PKI自动化状况

PKI自动化状况报告

PKI几乎是所有技术方面的核心。它对于为用户、服务器、设备、IoT、DevOps应用程序和服务、数字文档签名及其他许多事物进行身份验证和签名至关重要。

但手动PKI管理很快就会不再可行。近期的Ponemon研究[1]显示，企业需要管理的PKI证书数量同比增长了43%。再加上证书有效期的不断缩短，企业将面临PKI证书管理的巨大压力。

为了更好地了解企业如何应对这一挑战，DigiCert委托德克萨斯州达拉斯的ReRez Research对全球400家企业中负责PKI管理的IT管理人员进行调查。总的来看，调查结果显示了PKI证书的混乱情况，但也展现了最优秀的组织如何在PKI管理方面遥遥领先。

企业需要管理的PKI证书数量增长了

43%

什么是PKI自动化?

我们为本次调查的受访者定义了PKI自动化，包括以下几个方面：

- 发现现有的数字证书
- 颁发新的数字证书
- 在数字证书即将到期前续订证书
- 在必要时吊销数字证书
- 实现代码签名的自动化
- 客户端证书的注册流程
- 身份验证（例如，用于文档签名）
- 实现扩展预配活动的自动化，例如进入LDAP和Exchange
- 与PKI管理相关的其他基础工作

1 2020年全球PKI与IoT趋势研究（Ponemon）

PKI的快速增长在引发

我们研究的典型企业目前管理着超过50,000个证书。最常见的证书类型是用户与服务器证书，其次是Web服务器、移动设备和电子邮件证书。企业管理的公共证书，即公共证书颁发机构（CA）颁发的证书数量，比内部的专用CA颁发的专用证书数量多三分之一。

典型企业目前管理着超过 **50,000** 个证书。

这一数量与前几年相比大幅增加，并且有充分的证据表明，企业在工作量管理方面遇到了困难。实际上，有三分之二的企业经历过因证书意外过期而导致的中断。仅在过去六个月中，就有四分之一的企业经历了五到六次这样的中断。

为什么?部分原因是工作量增加。近三分之二的受访者对管理证书所花费的时间有比较大到极大的担忧。然而还有缺乏可见性的问题。37%的企业用三个以上的部门来管理证书，从而造成混乱的情况。典型企业表示，多达1,200个证书实际上没有受到管理，而且近一半、即47%的企业表示其经常发现所谓的“恶意”证书——即在IT人员不知情或未管理的情况下实施的证书。这类问题公认的解决方案是PKI自动化，因此我们研究了企业的PKI自动化情况。

61% 的受访者对管理证书所花费的时间感到担忧

47% 的受访企业经常碰到恶意证书

37% 的受访企业有3个或3个以上的部门在管理证书

1 IN 4

在过去六个月中经历了5到6次与PKI相关的中断

我们的调查结果显示,大多数企业——即91%的企业至少在讨论PKI自动化。只有9%的企业表示没有讨论PKI自动化,也没有计划这样做。大多数企业,即70%的企业希望在12个月内实施解决方案。四分之一的企业已在实施解决方案或甚至可能已经完成了解决方案的实施。但这并不容易。企业列举的挑战包括自动化的高成本、复杂性、合规性问题以及员工和管理层对变化的抵制。

趋势

企业采用PKI自动化的常见原因:

1. 恶意证书
2. 为后量子计算做好准备
3. 证书有效期迅速缩短导致工作量激增
4. 所管理的证书数量快速增加
5. 远程办公趋势

痛点

推动企业实施自动化的安全问题:

1. 预配新证书的速度缓慢
2. 错误配置证书的倾向
3. 员工工作负担过重
4. 恶意证书太多
5. 错过证书到期时间
6. 在需要吊销证书时吊销速度缓慢,甚至失败

惩罚

不进行PKI自动化的负面影响:

1. 合规问题
2. 安全问题
3. 成本
4. 停机时间
5. 愤怒的客户或员工

目标

实施PKI自动化的企业希望:

1. 提高安全性
2. 提高合规性
3. 提高敏捷性
4. 提高生产力
5. 减少停机时间和成本。

顶层对比底层

我们提出了一系列问题,以确定每个受访者在各种PKI指标中的表现如何:

- 避免因证书意外过期而导致的停机
- 在必要时快速吊销证书
- 管理数字证书的效率
- 尽量降低证书管理不当而造成的安全风险
- 证书管理不当而造成的合规问题
- 尽量减少恶意证书
- 满足与PKI相关的SLA
- PKI颁发和吊销速度

我们根据表现的好坏为每个问题指定一个值(从正到负)。然后我们加总他们的分数。为了找出受访者在表现方面的差异,我们将受访者分为三组:

1 **领先者**

在上述指标中得分最高的组织。

2 **居中者**

在上述指标中得分居中的组织。

3 **落后者**

在上述指标中得分最低的组织。

之后,我们对领先者和落后者进行了比较,以研究这些差异并探讨领先者的不同之处在哪里。

领先者对比落后者

受访者非常坦诚地讨论了其所面临的PKI管理挑战。他们发现了恶意证书、意外的证书过期导致的中断以及许多其他问题。但并非所有企业都面临同样程度的问题。我们将回复分为三层，并对顶层和底层进行了比较。其中的差异十分惊人。

