Критическая инфраструктура

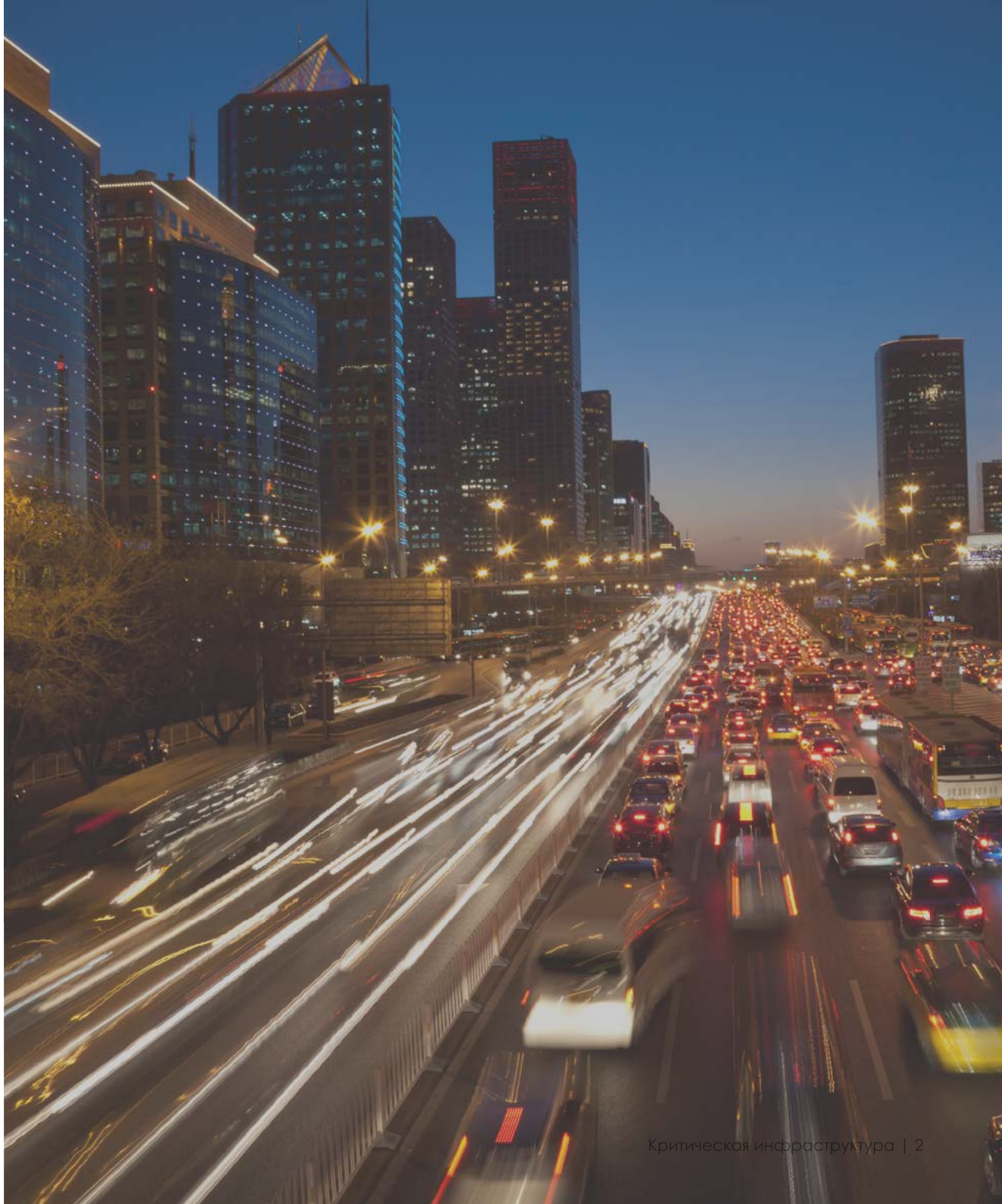
panda

Введение

Одна из самых сильных сторон нашего современного развитого общества является также одним из самых главных его недостатков. В нынешнем взаимосвязанном мире развитые и высокотехнологичные социумы сильно зависят от работы ряда служб и сервисов, которые в настоящее время стали жизненно необходимыми.

Определенная инфраструктура обеспечивает нормальную работу основных служб и производственных систем в любом обществе. Поэтому сбой в их работе в силу естественных причин, технических неполадок или преднамеренных действий может иметь серьезные последствия для поставки ресурсов или работы критических служб, не говоря уже об угрозе безопасности.

В последние годы во всем мире неуклонно растет уровень кибер-преступности. Развитие Интернета и цифровая трансформация общества представляет собой "палку о двух концах", т.к. все это дает определенные возможности для преступников. Но что может произойти, если критически важные сети станут целью для преступного сообщества?



Важные секторы и критическая инфраструктура

Защита критической инфраструктуры является важной проблемой для всех стран. Высокий уровень развития современного общества во многом зависит от ряда основных и важных услуг, в значительной степени оказываемых частным бизнесом.

Инфраструктура обеспечивает нормальную работу крайне важных для развития государства служб и систем: правительственные органы, водоснабжение, финансовые и налоговые системы, энергетика, космос, атомные электростанции и транспортные системы, крупные производственные предприятия.

