AhnLab

安全月刊

2020.12 Vol.97

2020 年安全趋势

通过 AISF 2020 问答回顾今年的安全趋势

2020 年，人们所关注的主要安全问题有哪些?

提问的本质是通过询问不知道的事实，以获得相关知识，而提问的理由则是因为提问者需要这个问题的答案。那么反过来，通过问题可以看出提问者需要什么，如果同样的问题反复出现，则可以说很多人对该主题感兴趣。

10月21日至22日，AhnLab 在网上进行了“AhnLab ISF 2020虚拟会议”，并收到了许多预先注册的提问和现场提问。第1天和第2天的演讲者通过“Live Talk”环节，现场直播回答了其中的28个问题。

本文将对会议当时演讲者回答的28个问题中，选出10个参与者最感兴趣的问题进行回顾，并分类介绍今年对安全的主要需求和解决方法。

云：如何保护已成为主流的“云”

现在，云的采用已经变得司空见惯，以至于声称云的时代已经到来的主张似乎有些陈词滥调。很多企业处于各种原因（例如灵活性和便利性）采用云，并以各种形式使用云，例如使用两个或多个公有云的“多云”、混合公有云和本地部署（或私有云）的混合云。在本次的AhnLab ISF 2020虚拟会议上，已经正式： 随着云的快速普及，用户自然会非常关注云安全。

【图 1】云安全（来源：Shutterstock）

问：采用云时，云公司是否提供安全？

这个问题应从“在云环境中发生事故时，由谁负责？”开始。在传统的本地部署环境中，用户（公司）承担全部责任。但在云的环境中，云服务的提供商（Cloud Service Provider：CSP）和公司通过划分范围来负责安全。这被称为“共同责任模式（Shared Responsibility Model）”。

例如，在亚马逊云服务（Amazon Web Services：AWS）的IaaS（Infrastructure as a Service）环境中，AWS负责基础设施（例如硬件、网络和主机）的安全 。客户负责直接在基础设施上管理的领域（如应用程序）的安全。在采用云时，公司必须事先明确认识到自己承担责任的领域，然后设计和管理云。

问：采用云时，云提供商提供的安全还不够吗?

CSP经常直接开发各类安全程序并提供服务。这对云的配置及运营来说虽是最合适的， 但初期在功能方面存在着不足之处。如今通过不断地研究与更新， 在各方面都得到了改善。虽然根据企业的环境情况会有所不同， 但是使用CSP提供的安全服务是个不错的办法。例如像AWS Web应用防火墙 （WAF） 就是兼顾了安装简便和运营便利性的优秀的安全解决方案。

但是， 仅使用一个云提供商的单一云环境下虽无大碍， 但是在多云或混合云的环境下， 由于每个环境都得使用不同的安全解决方案，这会导致管理资源消耗较大，运营上也会出现困难。

由专业云安全企业提供的解决方案， 可以提供对多种云环境的单一管理能力， 以节约管理资源， 且可利用相同的用户经验来运营。此外， 专业云安全企业的解决方案还具备了提供多种功能， 以及发生问题时立刻提供支援的优点。

问：当在具有完整信息安全的本地部署环境中迁移到云时，部署战略是什么?

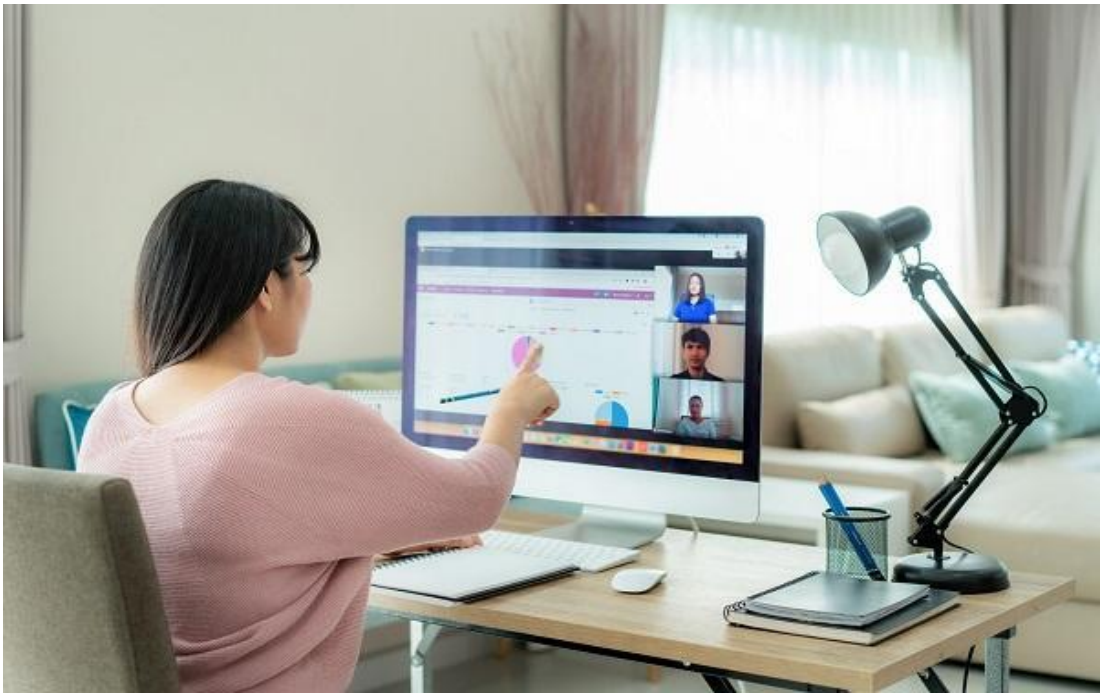
一开始就没有在云上构筑基础设施的企业，会在通常被称为MSP（Managed Service Provider）的合作伙伴的帮助下开始迁移到云。

如果企业已在本地部署的环境中使用安全解决方案， 并且已构筑了牢固的安全体系， 通常也会希望现有的安全环境也能在云上实现。但是， 他们马上就会明白这并非易事。虽然MSP对从本地部署环境迁移到云的工作经验丰富，但大部分都将重点放在了服务、应用程序、数据库等基础设施的配置。

最终， 在采用云时大多把重心都放在了迁移上， 而没有构建考虑安全的基础设施。想在基础设施迁移完成后再构筑安全体系， 但是由于云环境的差异和限制， 配置所需的安全级别变得困难。因此， 有必要配置从迁移初期开始充分考虑安全的基础设施。如果MSP的安全专业性不足， 那么最好的办法就是与拥有丰富经验且有能力提供安全基础设施方案的云安全企业合作。

无接触：由于新型冠状病毒，远程办公剧增

新型冠状病毒大流行带来的最大变化之一就是无接触（线上）趋势的出现。 为防止新型冠状病毒的扩散，企业根据情况采取了上班工作和远程办公并行的方式。但由于大多数的企业是首次引进远程办公系统， 所以面临着各种困难。在此次活动中，也收到了关于打造安全远程办公环境的问题。



【图 2】远程办公（来源：Shutterstock）

问：随着无接触时代的到来，企业该如何在变化的环境中为安全做准备？做哪些准备？

随着无接触时代的到来，许多事都发生了变化。但对企业来说，变化仅发生在工作环境和方式上，可持续发展以及提高生产效率的企业目标本身并没有改变。安全是为了实现企业的可持续发展而存在的，既然企业的目标没有变，那么安全的重要性和概念当然也不会发生改变。

但是，安全的方法论则有必要作出调整。假设无接触环境将长期存在，那么无接触环境下的安全不应仅是临时方案，而应该成为必要的响应体制。但没必要因为是新的环境，就非得引进全新的解决方案。

首先，应先决定在无接触时代所要保护的资产价值的优先顺序，优化现有的解决方案，并重新定位安全方法论和策略。同时，要巩固当前有效运营中的安全解决方案并修订指南，有必要检查在无接触环境中具有更高优先级的资产的安全级别。之后，通过补充（add-on/扩展）或重新配置（re-configuration）所需的部分的方向进行似乎是合理的。

问：远程办公时，安全方面的考虑越来越多。在VPN策略管理和整体安全以及解决方案运营的方面，建议的方案是什么？

通常，在远程办公时，为增强网络安全，会在内部网络中运行其他安全设备，并且系统访问权限被指定为内部使用的专用IP。此时，如果使用SSL VPN，就可以通过另外的IP进行内部通信。 关于SSL VPN的IP分配，AhnLab TrusGuard提供了两种方式。第一种是在设置的IP频带范围内随机分配，第二种是为每个用户分配固定IP。