顶层的领先者表现更好。值得注意的是，三分之一即33%受访者更可能表示他们认为PKI自动化原本就很重要。领先者在以下方面的表现要好两到三倍：

- 尽量降低PKI安全风险
- 避免PKI停机
- 尽量减少恶意证书
- 满足与PKI相关的SLA
- 管理数字证书
- 颁发和吊销证书
- 合规性

另一方面，落后者因缺乏管理PKI证书的技能而遭到了严厉惩罚。这包括：

- 合规问题
- 安全问题
- 生产率降低
- 延误
- 员工过度劳累
- 企业客户流失
- 企业收入减少。

那么是什么让领先者成为领先者?我们可以从这些PKI领先者那里学到什么经验?

PKI自动化领先者的特征

PKI领先者对管理PKI证书所需时间的担忧程度是其他企业的两倍。这使其专注于PKI管理。其次，他们更关注恶意证书。第三，领先者认为PKI自动化对其组织的未来非常重要。也许这就是为什么他们已经实施PKI自动化的可能性比其他企业高五倍的原因。那么，有哪些经验教训，您应该采取哪些不同的做法？

西部荒野效应

当我们深入研究数据时，我们注意到了一个有意思的现象。我们发现，从纸面上看可能应该可以更轻松地管理PKI证书的许多企业往往把证书管理得更差。

例如，证书数量最少的企业更有可能经历与意外证书过期相关的中断。他们在各种PKI管理指标中的表现也同样都是更差的。

因此，这些“少量PKI证书”企业明显更加关注PKI管理，即使他们所管理的证书数量比大量证书企业低好几个数量级。例如，少量证书企业表示他们担心管理PKI证书所需的时间的可能性比其他企业要高出近50%。他们在PKI自动化计划下的证书比例也几乎是其他企业的两倍。

乍一看，这似乎很矛盾。然而，实际情况是这些小量证书企业在PKI管理方面还不够成熟。经常管理超过10万个证书的大量证书企业已经拥有非常成熟的证书管理方式，而少量证书企业的情况则类似于在西部荒野——没有规则，每个人都以自己的方式管理证书。

对于少量证书企业，这就像在西部荒野——没有规则，每个人都以自己的方式管理证书。

PKI自动化领先者的特征

PKI管理领先者还表明,他们对证书库存所承担的责任要大得多,他们给自己的评分比不太担忧的同行更低。然而,这些组织所报告的与证书相关的中断或恶意证书的情况更少,证明实际上他们做得比他们假设的要好得多。

自我评估悖论

另一个有趣的发现是最担忧PKI证书管理的企业之间的差异。我们发现,在客观上担忧企业的问题更少,但主观上他们给自己的评分更低。

以最有可能表示他们认为PKI管理具有挑战性的企业为例。这些企业最有可能表示他们在新证书颁发速度、意外错误配置证书和发现恶意证书以及其他证书问题等方面有比较大到极大的担忧,这种可能性是其他企业的三到五倍。

然而,他们所报告的实际恶意证书要少得多(只有不担忧企业的三分之二)。他们所经历的与意外证书过期相关的中断也要少得多(过去六个月中只有一次中断,而不担忧的企业则发生了三到五次中断。)

我们经常在与安全相关的调查中看到这种现象。正在发生的情况是,关注程度最高的企业最清楚自己的短处和失误,因此往往比关注程度不太高的企业更严格地给自己评分。然而,正因为关注程度高,所以实际上这些企业的表现要比一般不知情的同行好得多。

客观上担忧PKI证书管理的企业问题更少,但主观上他们给自己的评分更低。

我们的建议

随着验证期变短、加密标准持续变化，以及数字证书在整个组织的业务流程中的采用范围不断扩大，在整个PKI证书目录中使用自动化会带来显著效益。但是，公司在开始自动化之旅时应考虑哪些因素?以下是自动化可能有助于实现证书管理目标的步骤清单。

证书管理

识别
识别并创建证书清单。

修复
修复不符合公司策略的密钥和证书。

保护
采取颁发和吊销证书的最佳做法，以提供保护。对注册、颁发和续订流程进行标准化及自动化。

监控
监控新变化。

证书流程自动化

识别
识别无人管理或手动的证书流程。

采用
通过集中管理证书流程的软件，采用自动化。

监控
通过集中式可见性和控制度进行监控。

常见的证书流程

- Web服务器
- 设备身份和管理
- 代码签名
- 数字签名
- 身份和访问权限

方法论

德克萨斯州达拉斯的ReRez Research调查了北美、欧洲、中东和非洲、亚太地区和拉丁美洲的400家企业的IT专业人员，这些企业的员工人数不少于1,000人。受访者被分为IT主管、IT安全经理与IT专员。我们聚焦于为用户、服务器和移动设备管理数字证书的IT专家，并且我们调查了小型、中型和大型企业。

与DigiCert PKI自动化专家交谈，以评估贵组织的需求并讨论量身定制的解决方案。在此处了解有关如何开始自动化PKI部署的更多信息。