К критически важной инфраструктуре мы относим объекты, сети, службы и системы, сбой в работе которых в любом случае отразится на здоровье, безопасности и благосостоянии граждан страны.

Гарантированное предоставление жизненно важных услуг в условиях новых угроз - это не только ответственность государственных органов, но также и частных компаний на национальном и международном уровнях.

Технические характеристики

Определенные технические характеристики и уровень уязвимости критических данных в таких сетях означают, что их защита не является тривиальной задачей.

Новые вторжения в кибер-физические системы производственных процессов, запущенных в критической инфраструктуре, создали потребность в новых стратегиях, адаптированных для обнаружения таких угроз без препятствий в работе самой инфраструктуры.

Гибридная архитектура

Различные критические инфраструктуры основаны на гибридной архитектуре, сочетающей в себе классические IT-сети и промышленные OT-сети, которые управляют компонентами, взаимодействующими с физическими объектами (кибер-физические системы).

Изоляция от Интернета

Этот аспект заслуживает отдельного внимания, т.к. растущая тенденция к взаимодействию всех типов инфраструктуры также расширяет количество доступных векторов атаки. Системы контроля для таких инфраструктур, как правило, изолированы от Интернета и подключены в пределах внутренней сети.

SCADA

Впрочем, существуют такие системы контроля SCADA, которые видимы и даже доступны через Интернет. Большинство таких систем не имеют прямой связи с теми системами, которые управляют критической инфраструктурой, но они могут использоваться в качестве шлюза, чтобы хакеры могли получать конфиденциальную информацию для планирования более сложных атак.

Стратегический приоритет решения проблемы

Современные народы сталкиваются с многочисленными проблемами, касающимися национальной безопасности. В этом плане стратегические приоритеты направлены на защиту критической инфраструктуры, которая может подвергаться ряду новых угроз. Для ее защиты важно составить план, который предлагает предотвращение и защиту от потенциальных угроз, как с точки зрения физической безопасности, так и защиты технологий и коммуникаций.

За последние годы произошел ряд ключевых событий, таких как 9/11, которые стали поворотным пунктом в глобальной безопасности. С тех пор в мире сложилась ситуация, когда сбой в работе определенных объектов критической инфраструктуры может повлиять на здоровье, безопасность и благополучие не только отдельных людей, но и целых наций.

Изменился и подход к обеспечению безопасности таких объектов. Раньше безопасность являлась исключительной прерогативой государственных органов. Теперь объекты критической инфраструктуры, в основном, находятся в руках частного бизнеса, а потому он также несет серьезную ответственность за их безопасность. После трагедии 11 сентября США создали Министерство внутренней безопасности и приняли целый ряд соответствующих законов и постановлений.

В Европе подобная инициатива появилась после своего ключевого события: 11 марта 2004 года, взрывы поездов в Мадриде. Европейская комиссия разработала глобальную стратегию по защите критической инфраструктуры ("The European Programme for Critical Infrastructure Protection"), которая включает в себя комплекс мер по профилактике, предотвращению и реагированию на террористические атаки в Европе.

Среди прочего, директива устанавливает, что основная и конечная ответственность за защиту критических инфраструктур лежит на государствах-членах Евросоюза и операторах такой инфраструктуры, а также она настоятельно призывает все страны Евросоюза внедрять в свое национальное законодательство ряд мер и инициатив.

11/09 США → DHS

11/03 Европа → EPCIP

История атак

В целом, общественность, хоть и допускает определенные риски, но все же считает, что в реальности речь может идти о небольшом количестве кибер-атак на критическую инфраструктуру. К сожалению, все намного печальнее: мы уже знаем сотни задокументированных случаев таких атак во всем мире. Атаки на такие сети ведутся уже десятилетия, и ниже Вы сможете познакомиться с историей таких атак.

Сибирский нефтепровод

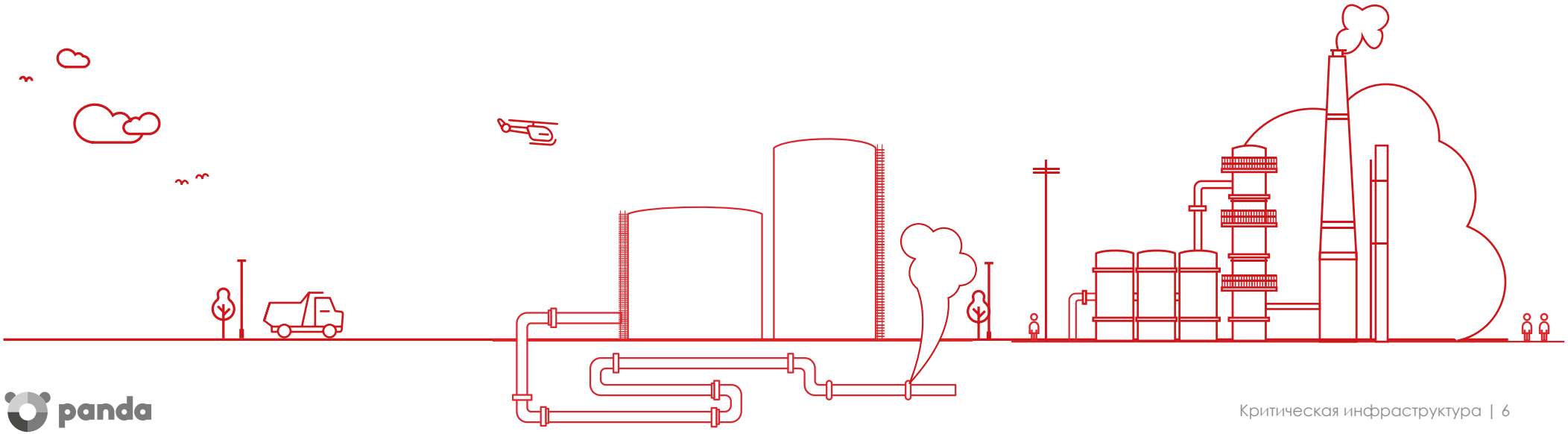
Термин "Интернет" приходит на ум всякий раз, когда мы думаем о кибер-атаках на критическую инфраструктуру.
Но первая подобная кибер-атака произошла еще до появления Интернета - в **1982** году. Тогда группа хакеров смогла установить троян в SCADA-систему, которая контролировала работу сибирского нефтепровода, что привело к мощному взрыву. Атака была организована ЦРУ, хотя об этом не было известно до 2004 года, когда бывший секретарь Министерства обороны США и советник Р. Рейгана Томас Рид опубликовал свою книгу “At the Abyss: An Insider’s History of the Cold War”.

