Interested in learning more about security?

SANS Institute InfoSec Reading Room

Lateral Leadership and Information Security

In almost every company, a defined hierarchy, job description and organizational chart defines who is in charge of a certain issue. Nevertheless, most employees will recall situations, in which teams without a predefined leader had to collaborate. Being able to navigate these settings effectively is extremely helpful for the information security professional. More often than not, different departments and heterogenous groups have to work together to improve the security posture of a corporation. An open mind, real inte...

Lateral Leadership and Information Security

GIAC (GSEC) Gold Certification

Author: Stefan M. Krampe, stefan@krampe.global
Advisor: Manuel Humberto Santander Pelaez
Accepted: June 12, 2017

Abstract

In almost every company, a defined hierarchy, job description and organizational chart defines who is in charge of a certain issue. Nevertheless, most employees will recall situations, in which teams without a predefined leader had to collaborate. Being able to navigate these settings effectively is extremely helpful for the information security professional. More often than not, different departments and heterogenous groups have to work together to improve the security posture of a corporation. An open mind, real interest in the ideas of colleagues as well as a reasonable distribution of responsibilities and tasks is needed. Well known principles in information security are actually quite well suited for these circumstances.

Disclaimer

If specific products are mentioned, it is to help make examples more lively and does not imply that one is inferior to some other product. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

1. Introduction

Since the 1990s, scientists became especially interested in situations in which employees are interacting in groups without definite leader. Many organizations and companies are making use of this kind of workgroups consciously or unintentionally. But they create considerable amount of friction, if involved staff works unfocused or against each other. With proper guidance and suitable communication, a workgroup without apparent leader can create excellent results (Fisher, Sharp & Richardson, 1998). Some authors even stress the advantages and positive dynamics of these environments (Strathausen, 2015). Nevertheless, in the perception of most organization, workgroups of this kind are not considered the regularity.

1.1. Lateral Leadership

Usually, the perceived standard situation for acting as a leader is the property to be in a superior, elevated or distinct role with authority. This authority is derived mainly from the position one holds within an organization hierarchy. But leadership can be more or less independent from authority and derived from other personal qualities.

1.1.1. Leadership with no authority

Examples of managers who are effectively powerless regardless of their position are abundant, and most people know powerful persons who are technically not in charge of something. The underlying problem is, that people tend to react repulsing to orders and commands. It does not motivate being forced to adopt new attitudes nor does it persuade someone with a lasting effect. Just telling somebody to accept something new implies the old way was inadequate and can even be understood as an accusation. Additionally, instructions typically need some level of detail to make sense. Subsequently, people feel left out of the creation process if they are just confronted with the finished end result, and consider this an assignment of less responsibility. There are still valid reasons for leading by issuing orders, e.g. if operations are under very tight time constrains or responsibility can't be transferred or shared. While military operations are a classic example for this, there are different examples for lateral leadership situations:

- Imagine an information security manager working in the headquarters of an organization, which has business units with a considerable amount of autonomy. Maybe the branch offices reside in different legislatures, which may even lead to different needs in infrastructure and/or integration with third parties. Often, these locations are not only separated by a geographical distance. They also tend to be far away from the head office figuratively speaking and may therefore have relatively strong leaders, and possess their own IT department. Other examples are healthcare providers who also offer education services, logistics companies who have a project/individual business stream, but are also subcontractor to a national postal service or

universities who have a fully-meshed campus network, but largely independent research departments. Network administrators employed in the branch offices are not the direct employees of the headquarters manager and she or he does not have direct authority to give orders. This means in theory, if she or he wants something done or changed in this setting, she or he would have to go to his C-level officer, who in turn gives an instruction to the branch manager, who in turn gives the instruction to his network team. Obviously, this is time-consuming and not suitable for day-to-day-operation. It creates friction when an order issued by the C-level officer is being understood as a complaint and lack of appreciation or information is somehow altered during the detour.

- Another example might be a small company that has no dedicated information security staff, and the chief information officer calls a group of administrators together with the rather unspecific task to "improve security". A lot of people who have experienced a situation like this will report that the original initiator of the meeting won't be attending and does not give any more specifics, nor will there be a defined leader.
- There is a widely-circulated story that in the early days of the World Wide Web the web site of Microsoft was running on Red Hat Linux and Apache instead of Internet Information Server and Windows, because the web administrators did not consider it a secure solution. Bill Gates was allegedly very upset about this and made the web administrators and the software developers collaborate to benefit from each other. This is an example of a missed opportunity to execute lateral leadership, because either the web administrators or the software developers could have approached the respective other ones to suggest sharing ideas for improvement.

