[제25호-2013.11월]

보안인닷컴 e-매거진 [보안人]

차 례

디자인: BK.Kim 편집: 전주현 발행: 전주현

http://www.boanin.com

발행인의 변

안녕하세요. 보안인닷컴 운영자 전주현입니다.

무더운 여름을 지나 깊어가는 가을의 끝자락에서 겨울 초입에 서 있습니다. 개인적으로 정보보안 기사 실기 교재 출간과 생업에 매달리느라 보안인닷컴 E-매거진 발행이 조금 늦게 나오게 되었습니다. 언제나 기다려 주신 분들에게 송구한 마음입니다. 그 기다리는 마음을 담아 보안인닷컴 E-매거진 **[보안人]** 25호가 발행되었습니다. 이번 25호에는 한국인터넷진흥원 장상수 팀장님께서 바쁘신 가운데 기꺼이 인터뷰에 응해 주셔서 좋은 말씀을 해 주셨고, 또한 고재호 스텝께서 옥고를 주셔서 더 값지게 발행 할 수 있었습니다. 참여 해 주시는 분들과 발행될때마다 구독해 주시는 여러분들에게 깊은 감사의 말씀을 드립니다.

한편, 지난 10월달에는 국가기술 정보보안 기사, 산업기사 국가 기술 자격증 제2회 필기시험이 전국에서 치러졌으며 많은 수험생들이 도전하였습니다. 이제 12월에는 올해 마지막 실기시험이 진행됩니다.

무료로 배포되는 보안인닷컴 E-매거진 **[보안人]** 은 국내외에서 잘 알려지지 않는 보안인, 보안교육센터, 보안기업, 보안제품등 다양한 콘텐츠를 가지고 찾아 뵐수 있도록 하겠습니다. 늘 읽어주시는 분들이 있어 **[보안人]** 이 빛나는 것이 아닌가 생각해 봅니다.

한번쯤 자신의 보안에 대한 이야기를 풀어주시고자 하시는 분들은 e-매거진 **[보안人]**의 문은 언제든지 활짝 열려 있으니까 참여 하시고 원고접수나 문의는 boanin@naver.com 이나 magazine@boanin.com 으로 주시면 되겠습니다.,

보안 관련하여 다양한 사이트에서 정보를 접하실 수 있습니다. BoAN人

보안/자격증, 정보보호자료공유 커뮤니티 보안인닷컴 : http://www.boanin.com
전주현 개인정보보호길라잡이 http://www.privacy.pe.kr http://www.privacyguide.co.kr
스마트폰으로 실시간 보안소식 접하기 http://www.facebook.com/jeonjuhyun

보안인닷컴 운영자 엔시스올림

[보안人 토막공지] 보안인닷컴 E-매거진은 여러분들의 많은 참여로 만들어 가고 있습니다. 진솔한 이야기, 보안에 대한 이야기, 자격증 취득후기, 면접등 다양하게 보내 주시면 더 많은 풍성한 읽을꺼리를 제공해 드릴 수 있습니다. 많은 참여를 바라겠습니다. 보내실 곳은 boanin@naver.com 입니다. -보안인닷컴 편집자 주

[보안人 인터뷰]

ISMS는 정보보호의 시작이자 끝이며 예술이다

(한국인터넷진흥원 장상수 팀장)

안녕하세요. 장상수 팀장님 보안인닷컴 운영자 전주현입니다. 우선 이렇게 인터뷰에 응해주셔서 진심으로 감사드립니다. 간단한 소속과 자기 소개 좀 부탁드립니다.

Q 간단한 소속과 자기 소개 좀 부탁드립니다.

A 먼저 '보안인닷컴' 회원 여러분에게 지면을 통해 인사드리게 되어 기쁘게 생각합니다. 저는 1989년부터 대항항공에서 네트워크 설계 및 기획 업무와 보안 담당자로 일해 오다 2000년도에 KISA에 합류하여 지금까지 정보보호 1세대로 24년간 보안관리 분야에 대해 연구·개발에 전념하여 왔으며, 국내 최초 정보보호 관리체계 프레임위크 개발하고 정립하였으며, 국내의 대부분 보안관리 제도를 직접 개발하고 운영하는 등 보안관리 분야의 최고의 전문가로 선구자 역할을 해오고 있다고 자부하고 있습니다. 현재도 보안관리 각종 제도를 연구·개발 및 직접 운영을 담당하고 있습니다.

Q 현재 한국인터넷진흥원(KISA)에 근무하시는데요. 주로 어떤 업무를 하고, 보안에 대하여 어려움을 겪는 분들에게 어떤 도움을 주고 계시는지요?

A 제가 KISA에 합류하여 13년동안 정보보호관리 분야에 산증인으로 일하게 된 것은 "정보보호 관리체계(ISMS) 인증 제도, 지식정보보안 컨설팅전문업체 지정, 집적정보통신시설 이행점검, 정보보호 안전진단 제도, 개인정보보호 관리체계(PIMS) 인증 제도, 전자정부 정보보호 관리체계(G-ISMS) 인증 제도, 중소기업 취약점 점검 서비스, 전자정부 대민서비스 정보보호 수준진단, 정보보호 관리체계 인증 의무화, 정보보호 관리 등급제 등" 10개 이상의 보안관리 제도를 직접 연구하고 제도화하여 운영하고 있으며 이러한 다양한 보안관리 정책을 제도화하여 실효성을 증진하는데 노력해 왔으며 국내 기관/기업의 정보보호 수준제고에 많은 기여를 해왔다고 생각하고 있습니다.

최근 “정보보호관리체계 구축 및 활용”이라는 책을 출간하여 화제가 되고 있는데요. 개인적으로는 누군가 한번 정리해서 책으로 나왔으면 하는 바램을 가지고 있었는데 아주 반가웠습니다.. 책을 출간하게 된 배경과 또한 책을 통하여 말하고 싶은 메시지는 무엇이며 책을 어떻게 활용하면 좋을까요?

정보보호를 디자인하라"라는 책을 집필하게 된 배경은 KISA에 근무하면서 13년동안 보안관리 정책 분야에 선구자로서 일해 오면서 뭔가 의미 있는 일을 해보고자 생각했고 오랫 동안 참여해 왔던 정보보호관리 제도를 누군가는 정리를 해야 한다는 요구와 제 스스로 사명감과 책임이 발동하여 작업을 하게 되었습니다.

제가 몸담아 왔던 제도가 성공적으로 정착했으면 하는 바램과 그동안 제도에 대해 이해 당사자들에게 정확하게 전달하지 못했던 내용을 전달할 방법을 찾다가 시기가 적절하다 싶어 책으로 발간하게 되었습니다. 아무쪼록 정보보호관리 제도의 성공과 기업들의 정보보호 수준 제고에 기여했으면 하는 바람으로 집필하게 되었습니다.

현재까지 제도를 연구 개발하고 직접 현장에서 정책을 집행한 사람으로서는 대학에서는 정보보호 관리체계에 대해 잘못된 방향의 교육이 이루어지는 것이 안타까웠으며, 또한 이를 적용해야 하는 국내 기관/기업 담당자는 무엇을 어떻게 해야 할지 당황하고 정보보호 컨설팅 업체 입장에서는 업체의 자율적인 해석으로 시장에서 왜곡되어 적용되는 현실을 보면서 제도를 개발한 당사자 입장에서 정확한 내용을 전달해야 한다는 책임감과 사명감을 가지고 집필하게 되었습니다.