Взрыв сибирского нефтепровода был спровоцирован ЦРУ

Chevron

Следующий инцидент произошел спустя десять лет, в **1992** году, когда был уволен рабочий нефтяной компании Chevron, который взломал компьютеры в офисах компании в Нью-Йорке и Сан-Хосе, отвечавшие за системы предупреждений, перенастроив их на аварию после запуска системы. Этот саботаж не был раскрыт до тех пор, пока не произошло утечки ядовитого вещества в Редмонде (штат Калифорния), при этом система не выдала соответствующих предупреждений. В результате тысячи людей были подвержены огромному риску в течение 10 часов, пока система была отключена.

Утечка токсичного вещества, что подвергло риску жизни тысяч людей



Salt River Project

В августе **1994** года Лейн Джаррет Дэвис сумел взломать сеть Salt River Project, получив доступ к информации и удалив файлы из системы, отвечающей за мониторинг и подачу воды и электричества. Он также сумел получить доступ к персональным и финансовым данным клиентов и сотрудников компании.

Удаление файлов из системы, отвечающей за мониторинг и подачу воды и электричества

Аэропорт Worcester

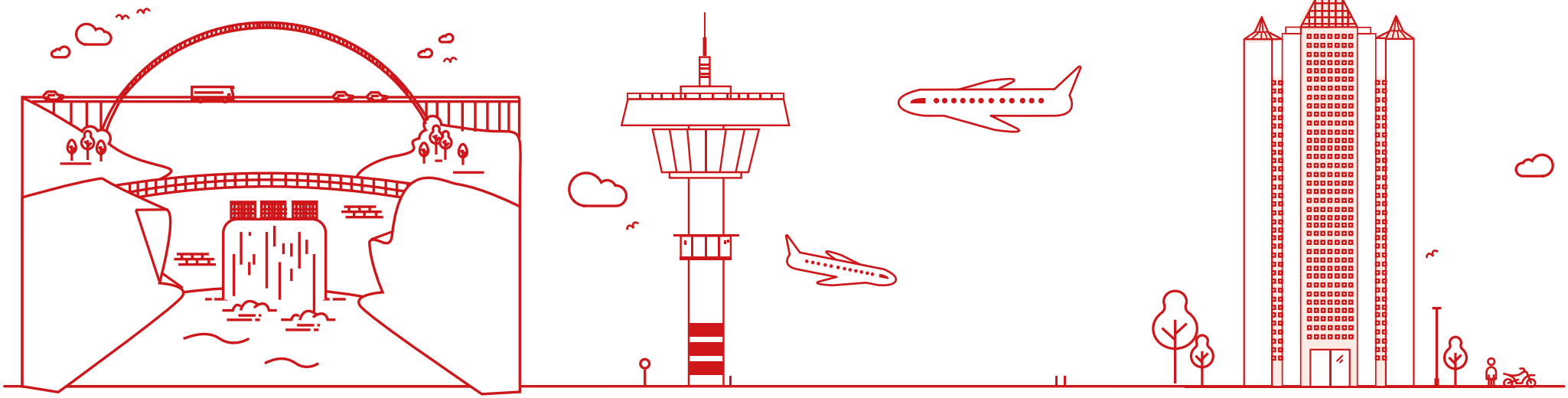
Другие ключевые секторы также пострадали от направленных атак. 10 марта **1997** года хакер проник в систему управления, используемую для коммуникаций системы контроля воздушного движения в Вустере (США, штат Массачусетс), вызвав сбой системы, которая отключила телефонную связь на шесть часов. Особенно это повлияло на телефонную систему башни управления, пожарной службы аэропорта и авиакомпаний, базирующихся в аэропорту.

Сбой системы, повлиявший на телефонную систему башни управления, пожарной службы аэропорта и авиакомпаний, базирующихся в аэропорту, в течение 6 часов

Газпром

В **1999** году хакеры нарушили работу систем безопасности российского энергетического гиганта - компании "Газпром". С помощью инсайдера они использовали троян, чтобы иметь возможность управлять SCADA-системой, контролирующей подачу газа. К счастью, это не привело к серьезным последствиям, а нормальная работа системы была восстановлена в кратчайшие сроки.