It is generally observable that groups without a designated leader do not work effectively in most cases. This means that time and money is wasted and companies do not benefit from the efforts. But there is a pretty good chance that ineffectiveness can be overcome. In the following chapters, ways of improving the results when working together in complex organizations and groups without apparent leader are discussed.

1.1.2. Finding solutions for complex organizations

The science around this topic is called lateral leadership. It encompasses an assessment of usual problems, the analysis of reasons for shortfalls and suggestions for navigating lateral leadership situations successful. This is not some kind of technique or recipe, but a way to get colleagues to think along and collaborate effectively. Three concepts are central to lateral leadership. The first proposal is to improve communication within the workgroup:

- Don't point fingers, be a consultant instead. It is recommended to improve personal skills in order to inspire colleagues. Trying to adopt the perspective of others helps understand their perspective.
- Don't consider your ideas to be perfect, but put real interest in the opinion of others. If the contributions of other participants are accepted unbiased into

the discussion process, the outcome will certainly improve. This is especially true if the resistance within a workgroup would otherwise derail a project completely.
- Don't try to enforce becoming a leader. Prefer to put your efforts into building a good working relationship. Company policies permitting, organizing a function to socialize with participants is a recommended idea.

Most important is a real change in attitude. Following the recommendations like a manual won't work if no new mindset is adopted.

The second basic idea is: It is very inefficient, and most of the time impossible, to change other people. So, instead of trying to persuade colleagues to support someone else's ideas about what is supposed to happen in a workgroup, everybody should be invited to contribute to the workgroup. This translates to the following suggestions:

- Include everyone in plans and discussions about the project and organization of the group. In particular, shaping a well-structured purpose is extremely important for the survival of the project. It is worth underlining that the purpose of a workgroup is at times not sufficiently outlined by the initiator. For instance, is the goal of a workgroup to create a recommendation (a piece of paper), or is the goal the implementation of system (a tangible result)? If the purpose is not clear, the workgroup will end up unfocused and discussions will be ineffective. Every aspect of the group collaboration should be agreed on and every conflict should be addressed.
- Never tell or command something. Every contribution to a conversation should be starting with a truly open question to every participant. "Don't you think we should get rid of Tomcat because of the flaws in Java?" is not an open question. "What is your opinion about the security of Tomcat, especially when thinking about the flaws in Java?" is a genuine open question that invites everybody to contribute. If a cause needs solid support, relevant data should be gathered and presented. Should that be impossible, it may indicate that a flaw in the project has been detected.
- Never assign blame to somebody. If a situation needs improvement, it should be underlined that the situation itself is to blame.

Thirdly, participants of workgroups want to contribute actively to the reach the defined goal. This leads to the following proposals:

- Avoid exclusive assignment of routine tasks (or assignments who lack some level of challenge) to one single person. Distributing demanding tasks makes participants feel important and relevant, thus creating a productive group dynamic.
- The collaboration in a group should make its participants feel needed and important. Every contribution should be honored and included in the process.
- If educating colleagues is necessary, it should never be in the sense of lecturing. This would tell a participant that he lacks a certain knowledge which is therefore a personal deficit. The idea of every education, if the term is used in the light of lateral leadership, does always mean that colleagues

will be empowered to make fully-informed decisions by having detailed knowledge of a certain subject.

The following sections will describe how these more abstract recommendations can be adopted to the domain of information security.

1.2. Challenges in information security

The challenges in complex organizations and workgroups without leader have already been discussed in a conceptual way. Most professionals occupied in the information security domain will probably recognize some of these properties from their work experience.

1.2.1. Identifying issues

In addition to the challenges arising from workgroup collaboration, the domain of information security has its own specifics. A frequent observation regarding information security is, that the subject is not at the center of everyday operations. Often, it is even expected to work quietly and invisibly in the background and protect the company data, assuming the task is done by simply installing some piece of technology or software. If the need for (re-) evaluation, changes and updates with impact to the business processes arise, not everybody concerned is necessarily aware of the priority and criticality of the topic. The task of changing that attitude rests often on the shoulders of the persons in charge of information security. Getting additional stakeholders to collaborate is not a fast-selling item. Somebody from accounting is probably not immediately motivated to join an information security meeting, even more so if active participation is expected.

