذیر با امنیت در انواع لایه‌ها از لایه فیزیکی تا نرم‌افزار و شبکه آشنا خواهد شد و خواهد توانست به عنوان یک کارشناس ارشد و متخصص خبره انواع تهدیدهای مرتبط بر سیستم‌های اطلاعاتی را کشف و با آنالیزهای مختلف چون آنالیز ریسک مدیریت تهدیدات را داشته باشد و یک طرحی برای امن‌سازی سازمان ارائه داده و به اجرا بگذارد. این متخصص می‌تواند بازرسی امنیت اطلاعات سازمان‌ها و پیگرد جرایم رایانه‌ای را به انجام برساند و برای مدل امن کسب و کار سازمان و جلوگیری از شکست سازمان در فضای بیزنس ارائه طریق کند. این دوره برای متخصصان ارشد امنیت اطلاعات و مدیران مربوطه پیشنهاد می‌شود. تدریس این دوره در سایبرتک مطابق با آخرین سرفصل ISC2 که ارائه دهنده مدرک آن است توسط مدرسان متخصص امنیت انجام می‌پذیرد.

• Security and Risk Management

• Asset Security

• Security Engineering

• Communications and Network Security

• Identity and Access Management

• Security Assessment and Testing

• Security Operations

• Software Development Security

در آموزشگاه مهندسی سایبرتک، مجموعه دوره‌های فوق در قالب یک پکیج آماده شده تا بتوان به طور یک‌نواخت و کامل، آموزش را برای دانشجویان فراهم آورد که در نهایت پس از پایان دوره‌ها یک متخصص واقعی امنیت اطلاعات داشته باشیم. چرا که در این آموزشگاه اصل بر کیفیت آموزش بوده است. در برآوردی که در جامعه IT ایران انجام شده، دیده می‌شود که آموزش‌های دوره‌های فوق به تنهایی در صورتی که فرد پیش‌نیازها و دوره‌های بعدی لازم را نداشته باشد مکفی نخواهد بود و در بازار کار موقعیت مناسبی را نخواهد داشت. همچنین پس از بررسی، کارشناسان و اساتید سایبرتک به این نتیجه رسیدند که ارائه این پکیج می‌تواند راه‌گشای مشکل امروز در جامعه IT باشد. شایان ذکر است در صورتی که دانشجوی پیش‌نیازهای لازم را رعایت کرده باشد، می‌تواند در دوره‌های مجزای سایبرتک که برای تک تک عناوین فوق تدارک دیده شده است شرکت و از آن‌ها بهره‌برد.



دوره (CEH) (Certified Ethical Hacker)

با توجه به این‌که هکرها و افراد دارای نیت‌های پلید در دنیای دیجیتال همانند قدیم که دزدی و راهزنی وجود داشته، پا به این عرصه گذاشته‌اند و روزبه‌روز بر تعداد و تنوع آنان افزوده شده و همچنین در سالیان پیش تدریس هک در کشورهای پیشرفته ممنوعیت داشته و با توجه به رشد هک و جوامع هکری و زیرزمینی، عقلای جامعه اطلاعاتی و امنیتی بر آن شدند با توسعه آموزش‌های امنیت و هک به افراد مورد اعتماد، عرصه را بر افراد بدخواه و هکر فراهم کنند. از آن‌جا بود که هک‌های کلاه سفید پا به عرصه وجود گذاشتند تا وظیفه حفاظت از سیستم‌ها در مقابل هک‌های کلاه سیاه را برعهده گیرند. دوره‌هایی چون CEH علاوه بر مرور مبانی امنیت اطلاعات، تئوری‌های نفوذ و هک در سیستم‌های اطلاعاتی را به دانشجو می‌آموزند و سازمان‌ها نیز با در اختیار داشتن این نیروها می‌توانند فکر هکرها را خوانده و برای مقابله با آن‌ها آماده باشند. تدریس این دوره در سایبرتک مطابق با آخرین سرفصل EC Council که ارائه دهنده این مدرک است، توسط مدرسان متخصص امنیت انجام می‌پذیرد.

سرفصل مطالب این دوره

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- System Hacking
- Trojans and Backdoors
- Viruses and Worms
- Sniffers
- Social Engineering
- Denial of Service
- Session Hijacking
- Hacking Webservers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- Evading IDS, Firewalls and Honeypots
- Buffer Overflows
- Cryptography
- Penetration Testing

Network +

(پیش نیاز سیسکو و مایکروسافت)

کد دوره	نام درس	نام استاد	تاریخ شروع	ساعت و روز تشکیل کلاس	پیش نیاز	مدت	قیمت / تومان
۱۱۹-	Network- (پیش نیاز دوره های آموزشی مهندسی شبکه)	مهندس شکر الهی	۱۳۹۴/۰۶/۲۸	روزی ۲ ساعت (۱۳:۰۰ تا ۱۵:۰۰)	آشنایی با ویندوز	۲۹ ساعت	۳۳۰,۰۰۰
۱۲۱-	Network- کتب ۴ دوره	مهندس جعفری	۱۳۹۴/۰۶/۲۱	سه شنبه تا جمعه (۸:۰۰ تا ۱۵:۰۰)	آشنایی با ویندوز	۲۲ ساعت	۳۳۰,۰۰۰
۱۲۳-	Network- (پیش نیاز دوره های آموزشی مهندسی شبکه)	مهندس غفاریان	۱۳۹۴/۰۷/۱۲	یکشنبه و سه شنبه (۱۷:۰۰ تا ۲۰:۰۰)	آشنایی با ویندوز	۲۹ ساعت	۳۳۰,۰۰۰
۱۲۴-	Network- (پیش نیاز دوره های آموزشی مهندسی شبکه)	مهندس آژیده	۱۳۹۴/۰۷/۲۵	روزی ۲ ساعت (۱۷:۰۰ تا ۱۹:۰۰)	آشنایی با ویندوز	۲۹ ساعت	۳۳۰,۰۰۰

MCSE 2012 Courses

۲۰۸-	Administering windows server 2012	مهندس آجورلو	۱۳۹۴/۰۶/۲۱	شنبه تا پنجشنبه (۸:۰۰ تا ۱۷:۰۰)	Network -	۵۴ ساعت	۵۹۰,۰۰۰
۲۰۹-	Configuring Advanced Windows Server 2012	مهندس آجورلو	۱۳۹۴/۰۷/۱۴	شنبه تا پنجشنبه (۸:۰۰ تا ۱۷:۰۰)	Configuring win srv 2012	۵۴ ساعت	۵۹۰,۰۰۰
۲۱۲-	MCSE 2012 Server Infrastructure Pack & win8	مهندس شکر الهی	۱۳۹۴/۰۷/۱۶	پنجشنبه (۸:۰۰ تا ۱۷:۰۰)	Network -	۲۲ ساعت	۲,۴۵۰,۰۰۰
۲۱۹-	MCSE 2012 Server Infrastructure Pack & win8	مهندس برومند	۱۳۹۴/۰۹/۰۷	روزی ۲ ساعت (۱۷:۰۰ تا ۲۰:۰۰)	Network -	۲۴۰ ساعت	۲,۴۵۰,۰۰۰

Other Windows Server Courses

۲۱۳-	کارگاه ۲ دوره Exchange Server 2013	مهندس محبی	۱۳۹۴/۰۷/۱۱	شنبه و یکشنبه (۸:۰۰ تا ۱۷:۰۰)	MCSE or MCITP	۱۸ ساعت	۳۳۰,۰۰۰
۲۱۴-	کارگاه ۲ دوره TMG 2010	مهندس محبی	۱۳۹۴/۰۷/۱۶	پنجشنبه و جمعه (۸:۰۰ تا ۱۷:۰۰)	MCSE or MCITP	۱۸ ساعت	۳۳۰,۰۰۰
۲۱۸-	Microsoft Security Pack به علاوه ۱۵ ساعت از ای UTM های کاربردی	مهندس برومند	۱۳۹۴/۰۱/۱۰	پنجشنبه و جمعه (۱۴:۳۰ تا ۱۷:۰۰)	MCSE or MCITP	۹۵ ساعت	۱,۲۳۰,۰۰۰
۲۰۴-	Exchange Server 2013	مهندس محبی	۱۳۹۴/۰۹/۲۶	پنجشنبه (۸:۰۰ تا ۱۷:۰۰)	MCSE or MCITP	۷۰ ساعت	۸۵۰,۰۰۰
۲۰۵-	Hyper V	مهندس آجورلو	۱۳۹۴/۱۲/۱۳	پنجشنبه (۱۷:۰۰ تا ۲۰:۰۰)	MCSE or MCITP	۴۰ ساعت	۶۰۰,۰۰۰

دوره های آموزشی ICDL

۷۰۱-	ICDL مقدماتی	مهندس تهرانی	۱۳۹۴/۰۶/۲۹	یکشنبه و سه شنبه (۱۷:۰۰ تا ۲۰:۰۰)	تدارک	۹۵ ساعت	۴۶۰,۰۰۰
۷۰۴-	ICDL شامل ۷ مهارت (با ارائه مدرک بین المللی)	مهندس دادگر	۱۳۹۴/۰۷/۱۶	پنجشنبه (۸:۰۰ تا ۱۷:۰۰)	تدارک	۹۵ ساعت	۴۶۰,۰۰۰
۷۰۳-	Exoel مقدماتی و پیشرفته	مهندس تهرانی	۱۳۹۴/۰۷/۲۳	پنجشنبه و جمعه (۸:۰۰ تا ۱۷:۰۰)	تدارک	۴۰ ساعت	۲۲۰,۰۰۰
۷۰۵-	ICDL پیشرفته شامل (Word - Excel - Access - PowerPoint)	مهندس تهرانی	۱۳۹۴/۰۱/۱۳	یکشنبه و سه شنبه (۱۷:۰۰ تا ۲۰:۰۰)	ICDL مقدماتی	۶۰ ساعت	۳۸۰,۰۰۰

دوره های آموزشی برنامه نویسی

۵۱۳-	HTML5 - CSS - JavaScript - ASP.NET) برنامه نویسی وب	مهندس حاتمیان	۱۳۹۴/۰۷/۰۹	پنجشنبه (۸:۰۰ تا ۱۷:۰۰)	تدارک	۵۰ ساعت	۶۵۰,۰۰۰
۵۱۴-	ASP.NET مقدماتی	مهندس گاوینی	۱۳۹۴/۰۸/۲۴	یکشنبه و سه شنبه (۱۷:۰۰ تا ۲۰:۰۰)	برنامه نویسی وب	۴۰ ساعت	۴۲۰,۰۰۰
۵۱۷-	SQL Pack	مهندس برومند	۱۳۹۴/۰۹/۰۵	پنجشنبه و جمعه (۹:۰۰ تا ۱۷:۰۰)	آشنایی با برنامه نویسی	۱۰۰ ساعت	۱,۱۰۰,۰۰۰
۵۱۶-	SQL Admin	مهندس گاوینی	۱۳۹۴/۰۱/۱۷	پنجشنبه (۸:۰۰ تا ۱۷:۰۰)	SQL Design	۶۰ ساعت	۶۵۰,۰۰۰
۵۱۵-	ASP.NET پیشرفته	مهندس گاوینی	۱۳۹۴/۰۱/۲۰	یکشنبه و سه شنبه (۱۷:۰۰ تا ۲۰:۰۰)	ASP.NET مقدماتی	۴۰ ساعت	۴۵۰,۰۰۰

دوره های آموزشی برنامه نویسی موبایل

۵۱۲-	Java Fundamental	مهندس خدایرست	۱۳۹۴/۰۶/۲۷	جمعه (۹:۰۰ تا ۱۷:۰۰)	تدارک	۳۳ ساعت	۳۸۰,۰۰۰
۵۰۹-	Java دوره مقدماتی	مهندس خدایرست	۱۳۹۴/۰۶/۲۹	یکشنبه (۱۷:۰۰ تا ۲۰:۰۰)	Java Fundamental	۳۰ ساعت	۳۸۰,۰۰۰
۵۰۷-	برنامه نویسی اندروید پیشرفته (Android)	مهندس خدایرست	۱۳۹۴/۰۶/۲۱	سه شنبه (۱۷:۰۰ تا ۲۰:۰۰)	برنامه نویسی اندروید مقدماتی (Android)	۳۰ ساعت	۳۹۲,۰۰۰
۵۰۸-	برنامه نویسی سیستو عمل IOS	مهندس خدایرست	۱۳۹۴/۰۷/۰۳	جمعه (۱۴:۰۰ تا ۱۷:۰۰)	تدارک	۳۶ ساعت	۵۵۰,۰۰۰
۵۱۱-	Java Fundamental	مهندس خدایرست	۱۳۹۴/۰۸/۲۴	یکشنبه (۱۷:۰۰ تا ۲۰:۰۰)	تدارک	۳۳ ساعت	۳۸۰,۰۰۰
۵۱۰-	برنامه نویسی اندروید مقدماتی (Android)	مهندس خدایرست	۱۳۹۴/۰۹/۱۷	سه شنبه (۱۷:۰۰ تا ۲۰:۰۰)	Java Fundamental	۳۰ ساعت	۵۷۶,۰۰۰

دوره های آموزشی مهندسی سیسکو

۲۲۰-	CCNA ۲۰۰-۱۲۰	مهندس محمدیان	۱۳۹۴/۰۶/۱۷	یکشنبه و سه شنبه (۱۷:۰۰ تا ۲۰:۰۰)	Network -	۶۰ ساعت	۸۵۰,۰۰۰
۲۰۶-	CCNA ۲۰۰-۱۲۰	مهندس نصرتی	۱۳۹۴/۰۶/۱۷	یکشنبه و سه شنبه (۱۷:۰۰ تا ۲۰:۰۰)	Network -	۶۰ ساعت	۸۵۰,۰۰۰
۲۲۲-	CCNA ۲۰۰-۱۲۰	مهندس آژیده	۱۳۹۴/۰۶/۲۴	پنجشنبه و جمعه (۱۴:۰۰ تا ۱۷:۰۰)	Network -	۶۰ ساعت	۸۵۰,۰۰۰
۲۲۳-	CCNA ۲۰۰-۱۲۰	مهندس اصلاحی	۱۳۹۴/۰۷/۱۶	پنجشنبه و جمعه (۸:۰۰ تا ۱۷:۰۰)	Network -	۶۰ ساعت	۸۵۰,۰۰۰
۴۰۵-	کتاب پنج دوره CCNP (Switch)	مهندس اسماعیل پور	۱۳۹۴/۰۶/۲۸	شنبه تا چهارشنبه (۸:۰۰ تا ۱۷:۰۰)	CCNA	۴۵ ساعت	۹۵۰,۰۰۰
۴۰۳-	CCNP (Switch)	دکتر نظامی	۱۳۹۴/۰۶/۲۹	یکشنبه و سه شنبه (۱۷:۰۰ تا ۲۰:۰۰)	CCNA	۵۰ ساعت	۹۵۰,۰۰۰
۴۰۱-	CCNP (Route)	مهندس آژیده	۱۳۹۴/۰۶/۲۹	یکشنبه و سه شنبه (۱۷:۰۰ تا ۲۰:۰۰)	CCNA	۵۰ ساعت	۹۵۰,۰۰۰

Other Cisco Courses

۴۰۷-	Routing & Switching pack (CCNA + CCNP Route&Switch) (۱۱۰ ساعت آموزش + ۲۰ ساعت کارگاه و اجرای سناریوهای واقعی)	مهندس خرمین بیز	۱۳۹۴/۰۶/۲۱	روزی ۲ ساعت (۱۷:۰۰ تا ۲۰:۰۰)	Network -	۱۳۰ ساعت	۲,۳۳۰,۰۰۰
۳۱۳-	CCNA Voice	مهندس خرمین بیز	۱۳۹۴/۰۷/۰۸	چهارشنبه (۱۶:۰۰ تا ۱۹:۰۰)	CCNA	۴۵ ساعت	۸۵۰,۰۰۰
۴۰۶-	Cisco Advanced Technologies (VPN technologies , VRF , Advanced BGP, Advanced BGP, Routing Protocol Updates , Embedded event manager)	مهندس اصلاحی	۱۳۹۴/۰۷/۲۵	روزی ۲ ساعت (۱۷:۰۰ تا ۲۰:۰۰)	CCNP (R & S)	۶۰ ساعت	۱,۰۵۰,۰۰۰
۲۱۴-	CCNA Datacenter	مهندس اصلاحی	۱۳۹۴/۰۹/۲۷	جمعه (۹:۰۰ تا ۱۷:۰۰)	CCNA	۴۵ ساعت	۹۵۰,۰۰۰

دوره های آموزشی مجازی سازی

۶۰۸-	Horizon View V6.1 ICM	مهندس اسماعیل پور	۱۳۹۴/۰۶/۲۱	روزی ۲ ساعت (۱۷:۰۰ تا ۲۰:۰۰)	VMware - v Sphere6:ICM-vcp6	۴۰ ساعت	۱,۱۲۰,۰۰۰
۸۰۵-	What's New in VMware vSphere 6	مهندس توکلی	۱۳۹۴/۰۶/۲۶	پنجشنبه و جمعه (۸:۰۰ تا ۱۷:۰۰)	VMware - v Sphere5 or v Sphere4	۱۸ ساعت	۵۷۰,۰۰۰
۶۱۰-	vSphere Optimize & Scale V6	مهندس اسماعیل پور	۱۳۹۴/۰۷/۰۹	پنجشنبه (۱۸:۰۰ تا ۱۹:۰۰)	VMware - v Sphere6:ICM-vcp6	۴۴ ساعت	۱,۲۳۰,۰۰۰
۶۰۹-	VMware - v Sphere6:ICM-vcp6	مهندس توکلی	۱۳۹۴/۰۷/۱۹	پنجشنبه و جمعه (۸:۰۰ تا ۱۷:۰۰)	آشنایی با شبکه	۵۰ ساعت	۱,۱۵۰,۰۰۰
۸۰۶-	Horizon View V6.1 ICM	مهندس اسماعیل پور	۱۳۹۴/۰۷/۲۱	سه شنبه تا جمعه (۸:۰۰ تا ۱۷:۰۰)	VMware - v Sphere6:ICM-vcp6	۳۶ ساعت	۱,۱۲۰,۰۰۰
۶۱۱-	Citrix XenApp V6 - Administration	دکتر کاظمی	۱۳۹۴/۰۳/۲۰	چهارشنبه تا جمعه (۹:۰۰ تا ۱۷:۰۰)	win server 2008	۴۴ ساعت	۹۵۰,۰۰۰

دوره های آموزشی امنیت شبکه و متن باز

۶۰۲-	Linux LPIC 1 (101 & 102)	مهندس نصرتی	۱۳۹۴/۰۷/۰۵	یکشنبه و سه شنبه (۱۷:۰۰ تا ۲۰:۰۰)	Network-	۶۰ ساعت	۹۵۰,۰۰۰
۶۰۶-	Security+	مهندس منصوری	۱۳۹۴/۰۷/۱۶	پنجشنبه (۱۶:۳۰ تا ۱۹:۳۰)	تدارک	۴۰ ساعت	۶۳۰,۰۰۰
۶۰۷-	CISSP	مهندس نوروزی	۱۳۹۴/۰۷/۱۷	جمعه (۹:۰۰ تا ۱۷:۰۰)	تدارک	۴۰ ساعت	۹۱۰,۰۰۰
۶۱۱-	Security Pack (SSCP, CEH, CISSP)	مهندس نوروزی	۱۳۹۴/۰۷/۲۰	پنجشنبه و جمعه (۱۴:۰۰ تا ۱۷:۰۰)	Network-	۱۲۰ ساعت	۲,۲۰۰,۰۰۰
۶۰۵-	(۱۰۰ ساعت آموزش + ۲۰ ساعت کارگاه و اجرای سناریوهای واقعی) CEH-Certified Ethical Hacker	مهندس منصوری	۱۳۹۴/۰۸/۰۷	پنجشنبه (۱۸:۳۰ تا ۲۱:۳۰)	CCNA&MCSE ۲۰۱۲ or Security-	۴۵ ساعت	۸۹۰,۰۰۰

استاندارد ها و دوره های حرفه ای شبکه

۸۰۱-	کارگاه سه دوره ITIL Foundation	مهندس ارغند	۱۳۹۴/۰۷/۰۸	چهارشنبه تا جمعه (۹:۰۰ تا ۱۷:۰۰)	آشنایی با IT	۲۴ ساعت	۷۵۰,۰۰۰
۸۰۵-	سمینار یک دوره آشنایی با ISMS	مهندس ارغند	۱۳۹۴/۰۷/۱۹	یکشنبه (۱۷:۰۰ تا ۱۹:۰۰)	تدارک	۸ ساعت	۲۴۰,۰۰۰
۸۰۸-	SIEM and Log Management system	مهندس آژیده	۱۳۹۴/۰۸/۰۲	پنجشنبه و جمعه (۹:۰۰ تا ۱۷:۰۰)	Network-	۳۰ ساعت	۸۵۰,۰۰۰
۸۰۷-	کارگاه سه دوره ISMS	مهندس ارغند	۱۳۹۴/۰۸/۲۷	چهارشنبه تا جمعه (۹:۰۰ تا ۱۷:۰۰)	تدارک	۲۴ ساعت	۷۵۰,۰۰۰

دوره‌های تخصصی مجازی سازی

CITRIX

vmware



۸۶ ۷۶ ۵۰۰۰



+ هر ماه یک سمینار رایگان

برای آشنایی با فناوری و دوره‌های مجازی سازی

سیسکو سبک ساینر تک

برای نخستین بار؛ به صورت اختصاصی

Routing & Switching pack

(CCNA & CCNP Route & Switch)

(۱۱۰ ساعت آموزش + ۲۰ ساعت کارگاه و اجرای سناریوهای واقعی)



CISCO™

CyberTech
The Leader in IT & Training

۸۶ ۷۶ ۵۰۰۰

آموزشگاه
مهندسی
ساینر تک
برگرفته دوره های تخصصی IT
سیسکو و مایکروسافت