Хакеры смогли управлять в Газпроме системой, контролирующей подачу газа



Maroochy Water System

Бывший сотрудник Maroochy Water System (Австралия) получил два года тюремного заключения за взлом в **2000** году системы управления водоснабжением, в результате чего миллионы литров сточных вод попали в ближайшую реку, что привело также к затоплению местной гостиницы.

Слив миллиона литров сточных вод в реку

Газоперерабатывающий завод

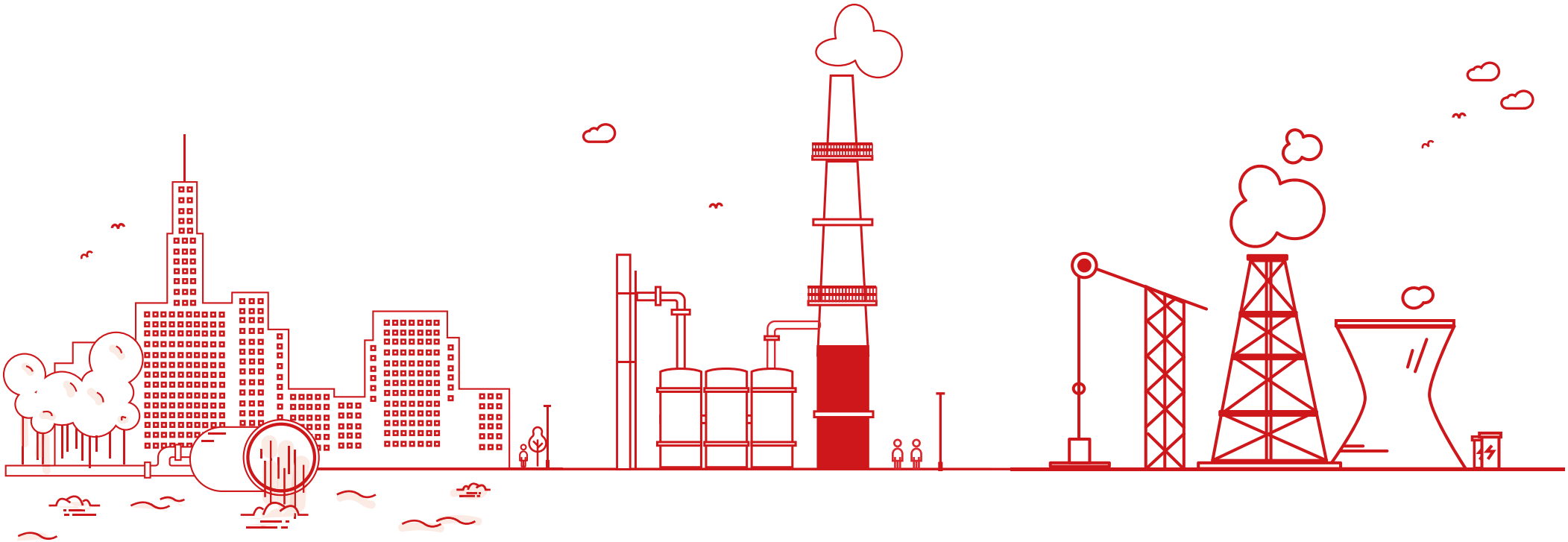
Газоперерабатывающий завод, построенный одной американской компанией, также подвергся атаке в **2001** году. 6-месячное расследование показало, что атака была проведена одним из поставщиков, который для сокрытия сделанной им ошибки, решил отвлечь внимание, взломав три ПК компании и вызвав отключение подачи газа для домашних и корпоративных клиентов в одной из европейских стран.

Атака привела к отключению газа у домашних и корпоративных клиентов в одной из стран Европы

PDVSA

В декабре **2002** года нефтяная компания PDVSA из Венесуэлы подверглась атаке, в результате которой добыча нефти сократилась с 3 млн. до 370 тыс. баррелей в сутки. Во время атаки было взломано несколько корпоративных компьютеров. Она была проведена во время забастовки сотрудников предприятия, чтобы можно было предположить их причастность.

Атака сократила добычу нефти с 3 млн. до 370 тыс. баррелей в сутки



Светофоры в Лос-Анджелесе

В **2006** году два инженера по организации дорожного движения в Лос-Анджелесе взломали городские светофоры в знак протеста. Им удалось изменить программу работы некоторых светофоров, размещенных на важных участках, после чего они стали гореть красным цветом, что привело к серьезным пробкам.

Хакерская атака привела к серьезным пробкам

Трамвайная сеть в Лодзе

В **2008** году 14-летний студент взломал системы трамвайной сети в польском городе Лодзь, в результате чего 4 трамвая сошли с путей, а 12 человек получили травмы. Студент создал инфракрасный пульт дистанционного управления, как у телевизоров, с помощью которого он смог контролировать трамвайные перекрестки.