1.2.2. Determine the need for techniques from lateral leadership

This opens the field to apply some form of lateral leadership. If a project faces resistance, or if friction within a project is detected, it indicates that an opportunity for lateral leadership has already been missed. The need for leading without authority becomes greater if participants come from different departments and levels of seniority. As mentioned earlier, this is also true if only the assignment or mandate came from a senior manager who afterwards does not attend at all. Likely, seasoned information technology experts, and those concerned with information security will recall that these descriptions apply to almost every project they supervised.

1.2.3. Getting from diverse requirements to practical solutions

If lateral leadership is executed with excellence, a powerful workgroup dynamic can be created. Ideally, the goals of the workgroup are clear and everybody can share her or his view on every challenge. But at the same time, this does not necessarily result into a practical solution.

For instance, imagine[1] a company that manufactures hip replacements globally, and wants to improve information security after incidents have been detected. A workgroup consisting of delegates from information security, IT operations, each global region, as well as from departments like accounting, manufacturing and human resources has been called together to discuss information security. One member of the group emerged to lead the group. Everybody has agreed that the security posture needs improvement. But the business units from around the world have very different requirements. While in the U.S., the hip replacements are basically sold to hospitals for implantation, some countries in the E.U. require pre-clearance of the surgical procedure with the health insurance and the bill goes directly to the insurance. The U.S. operations wish to have strong protection of their intellectual property and also have to comply with F.D.A. regulations concerning minimum security requirements. On the other hand, the E.U. business unit is required to establish a full-meshed VPN connection with the health insurer's datacenter. While there is overwhelming appreciation for everybody's positions and requests, it is unclear to the workgroup what solutions to propose.

The next chapters will give answers to these questions. The topics range from what can be done if one single security policy is impossible to create, through to how different technical requirements can be met, ending with how information security operations can look like under these circumstances. It will therefore serve the individual in a lateral leadership situation as reference and orientation. It outlines what to recommend when faced with difficulties to come up with feasible solutions.

2. Security policies for diverse environments

The first subject to discuss when dealing with practical solutions for security measures is the creation of policies, procedures and guidelines. This step comes after reaching consensus for risk assessments and resulting countermeasures.

2.1. Priorities in policies

Even though a consent for policies is also desirable, sometimes priorities and assessments diverge widely. At this point, an attempt to cover different policies per subdivision for the same underlying topic should be made. There are two possible approaches, but variations may also be likely. Firstly, the separation between mission, policy and procedures can be used to support diversity in the company. The mission can and should be created on the top level of the organization. Policies and / or procedures can be the responsibility of subdivisions. Another possibility is creating templates or minimum requirements for policies. This can be especially efficient if templates can be used by subdivisions with only small or no changes. Any preparation that reduces the workload for colleagues will usually be well received. Any stricter or more detailed policies could still be added if that wish arises.

[1] The example is fictitious. All resemblance to an actual company or occurrence is coincidentally.

2.1.1. Getting to know the company

In addition to the core task of a detailed problem assessment with information security in mind, noticeable knowledge of the inner workings of an organization usually creates tremendous respect from other departments. What is (and what's not) possible to achieve with help from subdivisions and departments makes every project much more predictable. Unsuccessful and frustrating attempts can be avoided that way.

2.1.2. Coordinating with departments and headquarter requirements

While the support of diversity in a complex organization is a way to advance projects effectively, the view from the headquarters management is often different. A certain pressure to reach a homogenous solution is at times present. One way to balance these needs is the continuous exchange of information regarding policies and procedures. Best practice examples from the departments can be pointed out and implementation of these examples can be shared and encouraged. Another way to get one accepted solution for every subdivision is to delegate the creation of policies to the subdivision. Every participant of the workgroup is responsible for one subset of policies and coordinates with the other colleagues. These policies don't feel like being imposed, because they are coming from peers on the same level. At the same time, participants know the problem of having to accept regulations conceived by someone else, since they do the same for their counterparts.

2.2. Contingency planning without central facilities

One central example for policies in diverse environments are different requirements for business continuity across departments or subsidiaries. It is often difficult to find a consensus across branch offices to agree on one single business continuity plan (BCP) and one single disaster recovery plan (DRP). Additionally, the assessment of the headquarters might be once more different. At times, the recovery times desired by the subsidiaries are much shorter (and the associated costs much higher) than those determined by the headquarters (and vice versa). If either document is not considered an assistance for the departments, it will sink into obscurity and has no benefit at all.

