重要的按需提供原则

20 世纪 90 年代，机密性、完整性和可用性 (CIA) 确立为主要的信息安全属性，那时并未发生全球大流行，世界各地的员工还没有采用在家办公的模式。CIA 三要素的扩展属性已经提出，[1] 但尚未进行全面调查，因为网络专业人员已经并且在某些情况下仍然忙于应用这三个属性。如今，勒索软件仍然是一种非常常见的攻击方法，企业正考虑向员工提供永久远程办公方案。尽管 CIA 三要素始终是网络专业人员工作的核心，但仍然需要审计信息安全原则，确定哪些方面有发展空间。

员工在实体工作场所中办公，这就为按需知密原则奠定了基础，而该原则规定，一个人只能访问其角色需要了解的信息。现在，大多数员工都采用远程办公模式，这项原则的应用变得极具挑战性，因为员工不需要一直访问所有数据。现代数据泄露[2] 和内部人员威胁[3, 4] 算法的运行方式为此提供支持。就像保安会怀疑试图深夜进入大楼的员工一样，员工在奇怪的时间段或批量远程访问其当前任务集不需要的数据时也会引发关注。

为了进一步限制对用于处理数据的信息的访问，其中用户或系统有权访问的所有数据并非都是他们执行下一组规定任务所必需的，此时应遵循按需提供的原则。

定义按需提供原则

“按需提供”一词是指在确认完成下一组预先策划的任务不需要访问这些数据后，中止向一个或多个用户或系统授予的数据访问权角色或权限。

这是保密性和可用性原则，根据完成下一组任务仅需的特定类型的信息确定，前提是提前知晓这些任务。因此，也可以预先确定完成任务所需的数据类型，最后往往只需要角色或权限的子集即可。当前一组任务结束后，需要重新评估角色和权限，并将该原则重新应用于下一组任务。

按需知密原则

与按需提供原则不同，按需知密原则假设数据都是可用的，而不考虑手头的具体任务。按需提供原则变得越来越细化，侧重于提供在任何给定时间执行特定任务所需的数据（**图 1**）。

YIANNIS PAVLOSOGLOU | 博士，CISSP

是一位拥有 20 年丰富经验的网络安全主管。他是 KIBERNA 的创始人兼首席执行官 (CEO)，这是一家专门从事数据驱动的信息安全、数据保护和运营弹性服务的企业。他曾在两个国家成功担任首席信息安全官 (CISO) 一职，在流程目录和服务定义方面开展了开创性工作，保护了组织的安全。2019 年，他入选 (ISC)² 董事会，负责监督 CEO 的工作，2021 年和 2022 年被推举成为 (ISC)² 干事。

按需提供原则的细粒化为数据访问增加了时间因素，需要提前计划。角色和权限变得更加动态化。在分配和重新评估角色与权限时，不仅要基于用户的角色和职责或系统的权限，还要基于正在计划的下一组任务。假设大多数组织已经应用了按需知密原则，[5]从业者应评估按需提供原则的计划和应用将如何提高企业的安全性。出于此原因，需要研究 2021 年以来发生的网络事故，以及如果应用了按需提供原则，影响将会有何不同。

2021 年重大网络事故分析

战略与国际研究中心 (CSIS) 的数据集提供了自 2006 年以来发生的重大网络事故记录的时间表。[6] CSIS 主要关注对政府机构、国防和高科技组织发起的网络攻击，以及损失超过 100 万美元的经济犯罪。

在评估事故时，假设已正确应用按需提供原则，因此，每次攻击的受害者或被入侵系统在事故发生前本应已中止执行下一组任务不需要的任何角色或权限。这本应该使每个受害者或被入侵系统只能访问相对其请求或被授予访问权限的数据集而言更小的数据集。

分析侧重于审查 CSIS 在 2021 年报告的前 101 起重大网络事故的每一起，审查工作分两个阶段进行。第一阶段需要研究报告的每个重大事故，以了解公共领域是否提供有关该事故的足够的信息，以便就该原则形成意见。第二阶段侧重于分析有足够信息可供形成意见的重大网络事故。根据这些数据形成意见，即如果提前正确应用了按需提供原则，是否会限制攻击带来的影响（**图 2**）。

结果表明，在审查的 101 起事故中，约 15% 没有提供可形成意见的足够的信息。如果在攻击发生之前应用了按需提供原则，其中有 23% 的事故在影响方面不会出现任何差异。如果准确、主动地应用了按需提供原则，2021 年报告的事故中有 62% 的影响会减小。

在其中一些情况下，使用按需提供原则会导致勒索软件加密的数据集更小，存储的加密货币需要进一步的访问权限，并且虚拟私有网络 (VPN) 漏洞会造成有限的数据访问（需要进一步分配角色）。但是，在网络活动持续时间超过 3 到 4 年的情况下，若结果并没有什么不同，则可以假设受害者在此期间使用了所有访问角色。即使是时间较长的网络活动，尽管无法限制攻击的影响，但应用按需提供原则后，攻击者需要花费更多精力才能获取数据。攻击者需要密切监控授予受害者的权限，并且根据这些权限逐渐提取额外的数据。这些例子说明，根据要执行的任务限制对数据的访问是有价值的。

图 1

按需知密原则与按需提供原则的比较

按需知密原则	按需提供原则
用户只能访问其工作职能所需的数据。	用户只能访问其工作职能执行特定任务所需的数据。
根据用户的角色和职责，向用户分配对数据的访问权限。	向用户分配对数据的访问权限以执行特定任务。
根据工作职能的需求授予和撤销权限。	根据规定的任务授予和撤销权限。
根据用户的职责重新评估权限。	根据用户完成一组任务的情况重新评估权限。

有关原则的批评意见和缺点

尽管按需提供的原则具有优势，但现代工作环境中的所有任务并不都是线性的或者可以按时间排序。按需提供原则需要就处理或产生的信息预先策划好步骤。以某企业的首席执行官 (CEO) 为例，他想查看 10 年前的战略文件。若指定一个角色单独完成该任务，这将是不切实际的。该原则不能适用于现代员工队伍中的所有角色和等级。要解决这一问题，可以向办公楼中的员工授予对更大数据集的访问权。

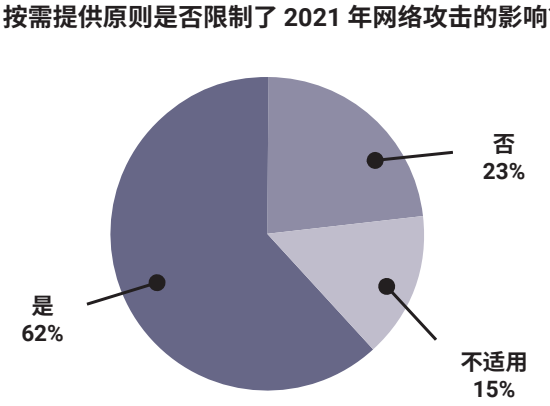
针对这项原则提出的第二种批评意见，即是认为它会扼杀创新。如果用户意识到他们可以将正在使用的数据与另一个数据集结合起来以提高效率，他们必须暂停手头的工作并请求额外的角色才能执行此操作。人类大脑的思维方式千变万化；因此，需要谨慎应用该原则，并且仅在出于充分理由保护特定数据集时才能应用该原则。为了促进创新，在集体讨论阶段，可以提前生成数据池并在有限的时间段内使用。

第三种批评意见认为，涉及的用户需要足够了解他们正在执行的任务，才能够描述执行这些任务所需的数据。再加上这样一个事实，即如果不经过深思熟虑就贸然放弃一个角色，可能会使任务完成工作面临风险，因此需要有技术真正娴熟的员工队伍，这是成功实施该原则的先决条件。在应用按需提供原则之前，必须确保员工了解他们使用的数据。

和其他信息安全原则不同，与限制重大网络事故的影响带来的回报相比，在对所需的数据以及组织内利用这些数据的人员分类（可能会出错）方面，按需提供原则带来了固有风险。尽管如此，在新冠肺炎大流行期间，大多数组织几乎都在潜移默化的影响下被迫这么做。因此，针对未来的员工队伍制定按需提供原则很有意义。

图 2

对 2021 年以来的 101 起重大网络事故的分析



真实示例

有这样几种资源规划系统，它们基于策略授予细粒化权限，仅针对特定的持续时间，并且通常具有完整性和信任的先决条件。例如，用于简化业务流程和降低复杂性的企业资源规划 (ERP) 系统不仅具有确保机密性的安全功能，[7] 而且还允许针对特定目的制定策略，例如：[8]