В результате кибер-атаки 4 трамвая сошли с рельсов, 12 человек получили травмы

Saudi Aramco

В **2012** году крупнейшая нефтяная компания в мире Saudi Aramco стала жертвой направленной атаки на свои офисы. Хакеры получили доступ к сети благодаря атаке на одного из сотрудников компании, через которого смогли получить доступ к 30 000 компьютеров в сети. В какой-то момент хакерам удалось удалить содержимое всех компьютеров, в то время как на экранах показывался горящий американский флаг. Ответственность за атаку взяла на себя группа хакеров, называвших себя “Меч правосудия”.

Удаление содержимого с каждого компьютера, в то время как на экранах показывался горящий американский флаг

Ram Gas

Всего лишь через две недели после атаки на Saudi Aramco, катарская компания RamGas, второй в мире производитель сжиженного природного газа, был атакован той же вредоносной программой, которая использовалась для атаки на нефтяную компанию из Саудовской Аравии. В течении нескольких дней не работали внутренняя корпоративная сеть и веб-сайт компании.

Хакерская атака обрушила корпоративную внутреннюю сеть и веб-сайт компании

Металлургический завод в Германии

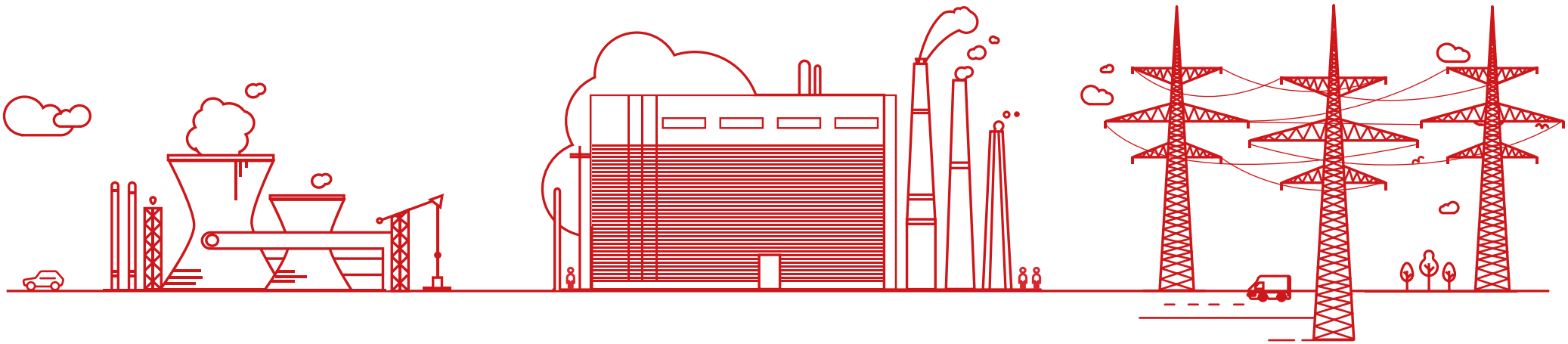
В **2014** году в Германии жертвой атаки стал один из металлургических заводов. Используя социальную инженерию, хакеры сумели получить доступ к компьютеру одного сотрудника, с которого они смогли получить доступ к внутренней сети системы управления. В результате этого стало невозможным выключить одну из домен, что нанесло огромный ущерб предприятию.

Кибер-атака нанесла огромный ущерб металлургическому заводу

Электросеть Украины

В конце **2015** года Украина подверглась кибер-атаке на свою национальную электросеть, в результате чего свыше 600000 жителей остались без электричества.

Кибер-атака оставила без электроэнергии свыше 600 0000жителей Украины



Первая в истории кибер-атака против Интернет-инфраструктуры

Несмотря на длинный список инцидентов, первая в истории кибер-атака на Интернет-инфраструктуру произошла 27 апреля **2007 года, когда в Эстонии ряд атак обрушил сайты различных организаций**, включая парламент, различные министерства, банки, газеты и различные СМИ и т.д.

Впрочем, атака также была направлена на определенные непубличные адреса, включая национальную систему обработки финансовых ордеров и телекоммуникационные службы. Урмас Пает, министр иностранных дел Эстонии, публично обвинил российские власти в причастности к данным атакам, хотя он не смог предоставить каких-либо доказательств этому.

Самый известный случай кибер-атаки на критическую инфраструктуру: Stuxnet

В **2008** году мы стали свидетелями одного из самых печально известных в истории случаев кибер-атак на критические инфраструктуры: **Stuxnet. Сейчас уже известно, что это была скоординированная атака израильских и американских спецслужб, направленная на срыв ядерной программы Ирана**.

Они создали червя, который заразил компьютеры, управляющие урановыми центрифугами на иранском заводе в Натанзе, в результате чего они стали работать на полной скорости, в то время как инженеры на своих мониторах наблюдали нормальный режим работы. Это нанесло физический ущерб всем урановым центрифугам на заводе. После этого случая общественность узнала о подобного рода угрозах.

Атаки в других компаниях также затрагивали объекты критической инфраструктуры

Помимо атак, специально осуществляемых для причинения ущерба подобного типа инфраструктуры, атаки, подобные тем, с которыми сталкиваются другие компании, также негативно влияют на критические объекты, а последствия иногда были такими же серьезными. **Подобные проблемы в основном начались в конце прошлого десятилетия, т.к. сетевые черви стали распространяться в Сети сами по себе.**

Например, случай на ведущей в США фабрике по выпуску продуктов питания, когда вирусная инфекция нанесла ущерб, измеряемый тысячами долларов. Один сотрудник удаленно подключился с домашнего ПК, который был заражен вирусом Nimda. Как только он вошел в корпоративную сеть, червь распространился на все системы управления.