2.2.1. Distinction between BCP and DRP

One elegant approach is to make use of the distinction between BCP and DRP. The BCP includes items like priorities and responsibilities, key risks and the emergency recovery process, which can be expressed as high level descriptions. The BCP can thus be created by a central entity without or with little consultation with the subdivisions or lines of business. The DRP can be written by the subsidiaries or departments.

2.2.2. Shape a common business continuity plan framework

A second option is the creation of a BCP framework for the entire organization. The framework can be the foundation for different BCP varieties in the

subdivisions. This framework consists of a questionnaire or manual and a BCP form. The BCP questionnaire or manual tells the user on how to assess the exact need for business continuity and how to write the BCP. The empty BCP is like a form with predefined sections that needs to be filled in. The items of the BCP become requests for analysis and catalogs of questions to be conducted and answered by the subsidiaries. For example, the instruction for the "Risk Assessment" section could read: "Please list all incidents from the following table, that would cut production by half or more …". The result is a different BCP for every subsidiary or department, but the structure is consistent and the contents is comparable. Senior management frequently still wants to have a say at some point, so a review process has to be implemented as well.

2.2.3. Align disaster recovery plans to an agreed minimum

After generating one single BCP or at least a common BCP framework, the DRP can take different views into account. It is suggested that the broad outline and sections of a DRP has an agreed form as well. This is equally intended to ensure consistency and the ability to compare documents. Procedures and guidelines are best created by the concerned entities, but collecting a copy and filing it centrally for regulatory reasons might be sensible. Also, dependencies between departments and subsidiaries have to be considered, meaning that some level of coordination and guidance might be needed.

2.2.4. Benefits from distributed contingency planning

While seemingly making contingency planning more difficult, this approach empowers all contributors, regardless of the position in the organizational hierarchy. This is a direct implementation of lateral leadership suggestions. It will therefore increase the awareness for business continuity, disaster recovery and the associated planning and documentation. The likelihood to derail such an important project will decrease significantly and benefit the entire organization tremendously. Needless to say, a written documentation for further reference is recommended. The goal is that that the binding nature of the reached accord is understood by everybody.

3. Defense in Depth in complex organizations

While the creation of policies and guidelines is a crucial first step, it is by tendency rather inexpensive because of the theoretical nature of the task. Once policies have been written, the specific implementations have to be prepared. Usually, that is the point where purchases have to be made and employees have to be hired. When doing so, a homogenous system landscape is a desirable goal. It keeps costs down and makes administration easier. But achieving uniformity by forcing an incongruous implementation upon an existing corporate structure will very likely backfire. In terms of lateral leadership, it gives the affected people a (unintended) feedback that they have done something wrong in the past. So, neither allowing a completely fragmented implementation nor a centralized, homogenous

solution is ideal. Layered protection to secure the company data is a very useful tool to accommodate the different implementation requirements of a complex organization. Every layer of the so-called Defense in Depth can be adjusted to specific needs in different divisions, departments and/or branch offices. In this chapter, properties of complex organizations will be discussed first. After that, the resulting implications for layered protection are described.

3.1. Differing risk assessments and various solutions

Being in a leadership role in a complex organization is quite challenging. An important element of successful collaboration in a lateral leadership situation is the ability to take every opinion into consideration. A detailed understanding of the company structure does help immensely with this task. This does also include identifying general business risks and ways to address them, in addition to the more technical standpoint of an information security professional.

3.1.1. Explore all options and respect different priorities

This understanding leads to the realization that almost no one who makes a claim concerning business needs is doing so just to derail a project, or to achieve some destructive goal. All departments have organized their procedures to support their tasks in a more or less optimal way. All change poses the risk of additional workload and is therefore met with skepticism. To balance the need for adequate protection, all possible options for layered protection have to come on the table, to be prioritized by all workgroup participants. Different expectations, experiences and other constrains should be taken seriously.

3.1.2. Prefer solutions with proven performance

To keep businesses up and running while implementing information security, software with proven performance and an excellent history should be chosen. Though advanced technology is very well suited in special circumstances and environments, a robust environment should be preferred. Some security software, or hardware respectively, is industry standard and very well understood. This includes costs and features as well as limitations. Other technology is still rather experimental, does not scale well or has no flexible licensing options.