如果设置了对IP的访问权限，建议在SSL VPN通信时，分配固定IP进行运营。在为每个用户分配固定IP的内部安全系统中，建议在现有的安全策略中添加用户的VPN专用IP。

此外，使用VPN时，用户身份验证和终端环境十分重要。对于使用VPN的用户，应通过双因素（2-Factor）身份验证或一次性密码（OTP）来允许访问，以此增强用户验证。此外，建议通过指定要访问VPN的终端来限制非特定的多个终端的访问。如果不是通过“指定终端”功能注册的终端，则AhnLab TrusGuard提供“防止VPN登录”的功能。

问：在中小企业在远程办公时，保护员工个人电脑的实际安全对策是什么？

由于新型冠状病毒的大流行，远程办公的需求急剧上升。但首先应该考虑的是，在新型冠状病毒出现之前就已经在进行远程办公。例如，位于建设现场办公室的电脑终端处于离总公司较远的环境中，我们有必要考虑在这种环境下如何构筑安全体系。

今年上半年，科学技术信息通信部门发表了《在家和远程办公时应遵守的信息保护守则》。主要内容包括防病毒软件（Anti-Virus：AV）、补丁管理、安全漏洞管理以及使用基于多因素身份验证的VPN等。中小企业不仅要应用VPN，也必须注意端点安全。但是，考虑到实际费用和运营上的困难，许多中小企都希望能找到兼顾成本效率和运营便利性的安全解决方案。

为满足这种需求，AhnLab在今年推出了基于SaaS（Software as a Service/软件即服务）的AhnLab Office Security。Office Security提供了基于云的管理环境，使用户可以轻松便捷地使用各种功能，包括恶意代码响应、安全补丁检查、漏洞检查和网络安全。有必要考虑引进一种在家办公环境中可以轻松便捷地使用的SaaS安全解决方案，而无需专业的安全人员。

端点：如何缓解端点安全复杂性?

端点领域从防病毒软件到EDR（Endpoint Detection & Response）和EPP（Endpoint Protection Platform）不断地在进化。但问题在于，为应对高级威胁而使用各种产品会加重运营负担。此次，也有许多参与者询问了提高端点安全运营效率的方案。

【图 3】基于AhnLab EPP的下一代端点安全系统

问：我认为EDR解决方案是由于现有防病毒软件的限制而开发出来的，那么EDR的不足之处是什么？

确实， EDR是由于现有防病毒软件的限制而出现的， 但EDR的出现并不是为了取代防病毒软件， 而是为了补充限制。

防病毒软件的主要功能是自动拦截或删除恶意代码。但随着新・变种攻击的持续不断以及利用社会工程学技术的威胁不断蔓延， 需要更精密的分析和响应。这意味着必须同时考虑企业的IT环境和可用性并从各种角度分析和响应事件和文件。防病毒软件负责预防（Prevention），EDR则负责响应（Response），两者形成互补关系，而不是替代彼此的领域。因此，如今的EPP和EDR是一个相结合的有机体。

有时候， EDR由于“只要有EDR不是所有的问题都能解决了吗？”的误解， 感觉比预期要差。此外， 还需要专业人员来处理EDR分析结果和信息。特别是，如果考虑与SIEM（Security Information & Event Management，安全信息和事件管理）、SOAR（Security Orchestration Automation & Response，安全编排自动化与响应）的联动，则需要更广泛的知识和经验。

为了解决此问题， 有必要通过制定收集信息的分类、轮询的周期和对象、分析点和通知的标准， 并长期建立以及逐渐完善响应恶意代码的方案。如果和AhnLab这样拥有丰富端点安全经验的企业合作，便可以更有效地完成此工作。

问：在端点安全领域使用多个解决方案时，可以采取哪些方案来缓解运营复杂性？另外，引进作为平台的AhnLab EPP时，客户能得到什么好处？

在端点领域使用多个解决方案时， 经常会出现因日志过多而发生问题的情况。与此相关， 需要基于平台和单一Agent来提高运营效率。

除了V3和EDR，AhnLab EPP 仅通过将许可证应用于已安装的EPP Agent，就可以构筑相应的插件。通过EPP可以便捷地集成运营“安全补丁管理（EPM）”、“个人信息泄露防护（EPrM）”、“检测和响应计算机漏洞（ESA）”。

AhnLab EPP的核心能力是通过有机连接多个端点解决方案之间的规则和响应措施，更有效地应对安全威胁。利用“AND/OR”条件将连接各产品的规则，以实现最佳的检测和响应效果。AhnLab EPP根据已设置的规则自动提供检测、监控和响应。此外，还可以远程收集 AhnReport（AhnLab诊断工具）以响应端点恶意代码并掌握异常迹象。

响应威胁：如何响应高级和新的威胁

黑客的攻击手法正在日新月异。除了最基本的传播新・变种恶意代码，还使用了针对人类弱点的社会工程学技术，并且攻击体系也在逐渐变得组织化。通过参与者的提问，可以了解到大家对于新威胁趋势和有效响应方案的需求。

【图 4】黑客们的安全威胁（来源：Shutterstock）

问：从长远来看，最重要的安全因素是什么?

从平台的角度来看， 安全威胁可分为端点、移动、云、物联网领域。攻击者会根据每个平台使用不同的攻击方法， 主要安全因素包括针对端点的电子邮件，针对移动的设备的短信和电话诈骗，针对云的帐户和权限管理以及针对物联网的漏洞。

特别是在端点的情况下， 管理系统的控制和供应链的攻击被认为是最具代表性的威胁。以前的网络攻击从寻找漏洞，制作并传播恶意代码，再到夺取信息都是由一个攻击集团完成的，但如今随着网络攻击的组织化、企业化和分工化，各个攻击阶段都由不同的组织负责，这使得网络攻击的经济效率也变得非常重要。

近来，企业为了提高业务管理及生产效率，正在使用多个管理解决方案或业务用程序，从攻击者的角度来看，只有当一次攻击造成尽可能多的破坏时， 才能提高经济效率。预计攻击者今后也将继续进行分工化的系统攻击，从企业的角度来看，帐户和权限管理以及可疑行为的监控的重要性也将越来越高。

问：我想知道如何有效响应利用电子邮件和附件的各种病毒和勒索软件。此外，还想知道Ahnlab的响应解决方案和防御原理。

恶意代码的主要感染路径是通过访问恶意网站或通过电子邮件。首先， 通过▲持续的漏洞补丁▲避免下载可疑文件▲拦截访问网站等方法来有效防止通过网站访问感染病毒。

而由于电子邮件大多用于业务目的， 因此很难防御。此外， 攻击者也正在增加电子邮件攻击的比重。要想防御电子邮件的攻击， 可以在电子邮件实际传递给用户之前， 先扫描电子邮件中包含的URL， 或是在虚拟环境中先运行附件，通过行为分析来判断该附件是否带有恶意代码。

应用这些响应方法的最具有代表性的解决方案是AhnLab MDS和AhnLab EDR。尤其是MDS，它可以将端点和网络有机连接，实现“多层”响应。如果将MDS的网络层响应（例如异常流量分析和拦截）和通过专用Agent的端点层响应（例如删除恶意代码和保留可疑文件的运行）连接起来，则可以构筑强大的勒索软件响应系统。另外，V3的勒索软件安全文件夹拦截未经授权的可疑进程的访问，并通过诱饵文件来预先检测并拦截勒索软件。

除此之外， 当预先无法拦截的恶意邮件传递给用户时， 这种情况下的附件大多是文档文件或脚本文件。此时，可使用基于特征码的静态分析来检测，或使用运行时分析行为的基于行为的检测技术进行分析。

结语

本文所讨论的问题是除了提问者的提问之外，还有很多与安全相关的工作人员都十分好奇的问题，AhnLab也在做出多方面努力来准确识别并应对客户的“痛点（Pain point）”，而不仅仅是回答问题。在新型冠状病毒导致很多企业经历着难以预测的变化的情况下，我们希望以上内容可以帮助企业在即将到来的2021年建立更加强大的安全系统。

要观看AhnLab ISF 2020虚拟会议重播，请访问AhnLab官方重播网页。有关现场提问和回答，请在“Live Talk”环节确认。

▶立即前往重播网页

AhnLab

安全月刊

https:// cn.ahnlab.com

https://global.ahnlab.com

https://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，
确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。
我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、
移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。
AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ahnlab.com