В 2003 году нефтяная компания из США пострадала от червя SQLSlammer, который проник во внутреннюю сеть. Хотя это не привело к остановке производства, но он повлиял на внутренние коммуникации. Пришлось потратить несколько дней для полного удаления червя из сети и обновления систем для предотвращения дальнейших атак. Кстати, данный червь был одним из самых разрушительных для компаний.

Для распространения, он использовал уязвимость в серверах баз данных SQL (стандартный инструмент в корпоративных сетях). Уязвимость была исправлена Microsoft в январе 2003 года. Кстати, другая американская нефтяная компания начала обновлять все свои объекты сразу же после появления этого патча, чтобы оградить себя от этого червя. Однако, для завершения обновления необходимо было перезагрузить серверы, на которых этот патч был установлен, в то время как некоторые из них находились на нефтяных платформах, где не было выделенного IT-персонала. Для этого пришлось отправлять специалистов на вертолете. И пока они не успели приехать, червь проник в некоторые корпоративные системы и заразил те из них, которые еще не успели обновить.

Ò ⱥɘ ɒɑ 2003 ɣəɐɟ əɔɔə ɔɓ ɖʒɟɛəɜɑɤɔg Rɣⱥəɛɜəɔɓɣəɒɔⱥɑɗɑɛ ɣ Ł ЧŐ ⱥRɖɒɑ ɛəɜⱥɜRɐRɗ əⱥ RⱥRɖɔ ɣɑɜɣɑə SQLSlammer, ɖəⱥⱥɜɦɛ əɣəəɣɑəəə ɜRɜɛɜəɜⱥɜRəɔɗʒɬ əR ɑɣə 17 ɓRɣəɐRg. Ⱥɾ ɥ ɔɛ ɟ ɥ ɑɜɾ ɐɗɬ ɖə ə ɛRəɔɔ ɜəɜⱥRɣɔɗ 150 əɖə. ɐəɗɗRɜəɣ Ł ЧŐ. ʔəⱥɬ ɛRⱥɣ ɟɒɑ ɾɦɗ ɐəɜⱥɟɛɑə əR ɛɜəⱥɬɒɑəɔɔ ɤ ɑɜⱥɔ əɑɜɬɡɑɣ, ⱡɣ-ə ɑəɑɐɒɑɜɦ ɖə ə ɛRəɔɔ ɐə ɜɔg ɛə ɜ əɑ ɟɜⱥRəəɣɔɗɔ ɑɣə.

Ò ⱥɘ ə ɒɑ ɣəɐɟ əⱥ ɣɜɑɐəəəɜəəɛ ɔə ɡ ɑɖɡɔɔ (ⱥR ɣɜɑɐəəəɜəRɬ ɛɜəɣɜR ə əR əɑ ɾɦɗR ɛɟɾɗɔɣəəɛ) ɛəɜⱥɜRɐRɗ ɖə ə ɛɨ ɨ ɡɑɜ RɣɔRɖə ə ɛRəɔɔ Air Canada, əⱥɣɑɣR ɨ ɥ ɔɛ ɓR ɖɑⱥəɟ ɨ ɔə ɡ ə ɜ əRɡɔɔ ɨ, ɓRɛɜRɣɖɟ ⱥəɛɗɔɣR ɔ ɛɜ. Ò ɜɑɓɟɖɨⱥRⱥɑ ɔə ɡ ɑɖɡɔɔ 200 ɜɑɛɜəɣ ɾɦɗɔ ɓRɐɑɜɒRəɦ ɔɗɔ əⱥə ɑəɑəɦ.

Ò 2005 ɣəɐɟ ɣ ɖɛəəɔɔ ɖə ə ɛɨ ɨ ɡɑɜ ɜəⱥɜɟəɔɖR ɖə ə ɛRəɔɔ Mitsubishi Electric ɾɦɗ ɓRɜRɒɑə ɣɜɑɐəəəɜəəɛ ɛɜəɣɜR ə əɑɛ, ɣⱥə ɛɔɣɑɗə ɖ ɟⱥɑɣɖɑ ɖəə ɡ ɔɐɑəɡɔRɗɨəɦg ɔəɜɛɑɖɡɔəəəɦg əəɟ ə ɑəⱥəɣ ə əɣɟg Rⱥə ə əɦg ɨɗɑɖⱥɜəɜⱥRəɡɔɬg, ɛɜɔəRɐɗɑɒR ɥ ɔg ɐRəəəɛ ɖə ə ɛRəɔɔ.