3.1.3. Prepare for incremental implementations and iterations

Furthermore, efforts and costs are serious obstacles for the approval of funds and other resources for a project. The attempt to realize a comprehensive solution in a single step overwhelms even large corporations. A vivid paraphrase for this is "Building a bridge halfway across a river would not pass this test. Building a bridge half as wide all the way across the river might." (Fisher, Sharp & Richardson, 1998) The successful setup of one working layer of protection should have priority. Starting an attempt to address every layer of protection simultaneously, resulting in no protection at all for a prolonged time, is much worse.

3.2. Layered protection

After the discussion of topics with focus on decision-making and project management, guidelines for specific implementations are desirable. The concept of layered protection supports solutions in complex organization and lateral leadership situations quite well.

3.2.1. Tailoring layered protection to enterprise needs

This is because Defense in Depth and layered protection has the fundamental principle, that each layer should be independent from each other. For the most part, it helps to stop an incident from happening, even if one layer of protection fails. But additionally, it has the advantage that the layers can also be configured independently. The creation of policies and procedures has been covered in the previous section. Resulting from these documents, implementations and responsibilities can vary. Especially the question whether to create a central facility for some task or to distribute it to local entities or subsidiaries makes a big difference. If local staff in subsidiaries is responsible, it usually ensures a nimbler response. As experience teaches, local staff may become unfocused when colleagues with seemingly more important concerns literally stand in the doorframe to press their own requests. On the other side, centrally organized implementations tend to be more focused. At the same time, central solutions usually mean that people involved have to rely solely on documentation and information not collected by themselves. Reading, understanding and transferring this information to create a solution may take additional time and is subject to inaccuracies.

3.2.2. Benefits of layered protection for efficient workgroup collaboration

It is once again important to note, that centralized solutions may jeopardize cooperative behavior from colleagues in the periphery. At the same time, inhomogeneous systems may not reach the desired performance. Two dimensions in the following chapters are usually independent: The workgroup that creates the concept for a specific measure should respect all ideas of lateral leadership and include all stakeholders in a cooperative manner. On the other side, the resulting implementation has to reflect technical and organizational requirements. Additionally, this dimension has to include considerations for efficient system operations. Therefore, support for central or distributed configurations should be kept in mind from the beginning, especially when selecting specific vendors or products. The directory service Active Directory from Microsoft is a good example for a solution that combines central management capabilities while at the same time allowing delegation of administrative tasks on lower hierarchy levels (Organizational Units). Then again, if some layer in the Defense in Depth is considered extremely critical (like the company firewall), a need for granular administrative access is most commonly obsolete (but distributed access to statistics or logs could be helpful).

4. Protection and incident response on different enterprise levels

The above-mentioned ideas behind Defense in Depth are essentially abstract concepts. If guidance for distinct measures complementing Defense in Depth is needed, the catalog of Critical Security Controls (CSC) is an excellent reference. CSC are tangible recommendations, which look at the same problem from a more hands-on angle than Defense in Depth. This chapter addresses the issue how CSC can support complex organizations. Effectively, that boils down to the question whether a measure can best be implemented in a central or distributed way. It is worth underlining that even if a central approach for the implementation is chosen, the planning should still be done in a cooperative way that respects all recommendations for lateral leadership. Therefore, the following suggestions for the implementation include arguments for driving a conversation in a workgroup in the planning stage forward.

4.1. Driving Critical Security Controls forward

CSC is a best practice suggestion from industry experts around the world. It helps approach the problem of defending against cyberattacks in a standardized and structured manner. At the same time, each CSC topic can be aligned to the centralized or decentralized structure of a complex organization. All considerations concerning central versus distributed implementations need to be made for each defense method separately.

4.1.1. Using CSC as a common agreement

Referencing CSC can be helpful if the necessity for a measure is disputed or the merit questioned. Underlining the history and the broad contribution to CSC is very helpful. Each of the controls already comes with a set of reasons, why it is a smart move to implement it and addresses a known attack. So, when someone has to do some advertising, it is possible to resort to numerous publications. While some effort is needed while implementing CSC, the goal is to support the installation of software, hardware or appliances along with the enactment of procedures. Obviously, these systems need maintenance and are by no way a fire-and-forget solution. But a huge amount of annoying routine tasks can be done automatically. Additionally, they usually allow to measure performance and create meaningful metrics and nice reports. This enables decision makers and superiors to get something in hand that justifies the investment and illustrates improvements. Implementations should always be deployed to address threads, which have been identified in collaboration with all stakeholders.