- **按需共享，其中组织必须共享数据才能开展运营**—这是按需提供原则的一个更通用的实例，根据进一步共享数据的方式授予对数据的访问权限。根据按需共享策略，该访问角色的任务是已知的，因此，按需提供原则同样适用。按需共享与按需提供是完全一致的，例如，接下来没有要共享的任务时，ERP 系统的管理员会撤销用户的访问权限。如果负责共享信息的人员在下一组活动中没有执行此类活动的任务，合理的做法是审查对象并删除其访问权，直到他们进一步需要时再授予访问权。
- **信任策略，其中数据仅在特定组织之间共享**—如何在对等级别的组织中应用按需提供原则的一个例子就是实施信任策略。当两个组织需要访问它们之间的数据时，通常会根据合同协议在特定时间段内实施信任策略。与其花时间调查员工更细粒化的任务，不如在组织合同规定的期限内授予对数据的访问权限。

- **完整性策略，其中只有特定人员可授权修改特定数据**—在确定谁可以修改数据以保证质量和准确性之后，可以更具体地应用按需提供原则。通常在用户不再需要修改数据的情况下，访问权限会被撤销，直至用户再次需要时才会授予。

凭借为特定目的制定策略的能力，各种商业 ERP 产品（包括 SAP、Oracle 和 Microsoft）向用例提供了在某种程度上使用按需提供原则的功能。除了 ERP，负责在其组织内设计策略的各方也可以考虑按需提供原则，但通常不会在任务的驱动下根据时间设定严格的期限。信息安全官、审计师和风险管理者等角色通常会指出，如果长时间不需要访问权限，就可以撤销该访问权限，然后在规定的活动即将开始时再次授予。在发生恶意软件或勒索软件攻击后，这样的讨论更为常见。

尽量降低勒索软件的影响

如果主动应用按需提供原则并以正确的严格程度实施该原则，则可以进一步降低勒索软件的影响。例如，假设一名员工成为第 1 阶段勒索软件有效载荷的受害者，第 2 阶段开始加密其文件系统中的文件。如果他们的访问仅限于执行下一组任务所需的数据，那么勒索软件对其文件的影响相应减小。而且，如果访问权限受到限制，则会有一组权限限制有效载荷可以访问和搜索要加密数据的位置。因此，勒索软件的影响将进一步降低，因为可供加密的数据会更少，并且这些权限将限制勒索软件有效载荷可以部署到的位置。此外，也可能有人认为，鉴于大多数第 1 阶段勒索软件是通过电子邮件传输的，如果通过电子邮件访问链接和文件不属于给定时间规定的一组任务，并且只要正确应用了按需提供原则，届时员工将免受勒索软件的进一步侵害。

结论

员工在办公室里办公，提供了建立信息安全原则的起点。面对全球新冠肺炎大流行，有必要重新审视哪些数据可用以及提供给谁。按需提供原则提供了一种限制重大网络事故的影响的方法，因此有助于管理远程办公的员工。为了使该原则有效，必须根据完成一组任务所需的数据预先策划需要哪些角色或权限。这可能导致撤销剩余员工角色并在撤销后才发现需要那些角色的风险。尽管需要思考在执行任务时应保留哪些角色，但此原则提供了一种无可争议的方法限制事故发生时造成的影响。

尾注

1 Parker, D. B.; *Fighting Computer Crime: A New Framework for Protecting Information*，John Wiley and Sons，美国，1998 年
2 Guevara, C.; M. Santos; V. Lopez; "Data Leakage Detection Algorithm Based on Task Sequences and Probabilities"，*Knowledge-Based Systems*，第 120 期，2017 年
3 Ye, X.; M. M. Han; "An Improved Feature Extraction Algorithm for Insider Threat Using Hidden Markov Model on User Behavior Detection"，*Information and Computer Security*，2020 年
4 Lv, Q.; Y. Wang; L. Wang; D. Wang; "Towards a User and Role-Based Behavior Analysis Method for Insider Threat Detection"，2018 年网络基础设施与数字内容国际会议 (IC-NIDC)，美国电气和电子工程师协会 (IEEE)，中国，2018 年 8 月
5 国际标准化组织 (ISO) 标准 ISO 27002:2013 *信息安全控制实践准则*将按需知密作为指导访问控制策略定义的原则。
6 战略与国际研究中心 (CSIS)，"Significant Cyber Incidents"，*https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents*
7 Thuraisingham, B.; 数据库和应用程序安全，*Integrating Information Security and Data Management*，Auerbach Publications，美国，2005 年
8 She, W; B. Thuraisingham; "Security for Enterprise Resource Planning Systems"，*Information Systems Security*，2007 年