Ò 2006 ɣəɐɟ ɐɣR ɖə ə ɛɨ ɨ ɡɑɜR ɣ ɾəɗɨəɔɡɑ (Ò ɑɗɔɖə ɾ ɜɔⱥRəɔɬ), əⱥɣɑɣR ɨ ɥ ɔɑ ɓR ɟɛɜRɣɗɑəɔɑ ɖə ə ɛɗɑɖɜəə ɗɟɣɑɣəɛ ⱥɑɜRɛɔɔ ɐɗɬ ɾəɗɨəɦg ɜRɖə ə ɗ ɨ ɐɑɛ, ɾɦɗɔ ɓRɜRɒɑəɦ ɣɜɑɐəəəɜəəɛ ɛɜəɣɜR ə əɑɛ. Ò ɜɑɓɟɖɨⱥRⱥɑ ɨⱥəɣə ɛɜɔ ɤ ɖəɜɨ əⱥɗəɒɔⱥɨ ɗɑɣɑəɔɑ 80 ɛRɡɔɑəⱥəɣ. Ł ɛɟɜⱥɬ ɐɣR ɣəɐR ɑ ɥ ɑ ⱥɜɔ ɾəɗɨəɔɡɦ ɣ Ò ɑɗɔɖə ɾ ɜɔⱥRəɔɔ ɾɦɗɔ ɓRɜRɒɑəɦ ɣRɜɔRⱥəə ɣɑɜɣɬ Mytob, ɛəɜɖɑ ɣɑɣə ɛɜɔ ɤ ɖəɜɨ əⱥɖɟɨɣɔⱥɨ ɣɜɑ ɖə ə ɛɨ ɨ ɡɑɜɦ əⱥ ɜɑⱥɔ əR 24 ɣRɜR ɐɗɬ ɜɑ ɤ ɑəɔɬ ɔəɡɔɐɑəⱥR.

Ò 2013 ɣəɐɟ ɾɦɗɔ ɓRɜRɒɑəɦ 200 ɖə ə ɛɨ ɨ ɡɑɜəɣ ÖɑɛRɜⱥRə ɑəⱥR Rɣⱥəɣəɾɔɗɨəɦg ɐəɜəɣ ɔ ⱥɜRəɜɛəɜⱥR ɣ əɖɜɟɣɑ ɬɟɖ (ɤⱥRⱥ ⱡɗɗɔəəɛɜ, Ł ЧŐ). ɟⱥɔ ɜɔɜⱥɑə ɦ əⱥɣɑɣRɗɔ ɓR ɛəɐɑɐɑɒRəɔɑ ɜəⱥəɔ ɖɔɗə ə ɑⱥɜəɣ ɐəɜəɣ ɣ ɛɜɔɣəɜəɐɑ ɮɔɖRɣə. Ò ɜɑɓɟɖɨⱥRⱥɑ RⱥRɖɔ пришлось отключать сеть на 9 дней, чтобы вылечить все компьютеры.

Этот список инцидентов показывает, что опасность кибер-атак на критические инфраструктуры вполне реальна, и сегодня правительства всех стран знают об этих рисках.

Дополнительная защита для критической инфраструктуры

Учитывая реальность, которую мы наблюдаем и в которой мы живем, необходимо регулировать защиту критической инфраструктуры, чтобы обеспечить ей более высокий уровень защиты от всех типов угроз.

В мае 2016 года после встречи министров энергетики стран G7, была принята совместная декларация, в которой, среди прочего, был поставлен акцент на важности создания отказоустойчивых энергосистем (включая газ, электричество и нефть), чтобы эффективно реагировать на появляющиеся кибер-угрозы и поддерживать нормальную работу жизненно необходимых служб.

Чтобы усовершенствовать меры по предотвращению и реагированию на логические атаки, правительства стран осуществляют ряд мер на глобальном уровне. Эти меры направлены на создание центров по сбору всей необходимой информации для улучшения защиты критических инфраструктур. Как результат, была разработана комплексная стратегия для решения данной проблемы, которая должна быть включена в национальное законодательство этих стран.

Нелегко ответить на вопрос, насколько безопасность объектов критической инфраструктуры адекватна в настоящее время, т.к. неизвестна информация или техники, которые могут быть использованы кибер-преступниками, а потому нельзя быть на 100% в безопасности. Что можно улучшить - это защиту от известных атак, для предотвращения которых необходимо применять ряд эффективных мер:

Эффективные меры

1. **Проверка систем на уязвимости, особенно тех систем, на которых уже были зафиксированы дыры безопасности и они были известны в течение некоторого времени.**
2. **Адекватный мониторинг сетей, используемых для контроля таких объектов критической инфраструктуры, и при необходимости их полная изоляция от внешних соединений, что позволит обнаруживать внешние атаки и предотвращать доступ к системам, управляемым из внутренней сети.**
3. **Контроль над съемными устройствами, что важно в любой инфраструктуре не только потому, что они являются направлением таких атак, как в случае с Stuxnet. При защите таких объектов критической инфраструктуры крайне важно, чтобы вредоносные программы не проникали во внутреннюю сеть через съемные устройства, которые также могут использоваться и для кражи конфиденциальной информации.**
4. **Мониторинг ПК, к которым подключены программируемые логические контроллеры (или PLC). Эти подключенные к Интернету устройства являются наиболее чувствительными, т.к. они могут предоставлять хакерам доступ к критически важным системам управления. Даже если они не смогут получить контроль над системой, они смогут получить ценную информацию для других направлений атаки.**

Решение

Решение состоит в защите от современных угроз и направленных атак, которая также должна позволить обнаруживать необычное или подозрительное поведение. Система, которая должна обеспечить конфиденциальность данных, защиту активов и репутации компании.

Интеллектуальная платформа, которая может помочь специалистам по безопасности критической инфраструктуры оперативно реагировать на угрозы и получать всю необходимую информацию для подготовки адекватного ответа.

Это Adaptive Defense 360 - единственная система расширенной ИТ-безопасности, которая сочетает новейшие технологии защиты и современные технологии обнаружения и реагирования на атаки с возможностью классификации 100% выполняемых процессов.

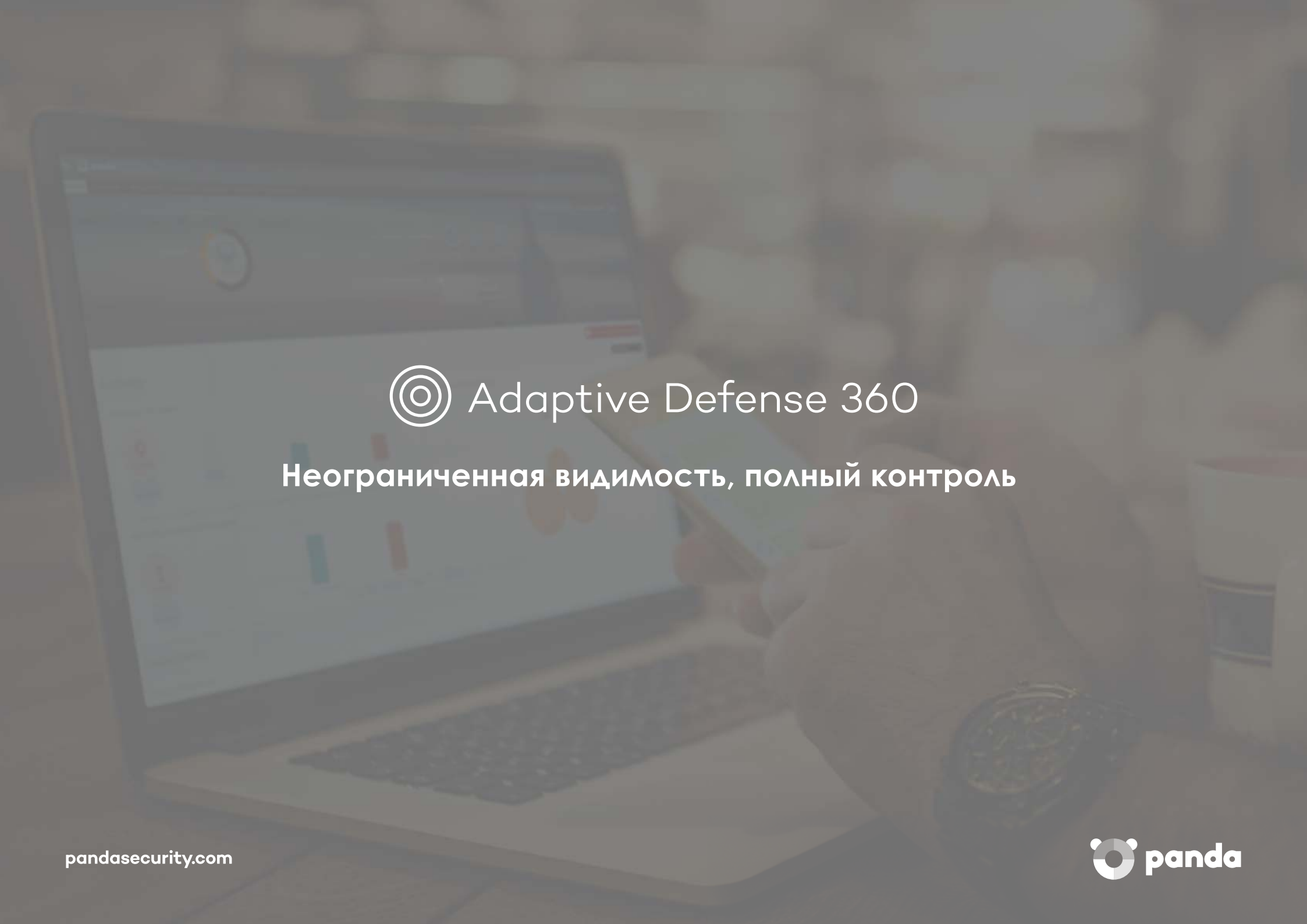
Adaptive Defense 360 классифицирует абсолютно все активные процессы на компьютерах, обеспечивая защиту от известных вредоносных программ и атак "нулевого дня", постоянных угроз повышенной сложности (APT) и направленных атак.

Платформа использует контекстную логику для выявления вредоносных моделей поведения и генерации улучшенных действий информационной защиты от известных и неизвестных угроз.

Решение анализирует, классифицирует и сопоставляет все собираемые данные о кибер-угрозах, чтобы выполнять задачи по предотвращению, обнаружению, реагированию и восстановлению.

Решение определяет, каким образом и кем был осуществлен доступ к данным, а также контролирует утечку данных в результате работы вредоносных программ или действий сотрудников.

Решение обнаруживает и устраняет системные уязвимости и дыры в установленных программах, а также предотвращает использование нежелательных приложений (тулбары, рекламное ПО, дополнения и пр.).



Adaptive Defense 360

Неограниченная видимость, полный контроль

pandasecurity.com

panda

Подробная информация:

pandasecurity.com/russia/enterprise/solutions/adaptive-defense-360/

По телефону:

+7 495 105 94 51

или по почте sales@rus.pandasecurity.com

panda