4.1.2. Implementing CSC

Not every item of the CSC is either best implemented centrally nor is a distributed system ideal. The following list weights the benefits and drawbacks of each approach.

- Inventory of authorized and unauthorized devices
  Unauthorized devices on the network are a considerable risk. They are usually unmanageable by the company and bring completely unknown software and hardware, which could perform malicious activities. A central implementation of the inventory is preferable, because it gives a possibility for oversight. There might be resistance, especially if local administrators ignore the problem and have the standpoint "in my network, impossible!". Therefore, in addition to setting the system up, sufficient help and guidance in addressing the problem of detected devices is necessary. After some time and routine has been established, it will be most efficient to send alerts directly to local administrators who can deal with the problem and only report back.
- Inventory of authorized and unauthorized software
  Authorized software needs to be maintained and up-to-date to be secure. Unauthorizes software might pose a risk to the network, either because it is malicious from the beginning or it is not updated and can be exploited. Giving end users the right to install software does seemingly reduce workload to the help desk, and increases user satisfaction. Educating administrators about the involved misconceptions and risks is an important first step. But it is equally important to implement an easy way for the end user to install additional software, when privileges are taken away. There is decent software available, which implements something like an online shop for software combined with a workflow for installation approval. It is noteworthy that the installation of software creates more and more licensing issues. Legal liability for this usually rests with the parent company, which makes a central installation mandatory. Otherwise, distributed installations are also imaginable.
- Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers
  Many default configurations are not secure or not as secure as desired. This includes anonymous logins, lack of encryption and unnecessarily enabled modules, just to name a few. The necessary configuration changes may be considered a pointless overhead. When considering whether a central or distributed approach might be sensible, it is worth considering a central approach in educating the involved administrators, who in turn might be located in the departments. The success of enforcing secure installations depends on whether an agreement about proper procedures has been reached.
- Continuous vulnerability assessment and remediation
  Protecting against vulnerabilities is never completed. As soon as a new vulnerability is detected, it has to be addressed in a structured, timely and efficient manner. When planning meetings or some other form of periodic communication, this should be a mandatory item on the agenda. Also, procedures for immediate preventive measures should be in place. Competent assessment of information regarding vulnerabilities is complex

and wide-ranging knowledge is needed. The origin of an alert to trigger remediation activities, and to give additional advice, is therefore preferably a central entity.

- Controlled use of administrative privileges
  The use of unprivileged user account does limit the extend of a successful attack to a host or user big time. The attack might even come to nothing. Gaining privileged access to a user or system is a huge problem, because illicit changes to the system and network can be performed. The biggest obstacle will be to have everybody agree on this. After extensive education of responsible personnel, distributed assignment of administrator rights is possible. It is advisable to have written and signed delegations, to make a point for the seriousness of the matter and to determine legal liability. This is very common in the business departments, where power of attorney and the like are also delegated to subsidiaries.
- Email and web browser protections
  When using a browser, or receiving emails, systems are inevitably at the forefront of information security with direct information exchange with the outside world. A focused approach to secure these two applications can make the network much more secure. While an agreement on the subject should be reached, a distributed deployment is possible and might be the more flexible solution.
- Malware defenses
  Malware is one of the most common threads to information security. This has to be addressed by anti-virus products at the host and network/perimeter level. Additionally, host-based intrusion detection systems can detect malware activity. While malware defense on devices with traffic filtering functions (e.g. mail gateway, web proxy) are best administrated from one workgroup alone, installation and maintenance of host-based anti-virus and IDS systems might be implemented most efficiently by distributed administrators, who are mentally and physically close to the systems.
- Limitation and control of network ports, protocols, and services
  If only a limited number of protocols, hosts and ports are exposed to an attacker, the more difficult it is to compromise a system. This does not only include internet-facing (e.g. DMZ) hosts, but also high-risk and vital systems on the internal network. Organizing these rules is a pretty critical task and are best assigned to one central workgroup, and implementation should only be distributed to local administrators if a stringent (but cooperative) oversight can be ensured.
- Data recovery capability
  The possession of a working and secure set of data backups is a last and generic defense against any kind of incident. The idea is to be able to revert to a working configuration after a disaster in a timely fashion. Usually, (local) administrators with excellent knowledge of the systems are the best colleagues to implement and test recovery procedures. Nevertheless, regular reports should be requested by a central authority. To avoid common

mistakes when planning and implementing backup procedures, a central expert should evaluate the plans in the departments.