이 책을 통해 전달하고자 했던 내용은 최근 3.20, 6.25 등 사이버테러 등 침해사고에 기관/기업에서 그 동안 일시적이고 단편적인 대응에서 이제는 정보보호 분야에서도 체계적이고 전략적인 디자인적 사고의 필요성이 대두되고 있습니다. 즉 정보보호에도 분석과 직관을 모두 활용한 사람들이 공유하는 문제를 해결하는 프로세스인 디자인 사고가 필요하다는 것입니다. 이 책에서는 이러한 정보보호에 전략적인 디자인적 사고를 강조하면서 정보보호도 새로운 비즈니스로 디자인하려는 노력과 기관/기업에 정보보호 전략 수립 및 프로그램 개발의 중요성과 방법론을 제시하고자 하였습니다.

또한, 보안관리 정책이나 ISMS에 대해 경험과 노하우를 체계적으로 정리하고 학문적 관점에서 분석한 입문서가 없어 많은 어려움을 겪는 현실에 안타까움을 금할 수 없어 실무 경험을 바탕으로 보안관리 정책, ISMS 지침서를 꼭 정리하기를 간절히 바랬습니다. 그러한 희망을 현실화하게 되어 이제 마음의 부채를 조금이나마 던 기분입니다.

"정보보호를 디자인하라" 책 활용은 CEO, 경영진, CIO/CISO, 정보보호 담당자, 정보보호 컨설턴트, 인증심사원, 정보를 다루는 모든 직원, 정책담당자, 정보보호 초심자 등 모든

분들이 우리나라 보안관리 정책을 이해하는 입문서로서 또는 유용한 지침서로서의 활용을 기대하고 있습니다.

팀장님께서는 국내 정보보호관리체계에 대한 남다른 관심과 그 기반을 다져 오신 분이라 알고 있습니다..IT경력과 보안쪽 업무를 많이 하다보면 결국 기업이든, 기관이든 정보보호에 대한 체계적인 관리가 필요한데요...현재 정보보호 관리체계에 대한 현황 및 필요성에 대하여 언급해 주신다면?

말씀하신 것처럼 저는 국내에서 아무도 가지 않았던 보안관리 분야에서 13년 동안 수많은 보안관리 제도를 연구·개발하고 현장에서 직접 수행하면서 역사의 현장에 있었던 저에게는 무한한 영광의 순간이 아닐 수 없었습니다. 국내 보안관리 선구자로서 사명감 하나로 진심을 다해 일할 수 있었던 것은 일에 대한 열정, 스스로에 대한 믿음이 아니었나 생각합니다.

정보보호 선진국의 자격 요건 중에 가장 중요한 것이 훌륭한 정보보호 제도, 즉 시스템이 얼마나 잘 마련이 되어있냐 라는 것입니다. 물론 이런 좋은 제도가 갖춰져 있다고 해도 현장에서 적용하고 운영하는데 형식적이거나 실효성이 없다면 유명무실 하고 말 것이다. 국내는 세계적으로 높은 수준의 보안관리 제도를 도입 운영하고 있으나, 보안사고는 더욱 증가되고 있습니다. 이는 무엇을 의미하는 것인가요? 보안관리 제도가 문제가 있거나 이를 구축하고 지속적으로 운영·관리하는 조직에 문제일 것입니다.

결국 기관/기업의 정보보호는 아무리 훌륭한 제도나 시스템으로 동기부여나 방법을 알려줄 뿐이며 최종 결정은 해당 기관/기업의 몫이 아닌가 합니다. 정보보호 관리체계를 구축하고 잘 운영한다 해도 조직에서 이를 적용하는데 이론이 아니라 현실속의 실천(행동)이 될 때 힘을 받을 수 있다고 봅니다. 경영은 살아 움직이는 것으로 시시각각 변화합니다. 정보보호 또한 살아서 움직입니다. 변화에 대비하는 절차를 확립하지 못한 기업은 살아남지 못하게 될 것 입니다. 이를 해결할 방법으로 정보보호 관리체계를 수립·운영하는 것이라 생각합니다.

올해 정보통신망법 개정으로 인하여 특정 조건에 부합하는 기업은 정보보호관리체계 인증심사를 의무적으로 받아야 합니다. 하지만 관리체계를 수립한다는 것이 단기간 이루어지는 것이 아니고 , 자체 수립하면 좋겠지만 그렇지 못할 경우 컨설팅을 받아야 하고, 이행증적을 제시해야 하는데 시일이 오래 걸립니다. 그렇다 보니 이런저런 비용 따져서 차라리 과태료 내는 것이 더 낫겠다라는 분위기도 일부 있습니다. 어떻게 보시는지요? 혹은 준비에 대한 조언 좀 주시지요..

2004년 도입한 정보보호 안전진단 제도가 그동안 많은 성과를 낸 것은 사실이나 일부 기업 또는 수행기관들의 형식적인 안전진단, 최소한의 보호조치(46개 통제항목)로 태생적 한계가 있어 언론이나 국회의 지적으로 2012년 법 개정을 통해 안전진단을 폐지하고 안전진단 의무대상자를 ISMS 인증의무대상자로 지정하였습니다.

안전진단 제도에서도 문제점으로 지적되어온 하반기 쏠림을 방지하기 위해 인증의무를 1년간의('2012.2.17 ~ 2013.2.17) 유예기간을 부여한바 있으며 또한 사업자 등록일 기준 해당 분기에 신청하도록 법에서 규정한바 있습니다. 의무 인증을 시행한 첫해에는 일부 기업의 준비부족으로 하반기에 신청을 많이 하고 있으나 연말까지는 인증심사와 인증서 부여에는 문제가 없어 보입니다. ISMS 의무 제도는 사업자가 정보보호 관리체계를 스스로 구축하고 운영하도록 하여 침해사고시 피해를 최소화 하는데 목적이 있습니다.

인터넷 침해사고는 해당 사업자만 피해를 입는 것이 아니라, 다른 사업자에게로 피해가 확산되어 국가 사회적으로 많은 피해를 주기 때문에 정부에서 규제를 하는 것입니다. 인증을 받지 않을 경우는 법규 준수 위반으로 과태료(1,000만원)가 부과되게 됩니다. 그동안 안전진단을 받아왔던 기업은 어느 정도 관리체계가 수립되어 준비하는데 어려움이 없을 것으로 판단되며 신규로 받아야 하는 일부 기업은 자체적으로 관리체계 수립이 어려울 경우 정보보호 컨설팅 업체 도움을 받아 근년 12월말까지는 인증을 받아야 법규 위반에 대한 불이익이 없을 것으로 보입니다. 산업안전보건법과 같이 개인의 건강진단 미수검시 과태료를 부과하 듯이 ISMS 인증 의무화가 과태료를 부과하고자 하는 것이 아니고 기업 스스로 기업정보와 국민의 개인정보를 보호하도록 공적인 차원에서 기업의 정보보호 투자를 유도하고 정보보호 수준을 한 단계 끌어 올리고자하는 것이 목적입니다. 하지만 보안에 투자하는 것이 아까워 벌금을 내겠다는 생각은 매우 위험한 발상이라 생각합니다.

인증을 받지 않을 경우 기업에 미치는 악 영향은 상상을 초월합니다. 과태료 부과 뿐만 아니라 정보통신서비스 이용자의 이탈과 기업의 이미지 추락, 언론 등의 해당 기업 공개로 인한 주가 하락 등 사업자에 엄청난 부정적 영향을 미치게 될 것입니다. 의무 인증 제도는 기업의 경제적 부담을 주고자 한 것이 아니고 기업의 비즈니스 연속성과 경쟁력 확보를 위해 침해사고시 피해를 최소화하여 기업이 수혜자가 될 수 있도록 한 제도임을 다시 한번 명심해야 할 것입니다.

최근 보안에 대한 이슈가 부각이되고, 기술적인 부분도 중요하지만 체계적인 관리적 부분도 무척 강화가 되고, 컴플라이언스(법준수)의 중요성도 대두되고 있습니다. 이에 많은 사람들이 관리체계 도입이나 인증심사원등에 관심을 가지고 있는데요..어떠한 준비와 노력을 기울이면 될지 이제 막 시작하는 비기너나 주니어 분들에게 조언을 한다면?

제가 ISMS 모델을 개발하고 적용하고자 했던 근본적인 취지는 정보보호를 기업 경영 전략의 하나로 보고 기업의 비즈니스 연속성 및 경쟁력 확보에 목표를 두고 제도화를 하였던 것입니다. 정보보호 관리체계를 일반적으로 관리적인 관점에서는 보는 경향이 있는데 관리체계란 기술적, 물리적 분야를 포함한 종합적인 체계를 의미하는 것입니다. 마치 기술을 몰라도 관리체계를 수립하고 운영할 수 있고 관리체계에 대한 인증심사나 컨설팅이 가능한 것으로 오해를 많이 하게 됩니다. **정보보호 관리체계는 정보보호 요소기술들이 모두 결집된 정보보호 분야의 융합기술입니다.** 관리체계의 철학과 사상을 이해하고 적용하는 데는 정보보호기술과 전략적 사고 즉 디자인적 사고를 모두 가져야 한다는 것입니다.

ISMS는 정보보호의 시작이자 끝이며 예술이라고 생각합니다. 물론 ISMS가 경영적 관점에서 보면 정보보호 초심자들이나 기술적 접근이 어려운 분들에게 쉽게 접근할 수 있는 매개체 역할을 하는 것은 분명합니다. 다만, 관리적인 것으로만 인식하여 나이 드신 분들이나 초심자가 쉽게 접근하려고 했던 분들은 관리체계 수립이나 인증심사를 경험하면서 너무 어렵고 힘들어 포기하는 분들을 많이 보아왔습니다. 정보보호 기술을 모르고는 쉽게 접근하기 어려운 분야라고 생각합니다. ISMS를 만든 사람 입장에서는 아마도 정보보호 분야에서 가장 어려운 분야가 아닌가 합니다. 그렇기 때문에 대부분 기관/기업의 정보보호담당자나 CISO 채용에 기본 자질로 ISMS 유경험자를 찾고 있다는 것입니다.

초기에 ISMS가 비즈니스 특성과 중요 정보자산의 환경을 반영하여 기업 스스로 최적화된 ISMS를 구축하기에는 어려움이 있게 마련입니다. 이런 어려움을 해소하고자 ISMS 프레임워크 개발 당시 PDCA 모델을 적용하여 지속적인 개선과 보완을 이행하고 조직에 내재화가 될 수 있도록 ISMS를 유지·관리를 기업 스스로 하도록 설계가 되어 있어 정보보호를 모르는 사람도 쉽게 접근이 가능하도로고 설계를 하였던 것입니다.

정보보호에 대한 기업의 사회적 책임과 역할이 어느 때보다 중요한 시점이며, 정보보호 컴플라이언스, 정보보호 거버넌스 등 정보보호 관리 문제가 기업 경쟁력의 핵심 요소로 인식되고 있으며 또한 정보보호 사고로 인한 법적 분쟁 발생시 정보보호 활동에 대해서도 어떻게 대응할 지 고민일 것입니다. 이런 문제를 해결하기 가장 좋은 솔루션은 관리체계를 구축·운영하는 것입니다. 그동안 조직별로 부분적, 일회성 활동을 통해 단편적 대응을 하였다면 관리체계 구축을 통해 중요한 자산보호를 위해 조직 전체에 걸쳐 서로 협력관계를 유지하여 지속적 체계적 대응이 가능하다는 것입니다.

또한 조직이 집중적으로 대응해야 할 위험 관리 체계를 유지하고 적절한 보호대책을 실시함으로써 정보보호 사고의 발생가능성을 줄이고 사고가 발생했을 경우에도 손실 경감으로 기업 가치 향상과 비즈니스 연속성을 보장할 수 있다는게 관리체계 수립의 목적이라 하겠습니다. 관리체계는 실천이며 기술이 아니라 예술이라 생각합니다.

ISMS(정보보호관리체계)와 PIMS(개인정보보호관리체계)는 출발 사상부터 다르게 출발을 하게 되었는데요. 정보보호관리체계는 기업(기관)의 자산의 위협에 대한 보호라 침해사고를 당하더라도 해당 기업(기관)이 피해를 보지만, 개인정보보호관리체계는 이용자(망법) 혹은 정보주체(개인정보보호법)의 개인정보를 보호하는 측면이기 때문에 침해사고를 당하면 개인정보처리자 혹은 취급자도 가해자가 될 수 있어 ISMS와 PIMS를 동시에 도입하고 인증을 받으려 합니다.

그렇다보니 이중규제와 서로 상충하는 부분이 있는데 이러한 부분에 대한 해소는 어떻게 진행이 되고 있고, 어떻게 준비하면 될까요?

말씀하신 것처럼 ISMS와 PIMS는 출발 사상이 다르게 출발하였습니다. 다만, 관리체계 프레임워크를 개발하면서 국내 보안관리 표준 프레임워크인 ISMS 모델을 대부분 준용하다 보니 인증 규격 자체에 대한 중복 또는 유사하다는 오해를 받게 되었습니다. 대부분 조직이 정보보호 조직과 개인정보보호 조직이 분리 되있듯이 두 제도간 차이점은 정보를 다루는 주체에 따라 범위가 다르다는 것입니다.

그러다 보니 일부 조직에서는 ISMS 범위와 PIMS 범위가 동일한 곳도 있어 중복이나 이중규제로 보는 것 같습니다. 현재 ISMS의 경우 미래부, PIMS의 경우 방통위 소관 업무로 제도 자체는 이원화 되어 있으나 이러한 부분을 해소하기 위해 인증기관을 KISA가 단독 수행하게 하여 인증 범위가 동일하거나 일부 중복 부분에 대해서는 동시에 심사를 받도록 하여 비용과 업무 부담을 줄여주고 있습니다. 다만 향후 민간 인증기관 추가 지정이 될 경우 인증기관간 업무 조정이 필요한 부분입니다, 하여튼 인증을 준비하는 기업에서는 범위가 중복 되는 경우에는 관리체계 수립을 동시에 준비를 하고 인증을 신청하는게 좋을 것 같습니다.

내년부터는 G-ISMS가 폐지되고, ISMS로 통합됩니다. 이에 따라 변화되는 점은 없는지, 혹은 준비해야 하는 사항은 무엇인지 짚어 주신다면?

G-ISMS 제도 도입 이전에도 전자정부서비스에 대해 ISMS를 적용하여 왔으나, 부처가 다른 문제로 ISMS를 적용하는데 한계가 있어 G-ISMS도입 한바 있으나 부처간 협의에 의해 제도 중복 및 유사성 문제를 해결하고자 2014년부터 G-ISMS를 ISMS로 일원화하기로 결정한바 있습니다. 침해사고와 관리체계 수립은 민간이나 공공이나 구별하기 어려우며 업종이나 기관성격, 규모 등에 상관없이 위험분석 · 평가를 통해 해당 기관/기업에서 정보보호 수

준을 정하고 보호대책을 수립하도록 하는 것이 관리체계의 기본 철학이라 생각합니다. G-ISMS도 결국 도입 당시 ISMS 표준 프레임워크를 적용했기 때문에 프레임워크는 큰 변화는 없으며 일부 보호대책 부분에서 약간의 전환 작업은 있을 수 있겠습니다.

제가 커뮤니티를 2004년부터 운영하였으니 올해가 햇수로 꼭 10년정도 됩니다. 그동안 수많은 사람들과 만나고, 온라인을 통하여 이야기를 들어보면 조직의 정보보호에 대한 로드맵을 그리지 못해 힘들어 하는 사람들을 많이 보았습니다. 팀장님께서 생각하시는 보안에 대한 로드맵을 제시한다면 어떤 것이 있을까요?

정보보호 로드맵은 거창한 목표 보다는 효과적인 정보보호 강화 전략(정보보호 디자인)수립, 혁신적인 정보보호 프로그램 적용하고 또한 정보보호 전담조직을 구성하고 정책 수립 및 정보자산에 대한 위험 평가 등 체계적이고 일관적인 정보보호 관리 활동을 할 수 있는 기틀을 마련하는 것에서부터 시작했으면 합니다. 정보보호를 위한 절대적이고 영속적인 대책은 없다고 합니다. 공격은 방어를 이길 수 밖에 없습니다. 이것을 해결하는 최선의 선택은 정보보호 관리체계(ISMS) 구축이라 생각합니다.

정보라는 눈에 보이지 않는 자산을 대상으로 하는 정보보호에서는 확실한 관리체계를 구축하지 않고는 정확하게 관리하고 운영할 수 없다고 봅니다. 관리체계는 정보보호의 가장 기본이자 시작입니다. 정보보호에 전략적인 디자인적 사고를 가지고 정보보호도 새로운 비즈니스로 디자인하려는 노력이 필요하다는 것입니다.

보안인닷컴 캐치프레이즈 중에 하나가 “전국중심의 보안”입니다. 즉, 보안인식제고를 전파하고, 보안에 대한 이슈논의나 정보교류를 하고 있습니다. 수도권 중심의 세미나, 교육집중현상이 일어나고 있습니다. 지역에서는 보안관련 세미나, 제대로 배울 수 있는 교육의 기회조차 없습니다. 이러한 부분에 대하여 어떻게 생각하고 그 대응방안은 없을까요?

그동안 저도 정보보호 업무를 수행하면서 가장 안타까운 부분이 대부분 세미나, 교육 등이 서울에 집중된 다는 것입니다. 대부분 기업들이 수도권에 집중된 것도 있겠으나 지방 기업이나 담당자들에게도 참여 기회가 공평하게 부여 될 수 있도록 개인정보 순회 교육 등이 좋은 예가 아닌가 합니다.

국가·공공기관들의 지방 이전으로 인해 주요기반시설도 함께 이전하면서 기반시설보호를 위한 정보보호전문가가 많이 필요로 할 것으로 보입니다. 정보보호 전문 인력 양성을 위해 지

역별 거점별로 대학에 정보보호학과 신설과 최고의 보안전문가를 배출하여 지역 기반시설에 대한 정보보호를 담담하도록 해야 할 것입니다. 또한 정보보호 분야에 대한 세미나, 교육 등을 지역 단위로 순회 교육이나 참여 인력을 지역 안배 등을 하는 방안이 있을 것 같습니다.

최근 정부 3.0으로 정부에서는 새로운 패러다임을 제시하고 있습니다. 이에는 소통,개방, 공유,협력이라는 키워드로 축약 될 수 있는데요..이는 또다른 측면에서는 보안과 아주 밀접한 관계가 있을 것입니다...정부 3.0과 보안의 관계 어떻게 보시는지요?

저도 케치프레이즈로 “정보보호를 디자인하자”와 “열린 보안”을 주장하고 있습니다. “열린 보안”을 실천하기 위해서도 정보보호 분야에도 능동적 공개 · 참여, 개방 · 공유, 소통 · 협력으로 새로운 가치를 창조해야 합니다. 최근 3.20, 6.25와 같은 침해사고 발생시 분석정보에 대한 공격 기법 공개 및 공유, 국가적 취약점 DB 구축 및 공유, 기업간 침해사고 정보에 대한 공유 및 협력 등이 있을 수 있을 것 같습니다.

정부 3.0과 마찬가지로 보안관리 제도 자체도 실효성 있고 효과가 있고 잘 활용되야 한다는 것입니다. 다시 말해 정보보호에도 분석과 직관을 모두 활용한 사람들이 소통 · 개방 · 공유 · 협력하는 문제를 해결하는 프로세스인 디자인 사고가 필요하다는 것입니다.

마지막으로 대한민국 최대 보안커뮤니티 “보안인닷컴” 회원 여러분들에게 보안에 대한 당부 사항이나 격려의 한 말씀 부탁드립니다.

이렇게 지면을 통해 회원들을 만나게 되어 영광스럽게 생각합니다. “보안인닷컴”이 10년을 넘었다고 하니 진심으로 축하를 드립니다. 현재 국내 기업의 CISO, 정보보호 담당자들은 정보보호를 위해 책임과 의무를 다하고 있지만 보안사고시 가장 먼저 문책을 당하는 것을 보면서 정말 안타까웠습니다. 점점 보안사고는 증가하고 기업 책임이 강화되면서 보안담당자 고충은 가중되고 직무만족도 또한 저하되고 있는 현실을 보면서 CISO와 정보보호 담당자들에게 많은 책임감과 사명감을 갖도록 요구만 하고 별다른 처우개선 방안을 제시 하지 못하는게 현실인 것 같습니다. “보안인닷컴”이라는 온라인 커뮤니티를 통해 정보보호 전문가들이 이 분야를 떠나지 않고 지속적으로 후배들에게 경험과 노하우를 전수하고 창의적인 정보보호 정보보호 전문가들이 모일 수 있도록 정보보호 전문가들의 권익을 보호할 수 있는

장이 되었으면 하며, 또한 정보보호 전문가와의 교류와 협력, 지식 공유를 통해 정보보호 발전에 많은 기여를 했으면 합니다. 저도 적극 동참 하도록 하겠습니다. 10년을 맞은 '보안인닷컴' 커뮤니티가 앞으로 정보보호 발전에 많은 기여와 역할을 수행할 수 있을 것으로 생각하며, '보안인닷컴' 커뮤니티의 발전을 기원합니다. BoAN人

* 바쁘신 가운데 기꺼이 인터뷰에 응해주신 한국인터넷진흥원(KISA) 장상수 팀장님께 진심으로 다시한번 감사의 말씀을 드리고 책 출간도 축하드리겠습니다.

[보안人 기고]
사이버 사령부 사태를 바라보는 불편한 마음
(고재호, 보안인닷컴 스텝3기)

제목: 사이버사령부 사태를 바라보는 불편한 마음.

작금의 사이버사령부 사태를 보면, 문득 군복무 시절 야전 훈련의 기억이 떠오른다. 훈련이나 작전간에도 지역 주민들에게 민폐를 끼치지 않기 위해 배추 잎 하나라도 밟을까 신경을 쓰다 보면 몸도 마음도 지치게 마련이었으나, 평생을 전방 산골짜기에서 살아오신 분들의 굽어진 허리와 주름을 보며, 다시금 힘을 내어 임무를 수행하곤 했었다.

한일월드컵과, 연평해전으로 기억되는 2002년, 당시 휴전선에는 고성능 확성기를 통해 대북 방송이 진행되고 있었다. 철책 경계등 바깥에 드리워진 DMZ는 적막함을 넘어 숨막힐 듯한 어둠이었고 유일하게 그 적막을 깨는 것은 자유대한을 알리는 방송과 최신가요뿐이었다. 하늘의 차가운 별빛 조차 얼어 붙은 듯, 그렇게 휴전선의 밤은 유독 다른 차원의 시간처럼 흘렀다. 필자가 대북방송을 좋아했던 이유는 야간 근무의 무료함을 달래줌과 동시에 끔찍한 대남 방송 소리를 막아주었기 때문이다. 북한 여성이 특유의 목소리로 노래를 부르는데 그것이 좋지도 않은 북측 확성기를 통해 들려 올 때면, 마치 귀신 목소리처럼 들려와서 등줄기가 오싹 거리 곤 했다. 어쩌다 스산한 바람까지 불어 오는 날엔, 노래 소리가 공기와 함께 울렁거려 나도 모르게 총을 내려놓고 DMZ의 어둠 속으로 걸어 들어갈 것 같은 기분까지 들었으니, 그들의 열악한 장비가 어쩌면 치밀한(?) 작전이었는지도 모를 일이다.

당시 동기 장교간에는 심리전단이네 공작단이네 하는 특수분야를 노리는 녀석들이 많았다. 그것도 그럴 것이 '정보요원'이 되는 것이 이상이자 목표였기 때문이다. 그러나 내가 야전 소대장이던 2004년, 심리전 소대장 녀석의 한 숨을 듣게 되었고 얼마 후, 그의 부대는 해체되고 말았다. 북한의 대북심리전 중단 압박으로 인해 휴전선일대의 대북방송이 전격 중단되었기 때문이었다. '서울 한 복판 국방부로 복귀하는데 무슨 앓는 소리냐'며 부럽다는 말을 그 친구에게 건넸지만, 그의 착잡한 마음을 누가 헤아릴 수 있으랴.

그렇게 정치적 상황에 따라 민감하게 움직였던 국방 정보본부 소속 심리전단이 6년만인 2010년, 큰 전환기를 맞게 되었는데 바로 '국군 사이버사령부'의 창설이다. 2009년 7월7일에 있었던 대규모 DDoS 공격 배후가 북한으로 지목되면서 정보본부 예하에 준장이 지휘하는 사령부가 창설되었고 심리전단은 사이버사령부 예하로 배속되었다. 하지만 이후에도 국가 전산망에 대한 사이버 테러가 끊이지 않았고 사이버사령부는 국방부 직할 부대로 배속전환 되었으며 소장급 사령관으로의 승격과 함께 인원 또한 2배이상 증편이 추진되고 있다. 북한에 의해 축소되었던 심리전단이 이제 다시 북한 때문에 확대 된 것이다.

그러한 심리전단이 지금 정치적 논란에 다시금 휘말리고 있다. 사이버사령부 소속 군인과 군무원이 작년 대통령 선거 당시 정치적 활동을 했다는 의혹을 받고 있기 때문인데, 정황 또한 구체적이어서 논란이 일파만파로 커지고 있다. 그러나 심리전단과 사이버전 부대는 분명 다르며 앞에서 언급한 심리전단은 사이버보안 전문가 집단이 아니다. 문제는 이러한 댓글의 주체가 심리전단 소속이 아닌 사이버전을 담당하는 부대 소속으로 보도 되는 등 사이버사령부는 이래저래 곤혹스럽게 되었다. 우리 국민에게 사이버사령부는 어떤 곳인가. 국정원 소속 '국가사이버안전센터', 경찰청 소속 '사이버테러대응센터'와 함께 사이버안보의 핵심이며 국민과 정치권 모두의 적극적인 지지를 등에 업고 성장한 국가급 정보보호 기관이다. 덕분에 우리나라는 세계에서 처음으로 사이버국방학과(고려대학교)를 보유하게 되었고 합격자 신상 대외비 관리, 4년 학자금 전액지원, 졸업 후 7년간 사이버 사령부 장교 복무 등으로 여러 방면에 큰 반향을 일으키고 있다. 더불어, 국가적 차원에서는 기반시설 지정 확대, 10대 세계일류 정보보호 제품 개발 및 보안전문가 양성 특별교육 프로그램 설치가 진행되는 등, 사이버사령부는 정보보안 인력의 확대, 전문성의 고도화, 국가 보안산업 강화와 시장확대에 중요한 역할을 하고 있다.

이러한 와중에 발생한 작금의 불편한 사태를 빌어 필자는 사이버 전장 인식, 사이버 전력 강화, 사이버 민군 협력 세가지에 대하여 보안인 여러분과 나누어 보고자 한다.

첫째, 사이버 전장 인식

국방부 장관이 언급한 '정치적 댓글이 아니라....북한이 대남 선전 선동 모략을 하는 데 대응하는 차원이었다'이라는 의미는 무엇일까. 과거 심리전단의 주요활동은 야포나 기구(풍선)등을 활용해 전단지(삐라)를 북측에 살포하거나 확성기, 라디오 방송이었다. 다시 말해, 북한 지역이 우리의 직접적인 공작 활동 대상이었고 북한 또한 남쪽 영토가 대남 심리전 공작 영역이었다. 하지만 국방장관의 말을 빌어보면, 지금은 인터넷상에 북한의 삐라가 뿌려지고 있으며 그것에 우리가 대응을 하고 있다는 뜻이다. 이것이 실상 무서운 것인데, 현재 북한의 사이버 대남 심리전 활동은 남한 내에서 활발히 이루어지고 있으나 우리군의 대북 사이버 심리전은 불가능함을 역설적으로 보여준다. 왜냐하면 북한에는 우리와 같은 인터넷이 없기 때문이다.

따라서, 정보보호 전문가를 꿈꾸거나 현업에 종사하는 분들은 사이버 전장이 이미 대한민국 한 복판이라는 현실 감각을 잊지 말아야 할 것이다. 이미 북한 해커 부대, 대남 공작 요원들은 북한에 있지 않고 우리 기업의 업무용 PC와 수많은 개인 PC의 취약점 속에 있다. 다시 말해, 그들이 머물 곳은 북한에 없다. 남한에 있다.

둘째, 사이버 전력 강화

얼마 전 마주친 촛불시위 현장에서는 어린 학생, 주부, 노인들이 '국정원 OUT' 팻말을 들고 규탄 대회를 하고 있었다. 그들에게 국가정보원 심리전단이 중요할까? 그저 국정원이 못미더울 뿐이다. 사이버사령부 사태도 마찬가지이다. 어느 소속이 더 이상 중요하지 않다. 그저 사이버사령부가 타깃이 되고 있고 해체 발언까지 나왔다. 물론 특정 단위 조직이 독자적으로

활동할 수 없기에 조직 전체가 책임지는 것은 당연하겠지만 긍정적인 임무 수행까지 차질을 빚게 되는 것은 우려할 만 하다. 몇 년 전 국가 사이버안보의 컨트롤 타워로 국가정보원이 지목되었다가 민간인 사찰 우려로 유야무야 되었는데, 그 대안으로 필자가 기대하고 있던 사이버사령부 조차 논란에 휘말리게 되니 사이버보안 컨트롤 타워 수립이 또 물 건너 가는 게 아닐까 조심스럽다.

컨트롤타워 역할을 사이버사령부로 기대했던 이유는, 바로 미국이 그러하기 때문인데, 미국 사이버전사령부(USCYBERCOM)는 전력망 등 민간 핵심기반시설 관련 컴퓨터와 네트워크에 대한 보호 임무까지 맡고 있다. 다시 말해, 국방 네트워크에 국한 되지 않고 민간 주요 시설을 포함한 사이버안보의 컨트롤타워 역할을 하고 있는 것이다.

또 다른 이유는, 우리 군이 미국의 군사 체계와 매우 닮아 있다는 점 때문이다. 북한, 중국의 위협이 존재하고 그로 인한 한미동맹이 지속되는 한 이러한 군사협력은 앞으로도 유지될 가능성이 높다. 유사시 연합작전 수행을 위해 양국이 어느 정도 양해하기 때문인데 이는 장차 사이버전장에서도 유효할 것으로 예상된다. 더구나, 미 사이버전 사령부는 미국 및 동맹국들이 사이버공간에서의 활동을 보장하고 적 활동을 무력화하기 위한 광범위한 활동을 그들의 임무로 선언한 바 있다. 미국 입장에서도 중국과 북한의 사이버부대를 견제하기 위해서 한반도의 지정학적 위치를 고려하지 않을 수 없는 것은 주지의 사실이다.(사이버전이 단순히 가상의 공간에서만 이루어진다고 생각하는 독자는 이 기회에 그 틀을 벗어나길 소망한다)

이렇듯 사이버전에 총력을 기울여야 할 시점에서 대한민국이 거꾸로 가서는 안 된다. 썩은 것은 버릴 지 언정 필요한 것도 도려내는 우둔한 조치는 하지 말아야 할 것이다. 이럴 때 일수록 사이버사령부 본연의 임무를 다시금 깊이 새겨 사이버보안 역량을 강화하는데 이전 보다 더 집중하길 바란다. 사이버 전력은 어떠한 경우에도 멈추지 말고 강화되어야 한다.

셋째, 사이버 민군 협력

사이버 전력강화 방안은 무엇일까. 현대에는 민군 협력체계가 매우 중요한 시대이다. 이는 전통적으로 재래식 전력에만 연관되어 있다고 생각되지만, 알고 보면 첨단기술 및 정보보안 분야도 뗄래야 뗄 수 없는 관계에 있다. 장차 사이버사령부 경력 간부 및 전역병사 채용을 확대하는 정보보호 기업은 민군 협력의 좋은 모델이 될 것이라고 필자는 생각한다. 학생 및 청년층에게는 전역 후 취업에 유리한 정보보호 분야에 대한 선호도가 높아질 것이고, 기업 또한 우수한 자원을 선발 할 기회가 확대 될 것이다.

사이버전장의 개념이 아직도 모호한 이유는 국가와 민간의 네트워크 영역이 명확하지 않기 때문이다. 다시 말해, 민간분야의 정보보호와 국가 정보보호를 분리해서 대응하는 것은, 그 모호함으로 인해 우리의 정보보호 대응체계를 약화시킬 요인이 될 수 있다는 뜻이다. 따라서, 정보보호 관련 업계와 군은, 국가 사이버전 정책 이해와 교류를 적극적으로 활성화하고 더 나아가 민군 합동 사이버대응체계를 수립하여 유사시 신속한 대응으로 적의 사이버도발을 무력화 또는 최소화해야 할 것이다. 이것은 민군이 상호 신뢰와 이해를 통해 만들어 나가야 하

며, 국가 총력전으로 정의 되는 현대전쟁의 특징이 사이버공간에서도 유효함을 분명히 인식할 때에 비로소 성공할 것이다.

마치며,
국가 정보보호 역량 발전에 탄력을 받아야 할 중요한 시점에 사이버사령부 사태는 개인적으로 매우 안타까운 일이다. 사이버전을 수행하는 정보보호 전문가에 대한 오해와 찬물을 끼얹는 게 아닌가 우려되고 그들의 노고가 외면을 받지 않을까 걱정된다. 사이버사령부의 신뢰성에도 타격을 입었지만 부대의 전략적 운용에도 큰 피해를 입었다. 그 동안 세부조직과 규모는 비밀에 부쳐 알려지지 않았으나 이번 사건으로 조직과 부대원 및 채용규모도 노출되었다. 적들에게 실시간으로 벌겨 벗겨지는 국가 사이버안보의 핵심전력을 보며 마우스 클릭 만으로도 최신 정보를 업데이트 할 적들을 생각하고 있자니 필자는 속이 쓰리고 가슴이 답답하다.

군은 존재 목적상 정치적 중립을 지켜야 한다. 개인적인 의사 표현은 투표권으로 행사하면 될 뿐, 복무시간에 군사시설 안에서 특정 정치 세력을 옹호하거나 비난하는 인터넷 활동을 했다면 분명 잘 못한 것이다. 게다가 본연의 임무인 정보보호 및 사이버테러 무력화와 상관없는 활동이라면 복무위반, 직무유기로 징계 받아 마땅하다. 하지만, 정치적 목적에 의해 국가 사이버안보의 역할론 까지 부정되어서는 안 될 것이다. 사이버보안 정책 추진이 지지부진한 사이, 우리의 취약점은 여전히 공격 받고 있고 그 피해는 고스란히 국민이 떠안을 것이다. 자칫 잘 못하면, 핵 전력과 함께 또 하나의 가공할 비대칭 전력의 위협을 목도하게 될지도 모를 일이다.

필자
고재호(em5cean@gmail.com)
사단/군단/군사령부 ASIC, CCC, EOC 에서 다 년간 특수정보 및 군사보안 업무와 한미연합훈련 등을 수행하였다. 현재는 기업에서 정보보호 분야를 담당하고 있다. BoAN人

*외부 기고는 본지 편집의도와 무관함을 알려 드립니다.

[보안人 지면을 빌려 드립니다]

이 코너는 구독자 여러분의 참여가 이루어지는 공간입니다. 여러 가지 소소한 일상적인 이야기나 공부이야기, 세미나후기, 멘토링, 취업기, 자격증 취득기등 여러 가지 이야기를 나눌수 있는 공간입니다. 축하, 승진, 입학, 졸업사연도 받습니다. 가급적 편집하지 않고 리얼하게 실어드립니다. 많은 참여를 바라겠습니다. 보내실 곳은 boanin@naver.com 으로 보내 주세요.

보안인닷컴 e-매거진 [보안人] 후원안내

매월 무료로 발행되는 보안인닷컴 e-매거진 [보안人]을 적극적으로 후원해 주실 분들을 찾습니다. 후원해 주신 분들은 e-매거진 [보안人]에 후원자 명단을 공개해 드립니다. 금액에는 제한이 없습니다.

우리은행 204-028530-02-201 예금주 : 전주현

2013.05월 기부해 주신분
손찬종님 10만원
2013.05월 기부해 주신분
김정선님 3만원
2013.06월 기부해 주신분
김정선님 3만원
2013.08월 기부해 주신분
김정선님 1만원

* 기부해 주신 분들에게 감사드립니다.

보안인닷컴 e-매거진 참여 하신 분

지금까지 보안인닷컴 e-매거진 [보안人]에는 많은 분들이 좋은 글과 인터뷰에 참여 해 주셨기에 가능하였습니다. 이에 참여 하신분들에 대한 감사의 마음으로 이번호부터는 참여하신 분들에 대한 간략한 글 소개를 올려 드립니다. 앞으로 많은 분들의 참여와 관심 부탁드립니다. 해당 내용을 보고자 하시는 분들은 카페 대문에 각 호별로 배너를 클릭하시면 다운로드 받아 보실수 있습니다.

1. 창간호: "wi-fi 무선랜 보안현실 및 사례" - 변동삼
"안티포렌식 기술의 소개 및 대응기술" - 김석
"보안의 핵심적 요소이자 취약요소 사람" - 신동일
"정보보호 기술병의 SIS 1급 합격수기" - 김무현
"부평스(부산평일스터디)를 소개합니다." - 김건오
"모의해킹 고수 어떻게 준비할까" - 조정원
"중소기업 자가진단압 소개" -김건오
"똑똑한 스마트폰 안전하게 사용하기" - 강정웅
"너무나 갖고 싶었던 명함" - 이재호
"The 17Th Network Security Workshop-korea 후기 - 이기성
[축하의말] 보안인식제고는 진정한 정보보호전문가의 첫걸음 - 강용남
[축하의말] 개인정보보호 최대의 적은 무관심 - 김종구

2. 제2호 : "보안의 시작은 관리체계수립하여 SLC만들어야" -전주현
"왜 우리는 위험을 관리하고 있지 못하는가? -문승주
"ISMS을 통한 기업보안구축사례 - 김용완
"모의해킹 컨설턴트가 되려면-(2) - 조정원

3. 제3호: "보안 업무의 마지막 단계 - 정보기기의 폐기업무에 대하여" -김재우
"모의해킹 컨설턴트가 되려면(3) - 조정원
"소상공인/준용사업자 사업시, 개인정보보호법 어떻게 대처할까?" -전주현
"2011 KAIST 사이버 워크샵 후기 - 이기성
"윈도우7 보안의 핵, 사용자 계정(UAC) - 박광수
"[책리뷰] 내부직원의 위협으로부터 기업의 정보 유출을 막아라 - 이기호

4. 제4호: "KUCIS 하계 워크숍 -김주영
"APT 해킹에 대하여" -유인재
"정보보호 동아리 창설 사례" - 이기성
"제2회 대학생 금융보안캠프" - 임효식

보안인닷컴 e-매거진 참여 하신 분

지금까지 보안인닷컴 e-매거진 [보안人]에는 많은 분들이 좋은 글과 인터뷰에 참여 해 주셨기에 가능하였습니다. 이에 참여 하신분들에 대한 감사의 마음으로 이번호부터는 참여하신 분들에 대한 간략한 글 소개를 올려 드립니다. 앞으로 많은 분들의 참여와 관심 부탁드립니다. 해당 내용을 보고자 하시는 분들은 카페 대문에 각 호별로 배너를 클릭하시면 다운로드 받아 보실수 있습니다.

5. 제5호: "BS10012에서 이야기 하는 PIMS" - 박준용
"스마트보안과 테스트의 중요성" - 유정훈
"개인정보보호법 컴플라이언스냐? 시큐리티냐?" - 전주현

6. 제6호 : "국내 정보보호 자격증 발전방안에 대한 소고" -박준용
[인터뷰] 한재호 (주)에이쓰리시큐리티 대표이사 -유인재
[인터뷰] 김휘강 고려대학교 정보보호대학원 교수 - 유인재
[특별기고] 개인정보보호법 시행에 따른 민간기업과 공공기관 애로사항 -전주현

7. 제7호: "[새해특집-1] 정보보호학과 탐방 - 고려대 사이버국방학과" -김승주
"[새해특집-2] 정보보호업체 탐방 - 안랩(구 안철수연구소" -전주현
"BackTrack이란? -조정원
"해킹대회에 대한 소개 - 유인재

8. 제8호: "BackTrack 안드로이드 설치 -조정원,전영재
"디지털포렌식분석-SANS 문제풀이 - 이준형
"해킹보안동아리 창설이야기 -국민대학교 - 유인재
"대학교 4학년 이후의 삶 - 임효재
"IT특화병, 정보보호기술병 -김주영

9. 제9호: "한국IBM 보안사업부 출범과 그 의의" - 박형근
"WireLess Security에 대하여" - 권오훈
"A3시큐리티 세미나 후기" - 김주영
"[인터뷰] A3아카데미 " 허아람
"[인터뷰] 수원대 정보보호동아리 "FLAG" - 유인재

보안인닷컴 e-매거진 참여 하신 분

지금까지 보안인닷컴 e-매거진 [보안人]에는 많은 분들이 좋은 글과 인터뷰에 참여 해 주셨기에 가능하였습니다. 이에 참여 하신분들에 대한 감사의 마음으로 이번호부터는 참여하신 분들에 대한 간략한 글 소개를 올려 드립니다. 앞으로 많은 분들의 참여와 관심 부탁드립니다. 해당 내용을 보고자 하시는 분들은 카페 대문에 각 호별로 배너를 클릭하시면 다운로드 받아 보실수 있습니다.

10. 제10호: [기고] "주말 Malware Launch Detected!" - 전상훈
[번역] "모바일 데이터 암호기술" - 임효식
"CentOS 5.5에서 하드디스크 추가하기" - 전주현
"모의해킹 방법론" - 조정원
"신종 MBR파괴 악성코드 분석" - 이규형

11. 제11호 : [기고] "IT기술사 도전해보자" -이이진
[기고] "해킹,악성코드 그리고 개인정보보호" -신원
[번역] "Security, Privacy and Policy Roundup" -권오훈
[인터뷰] "기사가 현실을 바꿀때 보람있어요" -장윤정

12. 제12호: [기고] "개인정보보호법 본격시행으로 다시본 국민식별체계" - 이형효
[칼럼] "개인정보보호 책임자 역할과 의미"-전주현
[매뉴얼] Snort IDS 윈도우버전 설치방법" -박현철
[화제의 책, 저자 인터뷰] "안철수, He Story" - 박근우
[기고] "네이트 해킹 사건 승소판결의 의미" - 유능종

13. 제13호: [기고] "보안컨설팅을 지망하는 분들에게" - 신수정
[칼럼] " 국가기술자격증 '정보보안기사/산업기사'에 거는기대 -전주현
[인터뷰] "정보보호전문가, 장인정신 가져야' - 최운호
[인터뷰] "보안의 다양성 보도와 취재원 보도가 최우선" - 길민권
[기고] 드라마 '유령'이 현실에 미치는 영향 -유인재

14. 제14호: [기고] "KAIST 악성코드 분석 프로세스" - 임효식
[인터뷰] "서비스 이용시 프라이버시 사전침해 제거가 최우선" - 이진규
[인터뷰] "IT경쟁력, 글로벌로 눈을 돌려라 - 이택동
[인터뷰] "보안책임자 IT역량과 비즈니스 역량 함께 갖주어야" - 차인환

보안인닷컴 e-매거진 참여 하신 분

지금까지 보안인닷컴 e-매거진 [보안人]에는 많은 분들이 좋은 글과 인터뷰에 참여 해 주셨기에 가능하였습니다. 이에 참여 하신분들에 대한 감사의 마음으로 이번호부터는 참여하신 분들에 대한 간략한 글 소개를 올려 드립니다. 앞으로 많은 분들의 참여와 관심 부탁드립니다. 해당 내용을 보고자 하시는 분들은 카페 대문에 각 호별로 배너를 클릭하시면 다운로드 받아 보실수 있습니다.

15. 제15호: [기고] "정보보안기사/산업기사가 풀어야할 숙제 3가지" - 전주현
[인터뷰] 보안인터뷰 한국인터넷진흥원 - 박해룡팀장
[인터뷰] KAIST 사이버보안연구센터
[기업탐방] 정보보호인식주식회사 - 문승주대표
[교육센터] 부산글로벌IT 교육센터 - 유종우 선임

16. 제16호 : [기고] 법과 정책으로 바라본 개인정보보호 현주소 -전주현
[인터뷰] 금융보안연구원 -성재모 본부장
[인터뷰] 개인정보보호협회 -전진환박사
[기술문서] " 아래한글 악성코드 분석 " -안랩 침해대응센터

17. 제17호 : [인터뷰] 테크엔로우 -구태언 변호사
[인터뷰] 중앙대학교 김정덕 교수
[지면임대] 서울 상경기 - 이현우

18. 제18호 : [특별기고] 훌륭한 인증심사원이 되려면 -전주현 보안인닷컴 운영자
[취재기] 지역별 정보보호교육센터 제3권역 부산대학교편

19. 제19호 : [인터뷰] 사회가 요구하는 기술인식해야 -고승철 수원대학교 교수
[강좌] 쉽게 배우는 암호학이야기 -김지현 부산대 박사과정
[기고] 개인정보보호법 8가지 분석 -이재욱 필라아이티 부사장
[생각] 보안전문가에 대한 생각 - 최재규 인하공전 겸임교수
[서평] 제로데이 - 유인재 안랩
참여 해 주신 모든 분들에게 감사드립니다. -운영자 올림

보안인닷컴 e-매거진 참여 하신 분

지금까지 보안인닷컴 e-매거진 [보안人]에는 많은 분들이 좋은 글과 인터뷰에 참여 해 주셨기에 가능하였습니다. 이에 참여 하신분들에 대한 감사의 마음으로 이번호부터는 참여하신 분들에 대한 간략한 글 소개를 올려 드립니다. 앞으로 많은 분들의 참여와 관심 부탁드립니다. 해당 내용을 보고자 하시는 분들은 카페 대문에 각 호별로 배너를 클릭하시면 다운로드 받아 보실수 있습니다.

20. 제20호: [강좌] "쉽게 배우는 암호학 이야기" - 김지현
[기고] 미디어 콘텐츠 소재로서의 보안 - 임효식
[기고] 사용자 관점에서의 윈도우 8 보안 - 박광수
[기고] 정보보안기사 산업기사 첫 시험 시행 -전주현

21. 제21호: [인터뷰] "보안에 대한 투자를 능동적으로 수행해야 - 이경현
[기고] 3.20사고를 보면서 느낀 10가지 - 전주현
[기고] "쉽게 배우는 암호학 이야기" - 김지현

22. 제22호: [기고] SK컴즈 개인정보유출사건 첫 패소 - 류호찬
[기고] 전자금융거래 인증방법 평가 - 함손겸
[기고] 4월 보안이슈사항 정리 - 이강원

23. 제23호: [인터뷰] 정보보호전문가 CEO와 소통 잘해야 - 박춘식
[기고] 국내 인터넷뱅킹의 보안현황 - 함손겸
[기고] 지역정보보안 인력양성과 나아갈 방향 - 전주현

24. 제24호 [인터뷰] 선순환을 위한 정보보안 생태계 마련 시급 - 염흥열
[기고] 보안 = 보험 , 이젠 NO!! - 백진성
[칼럼] 정보보안기사 1회 시험 후기 - 전주현

25. 제25호 [인터뷰] ISMS는 정보보호의 시작이자 끝이며 예술이다. - 장상수
[기고] 사이버 사령부 사태를 바라보는 불편한 마음 - 고재호

참여 해 주신 모든 분들에게 감사드립니다. -운영자 올림

보안인닷컴 e-매거진 [보안人] 원고 모집

보안인닷컴에서 매월 무료로 발행하는 e-매거진 [보안人]에서는 보안에 관심 있는 여러분의 소중한 글을 받고 있습니다. 소중한 글을 보내주실 분들은 magazine@boanin.com 이나 boanin@naver.com 으로 보내주시면 검토 후 실어 드리겠습니다.

보안은 실천이고 문화입니다. 스스로 알고 있는 지식이나 노하우를 널리 알릴 수 있는 문화가 필요합니다. 보안에 관심 있는 분들의 많은 참여를 기다리겠습니다.

보내 주실 원고 소재는 다음과 같습니다.

- 최근 보안이슈 및 동향 -기술적 분석
- 우리 회사 보안 실천 사례
- 나의 보안전문가 도전기
- 내가 공부한 보안 이론
- 보안 솔루션 소개
- 보안관련 책 소개 및 후기
- 악성코드 및 바이러스 분석
- 해외 보안소식
- 보안 세미나 및 컨퍼런스 참석 후기
- 기타 보안전문가 인터뷰
- 회원들의 소소한 일상

이외에도 보안에 관련된 여러 아이디어 및 관련 글 보여 주셔도 됩니다. 원고 마감기간은 매월 20일까지입니다.

매월 초에 무료로 배포되는 보안인닷컴 e-매거진 [보안人]이 잘 성장할 수 있도록 보안인닷컴 회원분들과 관심 있는 기업의 참여를 기다리겠습니다.
magazine@boanin.com