- Secure configurations for network devices such as firewalls, routers, and switches
  Thorough planning of the network structure and a flawless implementation is the very first step to a secure system. Usually, enterprise growth or other changes make adaptions necessary, which should be executed with the same care. If a company does centralized purchasing, it is optimal to use this circumstance to pre-configure all network equipment before sending it out to the locations. Otherwise, the configuration should only be done using detailed check lists, which have been created and/or reviewed by qualified professionals. Sometimes, a combination of both approaches is best for a given organization.
- Boundary defense
  Internet-facing networks and systems are the ones which can be easily compromised by an attacker. Additional safeguards should be implemented here. Aligned to the subject of malware defense in central systems, this task should be addressed by one special workgroup alone. However, heterogenous requirements from subsidiaries pose a challenge for a central administration. In most cases, improved functionality or flexibility (e.g. allowing additional network traffic or remote access) is associated with increased exposure of internet-facing systems and an elevated risk. It is essential that a predefined, agreed protocol is in place that controls the decision-making when balancing functionality and associated risks.
- Data protection
  Siphoning data outside the company network is a risk for confidentiality and intellectual property. It is preventable (sometimes not entirely) by numerous measures. While some technical solutions can only be implemented in central systems (like mail gateways), other protective measures can be efficiently delegated to local staff (e.g. blocking thumb drives and DVD creation).
- Controlled access based on the need to know
  Confidentiality requirements demand that information is only accessible, if an employee has a valid reason for it. This does also limit the scope of an attack if corruption is only possible to the accessible data. This can very well be managed by local staff, but a written consent about the procedures and security implications is necessary.
- Wireless access control
  Wireless access poses an increased risk compared to wired networks because the attacker might be outside company premises and physical safeguards are useless. Depending on the exact impact of a breach, the authority over wireless systems might differ. If a wireless network only connects to some kind of extranet, local staff might be all right for management. Should sensitive information (e.g. health records) be transmitted over wireless networks, a more centralized approach might be more appropriate.

- Account monitoring and control
  If accounts of departed employees are used or usage takes place at odd hours, this hints at malicious activity and should be prevented. To properly identify these events, close cooperation with the human resource and business departments is essential. The organization in the information security realm should reflect the best arrangement with these departments.
- Security skills assessment and appropriate training to fill gaps
  Skilled and alert employees are one of the best defenses of a company. On the contrary, uneducated, neglect or even disgruntled employees are among the biggest threads. And this does not only involve personnel involved in information security, but every person in the company. As mentioned, web browsing and email usage poses a big risk. But at the same time, it's something most employees will be doing. To reach in every corner of a complex organization, distributed solutions are needed. Nevertheless, a central group of advisors should be established.
- Application software security
  In an ideal world, software should accept any input flawlessly, never performs unintended actions and never generate illegal output. The real-world experience teaches that any kind of software (server or client, self-developed or of-the-shelf) is subject to flaws that can be exploited. Advice on these problems should always come from one workgroup in the organization. Following actions for remediation could be undertaken in a distributed way. A feedback from the subsidiaries should be collected centrally.
- Penetration tests and red team exercises
  Sometimes, even in the best plans something is overlooked. To be sure the network and system configurations do really protect from malicious activities, penetration testing makes it stand up against simulated attack attempts. Red team exercises show deficiencies in recovery plans and procedures. Initiation of these activities should always come from a central authority in the organization. Collaboration is inevitably needed from every person involved in administrative tasks. When vulnerabilities, misconfigurations or lacking procedures are detected, a careful discussion has to be initiated. The notion that someone did something wrong has to be avoided under all circumstances. It is advisable to already include these thoughts in the communication preceding testing and exercise activities.

4.2. Spread incident handling

Two elements of the Critical Security Controls will be discussed in this sections with additional focus on the implications of lateral leadership:

- Maintenance, monitoring, and analysis of audit logs
  The assessment of log entries for alerts and anomalies is a central task for detecting malicious activity.
- Incident response and management
  If an incident has been detected, a swift and efficient response to contain and eradicate it should take place.

4.2.1. Central security information and event management

Detecting an incident requires correlation of multiple event in most cases. This implies that all systems of interest send their logs to some kind of central facility to compute the correlations, and generate comprehensive reports. Nevertheless, local staff should not be locked out of this useful information. They might detect something with their intimate knowledge of the local environments that automated systems can't or the central staff is not capable of. Additionally, keeping someone in the loop gives a feeling of relevance and promotes active cooperation. Hence, when looking for a technical implementation of a SIEM system, granular access possibility is a mandatory feature. Just sending some pie chart by email monthly is usually insufficient.

4.2.2. Preparing together, responding coordinated

Apart from detecting an incident, an efficient and quick response is even more important. Detailed planning makes flawless incident response possible. Comprehensive input from headquarters as well as from departments and subsidiaries makes a good strategy possible. While centralizing incident response teams makes perfect sense to ensure a consistent approach, this undertaking may create resistance in the subsidiaries. A separate incident response team in every department and/or subsidiary of an organization can make sense in certain circumstances. Teams in the company periphery are often more involved in and familiar with day-to-day operations. Especially, if physical access to a system is needed, local administrators come into play inevitably. On the other hand, a (central) team of experts should be available for advice and support. A chain of communication should keep everybody informed.

4.2.3. Educate colleagues

"Lessons Learned" from incidents (detection and response) are valuable information for the entire organization and should be shared accordingly. Any report has to be written without putting blame on a person or group. On the contrary, any report can be used to praise the efforts of the people involved. This will improve the motivation to help in subsequent incidents. Additionally, it is advisable to keep in touch with a successful team. These connections can be useful for future collaboration and can provide feedback of any kind. Colleagues who had a positive experience can also smooth the way for collaboration with different participants from the same departments.

5. Conclusions

In summary, it is most important to emphasize that lateral leadership is not an emergency replacement or makeshift solution if leadership by authority fails. On the contrary, it is an efficient and inclusive management style that can create a tremendous amount of value for an organization. If applied properly, colleagues are willing to adopt new approaches and accept differing standpoints. When planning

and implementing improvements in information security, many well-known techniques and ideas already carry properties that can be applied to complex organizations. Examining the basics principles taught in the SANS Security Essentials course (for the corresponding GIAC certification) in the light of lateral leadership potential, the power of these concepts become evident.

Stefan M. Krampe, stefan@krampe.global

References

Cole, E., Krutz, R. L., & Conley, J. W. (2005). *Network security bible*. Indianapolis, IN: Wiley Pub.

Fisher, R., Sharp, A., & Richardson, J. (1998). *Lateral leadership: Getting things done when you are not the boss*. London: HarperCollins.

Strathausen, R. (2015). *Leading when you're not the boss: How to get things done in complex corporate cultures*.

Thalmann, S., Bachlechner, D., Demez, L., & Maier, R. (2012). Challenges in cross-organizational security management. In Annual Hawaii International Conference on System Sciences, R. H. Sprague, University of Hawaii (System), & IEEE Computer Society (Eds.), *Proceedings of the 45th Annual Hawaii International Conference on System Sciences: 4-7 January 2012, Maui, Hawaii* (pp. 5480-5489). Los Alamitos, CA: IEEE Computer Society.

Stefan M. Krampe, stefan@krampe.global

Last Updated: December 14th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Dubai 2018	Dubai, AE	Jan 27, 2018 - Feb 01, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NVUS	Jan 28, 2018 - Feb 02, 2018	Live Event
Cyber Threat Intelligence Summit & Training 2018	Bethesda, MDUS	Jan 29, 2018 - Feb 05, 2018	Live Event
SANS Miami 2018	Miami, FLUS	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS Scottsdale 2018	Scottsdale, AZUS	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS London February 2018	London, GB	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CAUS	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Secure India 2018	Bangalore, IN	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Dallas 2018	Dallas, TXUS	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Brussels February 2018	Brussels, BE	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Secure Japan 2018	Tokyo, JP	Feb 19, 2018 - Mar 03, 2018	Live Event
Cloud Security Summit & Training 2018	San Diego, CAUS	Feb 19, 2018 - Feb 26, 2018	Live Event
SANS New York City Winter 2018	New York, NYUS	Feb 26, 2018 - Mar 03, 2018	Live Event
CyberThreat Summit 2018	London, GB	Feb 27, 2018 - Feb 28, 2018	Live Event
SANS London March 2018	London, GB	Mar 05, 2018 - Mar 10, 2018	Live Event
SANS San Francisco Spring 2018	San Francisco, CAUS	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Secure Osaka 2018	Osaka, JP	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Secure Singapore 2018	Singapore, SG	Mar 12, 2018 - Mar 24, 2018	Live Event
SANS Paris March 2018	Paris, FR	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	OnlineCAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced